INVESTIGATIO
UNA PUBLICACIÓN DE LA UEES
UNIVERSIDAD ESPÍRITU SANTO
ISSN impreso: 1390-6399 | e-ISSN: 2602-8336

Investigatio
ISSN: 1390 - 6399 • ISSN-e: 2602 - 8336
Edita: Universidad Espíritu Santo © – UEES

Mapeo de la Estructura Intelectual de la Ingeniería Social: Un Estudio de Co-Citación y Acoplamiento Bibliográfico - Mapping the Intellectual Structure of the Social Engineering: A Co-Citation and Bibliographic Coupling Study

Mapeo de la Estructura Intelectual de la Ingeniería Social: Un Estudio de Co-Citación y Acoplamiento Bibliográfico - Mapping the Intellectual Structure of the Social Engineering: A Co-Citation and Bibliographic Coupling Study

Cristian Fabián NAVAS CAJAMARCA [1] **0000-0000-0000-0000**
Saulo David PÉREZ PUCHI [2] **0000-0000-0000-0000**

[1] Universidad Espíritu Santo, Guayas, Ecuador
[2] Universidad Espíritu Santo, Guayas, Ecuador

Cita: NAVAS CAJAMARCA, C., & Pérez Puchi, S. D. . Mapping the Intellectual Structure of the Social Engineering: a Co-citation and Bibliographic Coupling Study. INVESTIGATIO, 1(20). https://doi.org/10.31095/investigatio.2023.20.10

Fechas · Dates
Recibido: 01.04.2022
Aceptado: 09.09.2022
Publicado: 29.03.2023

Correspondencia · Corresponding Author
Cristian Fabián NAVAS CAJAMARCA
Universidad Espíritu Santo, Guayas, Ecuador
cfnavasc@uees.edu.ec

Resumen

Este artículo tiene como objetivo mapear la estructura intelectual del comportamiento de la ingeniería social (IS) basado en el análisis bibliométrico de co-citación (base de conocimiento) y acoplamiento bibliográfico (frente de investigación). Esta investigación presenta la conceptualización de IS, ingeniería social en la informática, análisis de idoneidad de seguridad, taxonomía de clasificación de ataques de IS y principios psicológicos de IS aplicado a las Tecnologías de la Información; se analizaron un total de 62 artículos de investigación de *Web of Science* de las últimas dos décadas. En la base del conocimiento, el análisis encontró artículos de co-citación que están relacionados principalmente con capacitación sobre métodos defensivos, marcos o mecanismos de trabajo para la concienciación y prevención de ataques de IS y actividades de comportamiento humano. En cuanto al frente de la investigación, el análisis nos muestra una clara tendencia hacia los métodos que se enfocan principalmente en componentes de trabajo para la concientización y prevención de ataques de IS, capacitación sobre métodos defensivos en las actividades del comportamiento humano. Los hallazgos son similares a la base de conocimientos. Se proponen investigaciones futuras para realizar nuevamente un análisis de co-citación y compararlo con los resultados del presente trabajo para establecer cualquier variación ya que su conocimiento científico se incrementa con el tiempo.

Palabras clave: Ataques de Ingeniería social, prevención, capacitación y concientización, engaño, seguridad de la información.

Abstract

This article's objective is to map the intellectual structure of the Social Engineering Behavior (IS) based on the bibliometric analysis of co-citation (knowledge base) and bibliographic coupling (research front). This research presents the conceptualization of IS, social engineering in computing, safety suitability analysis, IS attack classification taxonomy and psychological principles of IS applied to information technologies; a total of 62 Web of science research articles from the last two decades were analyzed. In the knowledge base, the analysis found co-citation articles related mainly to the training about defensive methods, framework or mechanisms of work for the awareness and prevention of the IS attacks and human behavior activities. Regarding the research front, the analysis shows us a clear tendency to the methods focused mainly on the mechanisms of work for the awareness and prevention of the IS attacks, training about defensive methods in human behavioral activities. The findings are similar to the knowledge base. Future inquiries are proposed in order to make an analysis again about co-citation and compare with the results of our work for establishing any variation since the scientific knowledge increases through the time.

Keywords: Social Engineering attacks, prevention, training and awareness, fraud, information security.

Introducción

Un acontecimiento que revolucionó la industria del hardware y software tuvo sus inicios en los años setenta con la aparición del microprocesador Noyce & Hoff (1981), relatan que este componente permitió por primera vez la construcción del computador personal (PC)(Noyce & Hoff, 1981). En la actualidad la evolución del PC trajo consigo nuevas tecnologías que integran a toda la humanidad (Cotteleer & Sniderman, 2017). Además, el desarrollo acelerado de las Tecnologías de la Información (TI), precisan que la informática está cada vez más cerca de convertirse en uno de los servicios básicos juntamente con el agua, gas, electricidad, y telefonía. Por consiguiente, las TI son esenciales para satisfacer las necesidades cotidianas de las personas, generando una alta dependencia de ellas (Buyya et al., 2009). Paralelamente a estos desarrollos el ingenio humano también ha evolucionado a pasos agigantados. Creando un sin número de aplicaciones de software para los diferentes escenarios de aplicación, con la finalidad de solventar las necesidades personales y corporativas. Así pues, el concepto de Ingeniería Social (IS) apareció en un artículo anónimo a mediados de la década de los ochenta. La IS consiste en el uso del engaño, para inducir a una persona a entregar involuntariamente información privada y proporcionar acceso no autorizado a un sistema de información o una red de computadores Joseph M. Hatfield (D, 2017). Hay que destacar que los ataques de ingeniería social son los ataques más poderosos porque amenazan a todas las infraestructuras de TI (Salahdine, 2019). Los expertos en seguridad de la información proponen que a medida que nuestra cultura se vuelva más dependiente de las TI, la ingeniería social se convertirá en la mayor amenaza para cualquier sistema de seguridad. Es decir, la IS explota las debilidades humanas aplicando ataques no técnicos basados en la interacción humana con el único afán de penetrar sistemas ajenos; uno de estos es el uso de la persuasión (Bull et al., 2015).

Ahora bien, Andreas Makridakis (2010), sostiene que la aparición masiva de redes sociales en línea, alojan información de millones de usuarios (Makridakis et al., 2010). Por consiguiente, son una fuente única de aplicación y explotación de técnicas de IS convirtiéndolas en redes antisociales. Es decir, plataformas para actividades maliciosas e ilegales como: violaciones de privacidad, accesos no autorizados, ataques distribuidos de denegación de servicio, entre otros. Así pues, la IS se ha convertido en una amenaza superior a las demás formas de piratería, su aplicación puede penetrar infraestructuras tecnológicas con altos estándares de seguridad física y lógica. El elemento clave para materializar esta amenaza son las personas, consideradas como el eslabón más

débil y vulnerable en lo referente a seguridad. Hay que tener en cuenta que la IS por su facilidad de automatización puede implementarse a gran escala o de manera específica. Por ejemplo, algunos vectores de ataque son: correos electrónicos de fuentes "confiables" (*phishing*), llamadas simuladas por teléfono (*vishing*), y suplantación de identidad (Krombholz et al., 2015).

En efecto estos vectores suelen ser efectivos atacando y obteniendo información confiable de gran fuente. Esto incrementa en cuatro veces más el número de probabilidades de convertirse en víctimas potenciales de los ingenieros sociales. Vale la pena decir que el *phishing* se ha convertido en uno de los riesgos de alto impacto gracias a sus facilidades de ataque; ofuscando y dificultando a la justicia la determinación de indicios y responsabilidades (Jagatic et al., 2007).

Airehrour y sus colegas (2018) sostienen que los vectores de ataque están técnicamente orientados a la manipulación psicológica y crecen a pasos agigantados sin un final definido (Airehrour et al., 2018). Cuando una persona se siente amenazada la persuasión es un elemento clave para reaccionar ante cualquier adversidad y se fundamenta en: la confianza, el miedo y el compromiso. Dicho de otra manera, crean una reacción defensiva que evade el ataque o permite la manipulación exitosa (Hjørland, 2010).

Según Grazioli (2004), los usuarios que realizan transacciones comerciales en línea tienen dos tipos de comportamiento que evalúan inconscientemente la posibilidad de engaño. Primero se aseguran evaluando el logotipo, sello del producto, términos de garantía, costo y reputación del sitio mediante un análisis de los comentarios de compradores anteriores. Por el contrario, lo segundo es valorar únicamente la apariencia del sitio web como sinónimo de alta confianza (Grazioli, 2004).

En cuanto a una encuesta aplicada a 3245 empresas ecuatorianas de los sectores del comercio, servicios, manufactura y minería. Describe que el 13,9% y el 9,2% utiliza el internet para realizar actividades de compras y ventas respectivamente. Además, el 95,3% de ellas utilizó el correo electrónico como medio de comunicación. Este es un indicador de que las corporaciones y sus usuarios finales son dependientes de las TI (Instituto Nacional de Estadística y Censos INEC, 2015). Además, en Ecuador, el uso de Internet y de teléfonos inteligentes ha aumentado en un 39,6% y 51,4% respectivamente en los últimos 6 años. Actualmente más de 5.4 millones de habitantes utilizan redes sociales online. Cifras que han ido aumentando con un crecimiento exponencial (Servicio Ecuatoriano de Normalización INEN, 2017). Al mismo tiempo el boletín publicado por la Fiscalía General del Estado (Fiscalía General del Estado, 2015), puntualiza que se receptaron 626 denuncias. Todas ellas relacionadas con el espionaje, suplantación de identidad, transferencias de dinero no autorizadas, obtención fraudulenta de datos personales, apropiación ilegal de números de tarjetas de crédito entre otros. Hay que puntualizar que los escenarios de ejecución de estas actividades son entornos de TI.

Al respecto, un estudio elaborado por la Policía Nacional, Interpol, y el Centro de Respuesta a Incidentes Informáticos del Ecuador. En coordinación con organismos similares de América Latina, menciona que el 85% de estas denuncias están relacionadas con ataques a los sistemas informáticos. En efecto los usuarios afectados carecen del conocimiento que les permita tomar las precauciones necesarias para gestionar sitios web tales como: redes sociales, correo electrónico, banca en línea y demás aplicaciones informáticas (El Telégrafo, 2016). Por lo que se refiere a Ecuador, las estadísticas referentes a violaciones de seguridad han sido en su mayoría dentro del

sistema financiero. Así en el 2014 se registró un aumento de 37% de robos a la banca virtual, 14% en tarjetas de crédito y 46% en cajeros electrónicos (Sancho-Hirare, 2017). Además, un estudio realizado con la participación de cinco entidades bancarias, sus autoridades revelaron que a menudo se enfrentan a ataques de *phishing* que pretenden obtener las credenciales de la banca electrónica de sus clientes. Agregaron que la falta de conciencia, capacitación y entrenamiento de los usuarios en la mayoría de los casos permiten que se comentan fraudes (Catota et al., 2018).

Con estos antecedentes se puede observar que los delincuentes utilizan una amplia variedad de técnicas de ataque de IS para inducir a la víctima en la toma de decisiones carentes de autonomía con la finalidad de materializar el objetivo malicioso (Bullée et al., 2017). Hay que mencionar, que es de vital importancia que todos los usuarios que ocupan plataformas digitales estén en la capacidad de reconocer las posibles amenazas. En definitiva, aplicar procedimientos de seguridad, detendrán a los ingenieros sociales al intentar eludir el control humano. Finalmente cabe mencionar, el simple hecho de que un usuario esté consciente, que ninguna persona de su entorno le solicitará sus contraseñas, puede ser la diferencia para frenar un ataque exitoso (Applegate, 2009).

Por este motivo, el objetivo de este artículo es identificar la cronología de investigación basada en el mapeo de la estructura intelectual de la ingeniería social utilizando análisis de co-citación y análisis de acoplamiento bibliográfico. La finalidad es garantizar que los usuarios comprendan las posibles vulnerabilidades técnicas y humanas sobre ataques dirigidos de Ingeniería Social (Kritzinger & Von Solms, 2010).

Marco Teórico

La Ingeniería Social en la Informática

La ingeniería social en sus inicios únicamente era utilizada por los planificadores de políticas, gente de negocios y los gobiernos como una técnica de conocimientos superiores. Su finalidad era y es la de inducir en el comportamiento de las masas. La IS en el contexto de seguridad cibernética comenzó con el "*phreaking telefónico"* a fines de la década de 1950 e inicios de 1970, consistía en hacer llamadas telefónicas sin pagar por ellas. Aquí es cuando la IS toma lugar en las Tecnologías de la Información hasta la actualidad Joseph M. Hatfield (D, 2017).

En el libro El Arte del Engaño de Mitnick (2003), relata que la IS utiliza la influencia, la persuasión y la manipulación para engañar a las personas y convencerlas de que el ingeniero social (atacante), es alguien que no lo es. Como resultado, el ingeniero social se aprovecha de las personas para obtener información con o sin el uso de la tecnología (Kevin D. Mitnick, William L. Simon, 2003).

En otras palabras, la ingeniería social es el arte de lograr que los usuarios comprometan la seguridad de los sistemas de información. Así pues, dejan a un lado los ataques técnicos, con el propósito de dirigir a las personas para que otorguen acceso a información reservada. Además, son manipulados psicológicamente para que divulguen información sensible o incluso pueden realizar sus ataques a través de la influencia y persuasión Mouton, Leenen & Venter (Mouton et al., 2016).

Análisis de idoneidad de seguridad

En definitiva, la falta de conciencia de la sociedad se destaca como un desafío importante (Aldawood & Skinner, 2019). Al mismo tiempo, la ciberseguridad se considera un problema emergente y se está volviendo cada vez más relevante a la luz de las conocidas violaciones de datos de acuerdo con las principales tendencias a nivel ecuatoriano (Deloitte, 2018). De igual modo, los ataques cibernéticos a la infraestructura pública y privada local, como el fraude impulsado por el *phishing* en los servicios financieros y la piratería de sitios web del gobierno ecuatoriano (Catota et al., 2019).

Por otro lado, se analizan encuestas que se realizaron a diecisiete universidades y escuelas politécnicas en las tres ciudades más grandes y una ciudad mediana en Ecuador. Considerando que los encuestados evaluaron intuitivamente la idoneidad de la seguridad en función de la efectividad percibida de los métodos de autenticación utilizados en los servicios financieros en línea. Debido a las mejoras implementadas por instituciones más sólidas en esta área, que incluyen factores como: biometría, contraseña de tiempo limitado, contraseña de un solo uso, comunicación fuera de banda, verificación de SMS y correo electrónico y autenticación, 6 encuestados evalúan la seguridad de sus bancos que es ligeramente inapropiado (18%), ligeramente apropiado (36%), apropiado (39%) o absolutamente apropiado (7%) (Catota et al., 2019).

Taxonomía de clasificación de ataques de ingeniería social

Krombholz y colaboradores (2015) desarrollaron una taxonomía que resume la clasificación de los escenarios de ataque. Presentan tres categorías principales: tipos, operador y canal. En los tipos están: ataque físico, consiste en acceder las instalaciones como oficinas y robar información de la víctima; ataque social, es aquel que manipula a la persona mediante engaños para obtener su confianza y obtener lo deseado; ataques técnicos, se ejecutan a nivel de ambientes web con la finalidad de capturar credenciales de los usuarios generalmente en sitios sociales; ataques socio-técnicos, son una combinación de los ataques descritos anteriormente y se consideran exitosos, explotan la curiosidad de las personas para instalar software malicioso e ingresar a un sistema o red de ordenadores (Krombholz et al., 2015).

Krombholz y sus colegas (2015) describen que los operadores de ataques pueden ser máquinas o humanos, así mismo los canales de ataque son el correo electrónico es el más común para atacar con *phishing*, mensajería instantánea para robo de identidad y crear relaciones confiables, teléfono voz sobre IP para obtener información sensible, redes sociales que facilitan el robo de identidad para recopilar información, además de servicios en la nube se pueden utilizar para conocer la situación del objetivo y los sitios web son los más utilizados para ejecutar inyección de código además de combinar con la suplantación de identidad para falsificar páginas web (ver Figura 1).

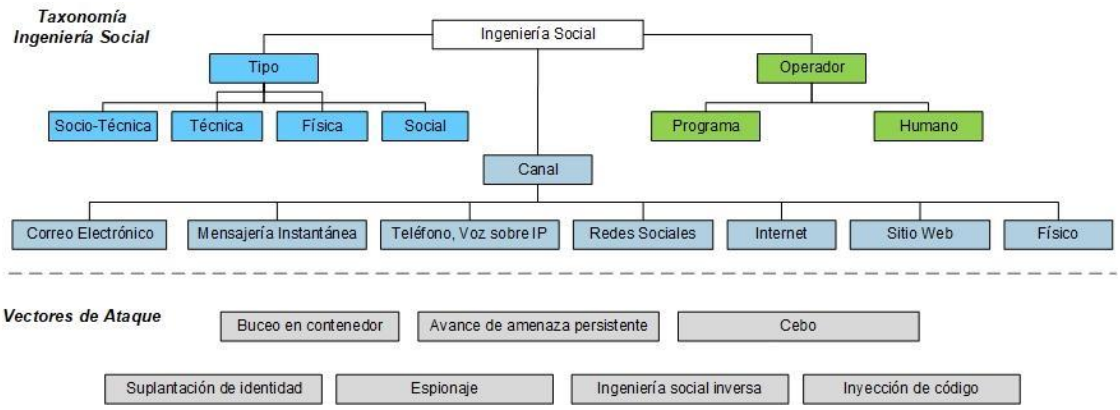


Figura 1. *Taxonomía de clasificación de ataques de ingeniería social.*
Fuente: Adaptado de (Krombholz et al., 2015)**.**

Principios Psicológicos

Curtis y colaboradores (2018), describen a la triada oscura como la agrupación de tres rasgos de personalidad, conformada por el maquiavelismo, el narcisismo y la psicopatía (Curtis et al., 2018). El maquiavelismo es un comportamiento manipulador dirigido a maximizar la obtención de la confianza personal, a través del engaño estratégico y tácticas morales flexibles. El narcisismo está asociado con el dominio interpersonal, es decir la falsa percepción de personas populares, atractivas y agradables con la finalidad de explotar a otros. La psicopatía se asocia con la ausencia de empatía, tendencias hacia la impulsividad, la agresión y el engaño. Los tres rasgos de personalidad son utilizados por los atacantes generalmente utilizando como vector de ataque el *phishing;* así mismo los usuarios finales o víctimas administran sus correos electrónicos con los rasgos antes descritos.

Curtis y sus colegas (2018) demuestran que la aplicación de la triada oscura, aplicada por los ingenieros sociales, son las técnicas de manipulación en línea; el maquiavelismo se relaciona con el esfuerzo, precaución y planificación para redactar mensajes de correos electrónicos *phishing*. Por otro lado, el narcisismo y la psicopatía se relacionan con la impulsividad del atacante; es decir, si cuentan con la experiencia suficiente no invierten demasiado tiempo en diseñar un correo de suplantación de identidad. En cuanto al comportamiento de los usuarios se analiza en las técnicas defensivas (Curtis et al., 2018).

Al mismo tiempo cabe señalar que la persuasión en el ámbito de IS es el proceso de lograr que alguien quiera reaccionar, pensar, actuar o creer del modo en que usted quiere que lo haga. Hay que mencionar, además que la influencia y la persuasión auténtica es elegante, sutil y casi siempre indetectable para quienes están siendo influenciados (Mózo, 2017). Además, existen seis principios de persuasión para aumentar la probabilidad de éxito y está formada por la reciprocidad, conformidad, gusto, escasez, compromiso y autoridad. La reciprocidad se refiere a dar algo a cambio, el objetivo se siente en deuda con el solicitante ya sea por hacer un mínimo movimiento. La conformidad, es imitar el comportamiento de otras personas. Las personas tienden a gustar a otros que son similares en términos de intereses, actitudes y creencias. La escasez ocurre cuando un producto, servicio o información tiene una disponibilidad limitada. El compromiso se refiere a la probabilidad de apegarse a una causa o idea después de hacer una promesa o acuerdo (Bull et al., 2015). La autoridad es el principio que describe

la tendencia de las personas a obedecer la solicitud de figuras autorizadas. Si las personas no pueden tomar una decisión bien informada, la responsabilidad de hacerlo se transfiere a la persona que cree que está a cargo. La crisis y el estrés activan el rasgo de comportamiento de la transición de la responsabilidad (Basri et al., 2018).

Técnicas defensivas

En el campo de la seguridad de la información a menudo se afirma que el eslabón más débil es el ser humano. Sin embargo, al involucrar a estos usuarios débiles, en la detección de ataques semánticos de IS como sensores de seguridad humana previo un entrenamiento de detección de engaño, e incursionar en el corazón de una plataforma técnica de defensa se convierten en uno de los vínculos más fuertes para detectar amenazas. Por consiguiente, si un solo usuario detecta correctamente un ataque y puede comunicar internamente, entonces la organización ha detectado con éxito el ataque (Heartfield & Loukas, 2018).

Metodología

El análisis de esta investigación se fundamenta en mapear la estructura intelectual que se enfoca específicamente en: contramedidas eficientes, taxonomías y vectores de ataque de Ingeniería Social, comprendido entre el año 2003 al 2019. Así pues, el alcance de esta investigación sigue la metodología de Kitchenham & Charters (2007) que se rige en revisiones de investigación y está compuesta de la siguiente manera:

- Definir los objetivos de investigación.
- Definir las preguntas de investigación.
- Determinar las técnicas o estrategias de búsqueda con base en las preguntas de investigación, identificar las bases de datos científicas y/o motores de búsqueda que se van a utilizar.
- Establecer el procedimiento de selección de estudios en el que se aplican los criterios de inclusión y exclusión.
- Definir el proceso de recopilación de datos y aplicar criterios de selección.
- Evaluar la calidad de los estudios mediante los resultados más sobresalientes para el análisis de resultados.
- Análisis del acoplamiento bibliográfico.

Además, es importante recalcar que se analizaron estudios científicos de expertos en ataques de ingeniería social, contramedidas, marcos de trabajo, experimentos y técnicas defensivas con la finalidad de educar al usuario en sus actividades rutinarias que involucran el uso directo e indirecto de TI dentro y fuera de una organización (Kitchenham & Charters, 2007).

Preguntas de Investigación

Para identificar el análisis de la investigación del mapeo de la estructura intelectual de la ingeniería social, planteamos las siguientes preguntas:

a) ¿Cuáles son los temas estudiados de la IS en las organizaciones que basan su funcionamiento en TI?
b) ¿Cuál es la cronología de producción de las publicaciones?
c) ¿Cuáles son las teorías más utilizadas en la IS?

Proceso de Búsqueda

En la estrategia de búsqueda se consideró recursos que incluyen palabras claves, frases o conceptos relacionados con las preguntas de investigación. Además, se utiliza la plataforma *Web of Science* basada en tecnología Web que recoge las referencias de las principales publicaciones científicas de cualquier disciplina del conocimiento, tanto científico como tecnológico, humanístico y sociológicos para el desarrollo de estudios de estructura intelectual (FECYT, 2001). Se exportaron los resultados con el registro completo y referencias citadas en formato *BibTex*; esta búsqueda se muestra en el Anexo A Tabla 1. En efecto la investigación se limitó estrictamente sólo a las áreas de estudio de ciencias de la computación, telecomunicaciones e ingeniería dado a la gran cantidad de artículos obtenidos.

Criterios de inclusión y exclusión

Criterios de Inclusión

Consideramos solo artículos de investigación en un rango que comprende desde el año 2004 a 2019 donde se evidencia términos relevantes sobre esta temática, además de estudios que incluyan variables o términos relativos a las preguntas de investigación y al resumen, además, artículos no publicados para evitar el sesgo de publicación (Manterola & Otzen, 2015).

Criterios de Exclusión

Se excluyen los estudios que no tienen relación alguna con el objetivo de esta revisión de ingeniería social y seguridad de la información, así mismo no se incluyen tesis doctorales, libros, capítulos de libros, ni trabajos conceptuales, teóricos o secundarios (Pluas & Jazm, 2020a), además de estudios que estén fuera del rango seleccionado entre los años 2004 al 2019 y estudios no indexados a *Web of Science*.

Proceso de recopilación de datos

En el proceso de selección de estudios de análisis de mapas científicos utilizamos el software de (Aria & Cuccurullo, 2017) ya que trabaja y se fundamenta en el entorno de desarrollo R donde se puede escalar con otros paquetes de estadísticas y técnicas de ciencia de datos para personalizar los resultados. (Liu, 2013)

Ahora bien, con la bibliografía registrada, se manejó un archivo en Excel con opciones relevantes y se utilizó Mendeley para almacenar y administrar las citas de los estudios. Luego se archivó los datos bibliográficos entregados por *bibliometrix* y se adicionaron pestañas para los factores demográficos y metodológicos, como constructos, conclusiones, limitaciones y futuras investigaciones (Pluas & Jazm, 2020b).

Así mismo, para el análisis de co-citación, se examinó 35 artículos (nodos) ya que, con 30 nodos, el número de grupos es el mismo (ver Figura 2). Luego de analizar los 35 artículos, no se incluye en el análisis final veinticinco artículos debido a que dos artículos están relacionados con revisiones sistemáticas y veintitrés corresponden a tesis doctorales, libros y capítulos de libros (ver Anexo B: Tabla 2). En efecto se asume como resultado, 10 artículos de los cuales 4 pertenecen al grupo 1 y 6 al grupo 2 (ver Anexo B: Tabla 3).

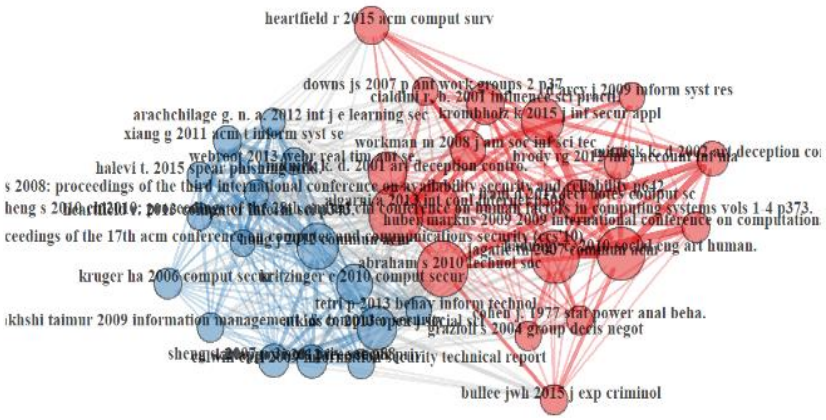


Figura 2. *Red de co-citación.*
Fuente: propia de autores

En definitiva, para el análisis de acoplamiento bibliográfico, se examinan 30 nodos porque, con 35 nodos los resultados se dispersan, el número de conglomerados están por fuera del rango (ver Figura 3). Luego de analizar los 31 artículos, no incluimos en el análisis final seis artículos; cuatro estaban relacionados con revisiones sistemáticas (ver Anexo C: Tabla 4) y dos se incluyen en los últimos clústeres con un solo nodo, teniendo como resultado, 25 artículos de los cuales nueve pertenecen al grupo 1 y dieciséis al grupo 2 (ver Anexo C: Tabla 5).

Figura 3. *Red de acoplamiento.*
Fuente: propia de autores.

Análisis de resultados

Ahora bien, los artículos de co-citación están relacionados principalmente con capacitación de concientización sobre métodos defensivos, marcos o mecanismos de trabajos para la concientización y prevención de ataques de IS y actividades de comportamiento humano. Además, las revistas más productivas son *Communications of the Acm* con dos publicaciones al igual que *Computers & Security*. En cambio, *Journal of Information Security and Applications, Journal of Experimental Criminology, IEEE Security & Privacy y Behaviour & Information Technology* cuentan con una sola publicación.

Según el análisis los clústeres 1 y 2 se iniciaron en el 2004 con el trabajo de Grazioli (2004) y concluyeron en el 2015 con los trabajos de Bullee, Montoya, Pieters, Hartel (2015) y Krombholz (2015). En los años 2012 y 2015 se consideran los más productivos ya que tuvieron cuatro trabajos (ver Anexo C: Figura A1).

Por un lado, Estados Unidos es el área donde se desarrollaron la mayoría de los estudios (4/10). Además, Australia e Inglaterra produjeron dos estudios cada uno. No existe una tendencia clara en el tipo de industria ya que seis artículos basan su trabajo en organizaciones privadas y al menos tres empresas fueron la muestra de los modelos, el resto de los estudios basó su fundamento en universidades.

Así pues, el enfoque estadístico utilizado en este grupo es cuantitativo. La técnica estadística utilizada con mayor frecuencia es el chi-cuadrado con tres estudios (3/10), de igual forma varianza utilizó dos estudios (2/10), como también un estudio aplicó la correlación de datos (1/10). Los modelos teóricos aplicaron teorías como Psicología Social (3/10), Conciencia Electrónica (1/10) e Ingeniería Social (1/10) las cuales fueron los más utilizados (ver Anexo C: Figura A2).

Una concientización más profunda en la educación actual de los usuarios, ya que ésta se ignora debido a que se enfocan en indicadores que los usuarios no comprenden. Además, la literatura de IS se encuentra dispersa y no contiene conceptos analíticos, estos son aspectos relevantes que se consideran principales limitaciones descritas por los autores de esta sección (ver Anexo C: Figura A3).

Para investigaciones futuras los autores de los artículos recomiendan que los estudios se concentren principalmente en la capacitación al usuario y en sus evaluaciones de campañas educativas implementadas a largo plazo. Además, se debe poner énfasis en la efectividad de las intervenciones de IS, como también en las políticas de seguridad, la toma de conciencia de riesgos potenciales en línea y al establecimiento de marcos, modelos y algoritmos de aprendizaje donde conduzcan a nuevas mejoras (ver Anexo C: Figura A4).

Mientras tanto, en el grupo de acoplamiento bibliográfico (*coupling*) se analiza métodos que se enfocan principalmente en mecanismos de trabajo para la concientización y prevención de ataques de IS (16/25), capacitación de concientización sobre métodos defensivos (5/25) y actividades de comportamiento humano (4/25). Además, la revista más influyente es *Computers & Security* con seis publicaciones seguida por la Revista *Computers in Human Behavior* con dos publicaciones. El resto de las revistas: *Saiee África Research, Information & Management, Science and Engineering Research Support Society, Journal of Investigative Psychology, IEEE Access, Information and Computer Security and Journal of Experimental Criminology* produjeron un artículo cada una.

Los trabajos de investigación de los clústeres 1 y 2 se iniciaron en el 2013 con la obra de *Ivaturi* y *Janczewski* (2014) concluyendo en el 2019 con las publicaciones de *Tsakalidis* y sus colegas (2019a) y *Mao* (2019). El artículo fundamental de *Ivaturi* (2014), es donde se formó la base de conocimientos. El trabajo, establece que en el campo de la IS las organizaciones deben obtener primordialmente tres componentes principales como parte de sus políticas de seguridad: concienciación, capacitación y educación.

Además, los responsables de las políticas deben conocer los diferentes escenarios de ataque e incluirlos como parte de los esfuerzos de concienciación de seguridad (Ivaturi & Janczewski, 2014). En cuanto a la tasa de publicación, el año 2018 es el más productivo con doce artículos (ver Anexo C: Figura A5).

Los resultados del grupo 2 son similares al grupo 1 en cuanto a factores demográficos y tipo de industria. Inglaterra cubrió la mayoría de los estudios (7/25) seguido de EE. UU. (3/25), Sudáfrica (2/25), Países Bajos

(2/25), China (2/25) y los otros países: Portugal, Grecia, Nueva Zelanda, Israel, Alemania, Escocia, Australia, Austria y Malasia tuvieron una obra. No existe una tendencia clara en el tipo de industria ya que la mayoría de los artículos basan su trabajo en organizaciones privadas. El resto de los estudios basó su fundamento en universidades.

El enfoque estadístico implementado fue cuantitativo (12/25). Las técnicas cuantitativas incluyen, varianza (4/12), regresión logística (3/12), Chi2 (3/12) y prueba de hipótesis (2/12). La Ingeniería Social (10/25) y la Psicología Social (4/25) fueron las teorías más aplicadas en los estudios (4/25), y el resto de los modelos fueron tomadas teorías de otras disciplinas (ver Anexo C: Figura A6).

Las principales limitaciones descritas por los autores de esta sección están relacionadas con tamaño de la muestra y empírico no validado, la falta de estudios en industrias específicas es notable (ver Anexo A: Figura A7).

Para investigaciones futuras los autores de los artículos recomiendan que los estudios se concentren principalmente en comprobaciones de aplicabilidad, acoplamientos de tecnologías, comportamiento humano como otros aspectos representados en la Figura A8 (Anexo C).

Análisis de acoplamiento bibliográfico

La capacitación de concientización sobre métodos defensivos es la base principal en el grupo 1 con 5 artículos. Luego le sigue Krombholz y sus colegas (2015), Kritzinger & Von Solms (2010), Kruger & Kearney (2006), Xiang (2011), que estudian los mecanismos de trabajo para la concientización y prevención de ataques de IS y Tetri & Vuorinen (2013) estudia el control social. Así, podemos afirmar que este clúster estudia comportamientos positivos como capacitación de concientización sobre métodos defensivos.

Con respecto a la producción de revistas, *Computer & Security* es más productiva con nueve artículos. Además, *Communications of the Acm*, *Computers in Human Behavior* publicaron dos artículos cada uno. En cambio, el resto de revistas como: *Journal of Strategic Information Systems, Information Systems Research, Information Systems Management, Information Resource Management Journal, IEEE Transactions of Professional Communications, Decision Science y Computer in Human Behavior* publicaron un estudio.

En cuanto a la producción científica se inició en 2004, con el trabajo de Grazioli (2004) terminando en 2019 con el trabajo de Tsakalidis & Vertidas, (2019a) y Mao (2019). Mientras que en el año de 2018 se dio la máxima producción científica de doce artículos (ver Anexo C: Figura B1).

Ahora bien, según análisis todos los estudios utilizaron IS y 18/35 de ellos basaron sus modelos en mecanismos de trabajo para la concientización y prevención de ataques de IS y 12/35 utilizaron capacitación de concientización sobre métodos defensivos. Con respecto a factores demográficos, Inglaterra concentró la mayor parte de los estudios con 8 artículos, seguida de Estados Unidos con 7 artículos. Países Bajos y Sudáfrica contribuyeron con tres artículos cada uno. Australia, China y Austria produjeron dos obras cada uno y Alemania, Malasia, Israel, Finlandia, Escocia, Portugal, Grecia y Nueva Zelanda contribuyeron con un artículo cada uno.

Por lo que se refiere a la tendencia, no se tiene una perspectiva clara en el tipo de industria. Veinte y tres estudios pertenecen a diversos tipos de negocios, nueve a universidades, uno a minería, salud y banca.

Las técnicas cuantitativas son el enfoque estadístico dominante con 20 artículos. Al igual que en el análisis de técnica estadística, varianza y chi-cuadrado es la técnica más popular con 6 artículos cada una. En un nivel menor, regresión logística contribuyó con tres trabajos, prueba de hipótesis con dos trabajos y correlación de datos con un solo artículo. Los estudios basan sus modelos en una variedad de 35 teorías (ver Anexo C: Figura B2). Las teorías más populares son Ingeniería Social (11/35), Psicología (7/35) y Taxonomía de ataques (2/35). De acuerdo con la figura B3 (Anexo C) las limitaciones más relevantes son el tamaño de la muestra (7/35), validación del diseño (6/35), comportamiento humano de seguridad (5/35) y sesgo de respuesta (4/35). En cuanto a las investigaciones futuras, los resultados están alineados de acuerdo con el análisis de co-citación y de acoplamiento (*coupling*). Así pues, las determinantes se despliegan en este sentido, desarrollar una comprobación de aplicabilidad (9/35), capacitación de concientización sobre métodos defensivos (6/35) y comportamiento humano (6/35) son los temas más relevantes (ver Anexo C: Figura B4). En contraste con los hallazgos del análisis de co-citación, pocos artículos examinaron factores organizacionales (2/10). Sin embargo, los factores individuales (8/10) fueron los más estudiados.

Discusión

Con respecto a la producción de revistas, *Computer & Security*, extendió su número de publicaciones. En cambio, ocurrió lo contrario con las revistas *Communications of the Acm* y *Computers in Human Behavior*, que en un inicio eran las revistas más productivas, pero actualmente no cuentan con publicaciones presentes.

En cuanto a la base intelectual que dio inicio en el año 2004 y finalizó en el año 2015. Por el contrario, el frente de investigación comenzó en 2013 y finalizó en 2019. Se deduce que existe una variación en la tasa de publicación en los indicadores, el primero publica máximo dos artículos por año y el segundo un promedio de tres a cuatro artículos por año.

Ahora bien, en cuanto al tema estudiado, la mayoría de las investigaciones trataron conductas positivas, pero la base de conocimientos trató conductas positivas y negativas por igual. Los factores individuales son los más estudiados, pero existe una pequeña proporción de factores organizativos. Se da una tendencia mayoritaria en las investigaciones para los comportamientos positivos en aplicar mecanismos de trabajo para la concientización y prevención de ataques de IS y también en la capacitación de concientización sobre métodos defensivos. La tendencia para el comportamiento negativo es la actividad del comportamiento humano. Al principio, la mayoría de los estudios se llevaron a cabo en Estados Unidos, Inglaterra y Países Bajos. En la actualidad, Inglaterra es el país con más estudios; pocos se llevan a cabo en Finlandia, Alemania, Australia, y Sudáfrica. Mientras tanto, se llevaron a cabo nuevos estudios en Grecia, China, Austria, Israel y Nueva Zelanda.

Tanto la base de conocimiento como el frente de investigación, no tiene una tendencia clara en el tipo de industria a tratar. La mayoría de los estudios se basó en negocios diversos ya que las organizaciones no están dispuestas a participar en la investigación por temor reputacional por lo que generaría resultados negativos que pueden afectar su desempeño.

Con respecto a los modelos teóricos los estudios se basan en encuestas para probar sus modelos, implementando técnicas cuantitativas, como varianza y chi cuadrado en la mayoría de sus estudios y regresión logística en pocas situaciones.

No obstante, los modelos teóricos manejan diversas teorías como la seguridad de la información, conciencia electrónica, IoT (internet de las cosas), inteligencia del código abierto y heurísticas. Pero para el conocimiento básico, existe una principal tendencia a utilizar métodos como la IS y Psicología Social para predecir comportamientos positivos y negativos. Por lo tanto, la mayoría de los artículos se centran en comportamientos positivos aplicando IS y Psicología Social como las teorías más relevantes. Sin embargo, la conciencia electrónica e inteligencia de código abierto son otras teorías prevalentes que se utilizan para medir comportamientos positivos (Bitton et al., 2018).

Los estudios actuales utilizan IS porque exploran incidentes en los que se penetra en un sistema de información mediante el uso de métodos sociales. En definitiva, la base de conocimiento y el frente de investigación coinciden en que existe la necesidad de estudiar el tamaño de la muestra propuesta como principal limitación. Por ejemplo, el tamaño del conjunto de datos y el número de muestras de pruebas empleadas para obtener la precisión y la solidez de las soluciones están muy influenciadas y delimitadas, mientras más muestras se realicen se promoverán mejores resultados.

Otra limitación estándar es la validación del diseño. En la actualidad existen modelos de IS empíricos que no se han probado en un ambiente real. Es necesario realizar ensayos de eficiencia de los métodos propuestos en ambientes de producción (Tsakalidis et al., 2019b).

Así pues, la comprobación de aplicabilidad, la capacitación de concientización sobre métodos defensivos, el comportamiento humano, el acoplamiento de tecnologías y estudios de laboratorio, son determinantes que necesitan investigación futura. La base intelectual y el frente de investigación concuerdan con las principales determinantes de los estudios que se examinarán como investigaciones futuras.

Conclusiones

La protección de la información es extremadamente importante en una sociedad moderna y aunque el nivel de seguridad en torno a la información se mejora continuamente, el único punto débil sigue siendo el ser humano que es susceptible a las técnicas de manipulación. Los ataques de IS como ya se mencionaron en esta investigación explotan negativamente los principios psicológicos de sus víctimas, siendo estos el maquiavelismo, el narcisismo y la psicopatía con el único propósito de influir directamente en la toma de decisiones inconscientes y con consecuencias de violaciones a la integridad, disponibilidad y confidencialidad de la información tanto en el ámbito organizacional y en el particular.

Este artículo presenta un mapeo de la estructura intelectual sobre la ingeniería social, donde se pretende identificar los enfoques que han recibido mayor atención por parte de los investigadores, además encontramos posibles explicaciones para las preguntas de investigación establecidas. Además, nuestra contribución al mapeo de la estructura intelectual de ingeniería social es amplia ya que implementamos la co-citación y el acoplamiento bibliográfico juntos.

En lo que respecta a las limitaciones de este estudio se dio en los artículos de investigación del grupo de co-citación debido a que la mayoría de los artículos fueron excluidos de acuerdo con el diseño de cómo estaban elaborados. Por lo tanto, la investigación no puede considerarse una tendencia nueva o en desarrollo. Además, otra limitación que se tiene en el estudio es la exclusión de bases de datos bibliográficas como *Scopus*.

Pero la Ingeniería Social pertenece al campo de investigación de Tecnologías de la Información y su crecimiento científico es vertiginoso por lo tanto *Web of Science* es la base de datos más adecuada para el análisis.

En definitiva, en investigaciones futuras se necesita realizar nuevamente un análisis de co-citación y compararlo con los resultados de nuestro trabajo para establecer cualquier variación ya que su conocimiento científico se incrementa con el tiempo.

Finalmente, el análisis de la literatura coincide en que la única manera de protegerse contra los ataques de IS es la de dotar de una cultura orientada a la seguridad de la información dentro de la organización mediante la capacitación y concienciación continua sobre métodos defensivos, es decir aplicar un bucle en la creación, aplicación, evaluación y mejora de un marco de trabajo para prevenir y mitigar los diferentes escenarios ataques de IS y que sirva como repositorio de información para el profesional de seguridad, el probador de penetración o el investigador entusiasta aprenda de los vectores de ataque más utilizados en el medio y tenga una capacidad de respuesta oportuna y eficiente.

Referencias

Airehrour, D. (2018). Social Engineering Attacks and Countermeasures in the New Zealand Banking System : Advancing a User-Reflective Mitigation Model. https://doi.org/10.3390/info9050110

Aldawood, H., & Skinner, G. (2019). Reviewing Cyber Security Social Engineering Training and Awareness Programs — Pitfalls and Ongoing Issues. https://doi.org/10.3390/fi11030073

Applegate, S. D. (2009). Social engineering: Hacking the wetware! Information Security Journal, 18(1), 40–46. https://doi.org/10.1080/19393550802623214

Aria, M., & Cuccurullo, C. (2017). bibliometrix: An R-tool for comprehensive science mapping analysis. Journal of Informetrics, 11(4), 959–975. https://doi.org/10.1016/j.joi.2017.08.007

Artículo de revista científica

Basri, W., Ismail, W., Yusof, M., & Science, I. (2018). Mitigation Strategies for Unintentional Insider Threats on Information Leaks. 12(1), 37–46.

Bitton, R., Finkelshtein, A., Sidi, L., Puzis, R., Rokach, L., & Shabtai, A. (2018). Taxonomy of mobile users' security awareness. Computers and Security, 73, 266–293. https://doi.org/10.1016/j.cose.2017.10.015

Bull, J. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. https://doi.org/10.1007/s11292-014-9222-7

Bullée, J. H., Montoya, L., Junger, M., & Hartel, P. (2017). On the anatomy of social engineering attacks — A literature-based dissection of successful attacks. October 2015, 1–26. https://doi.org/10.1002/jip.1482

Buyya, R., Shin, C., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25(6), 599–616. https://doi.org/10.1016/j.future.2008.12.001

Catota, F. E., Granger Morgan, M., & Sicker, D. C. (2018). Cybersecurity incident response capabilities in the Ecuadorian financial sector. Journal of Cybersecurity, 4(1), 1–20. https://doi.org/10.1093/cybsec/tyy002

Catota, F. E., Granger Morgan, M., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. Journal of Cybersecurity, 5(1), 1–19. https://doi.org/10.1093/cybsec/tyz001

Cotteleer, M., & Sniderman, B. (2017). Forces of change: Industry 4.0. Deloitte Insights, 1–20. https://doi.org/10.1007/s11947-009-0181-3

Curtis, S. R., Rajivan, P., Jones, D. N., & Gonzalez, C. (2018). Phishing attempts among the dark triad: Patterns of attack and vulnerability. In Computers in Human Behavior (Vol. 87). Elsevier Ltd. https://doi.org/10.1016/j.chb.2018.05.037

D, J. M. H. P. (2017). Social engineering in cybersecurity: the evolution of a concept. Computers & Security. https://doi.org/10.1016/j.cose.2017.10.008

Deloitte. (2018). Ciberseguridad Encuesta 2018 sobre tendencias de Cyber Riesgos y Seguridad de la Información Ecuador. https://www2.deloitte.com/content/dam/Deloitte/ec/Documents/risk/Deloitte 2018 Cyber Risk Information Security Study - Ecuador vF.pdf

El Telégrafo. (2016). En Ecuador, el 85% de los delitos informáticos ocurre por descuido del usuario. https://www.eltelegrafo.com.ec/noticias/judicial/1/en-ecuador-el-85-de-los-delitos-informaticos-ocurre-por-descuido-del-usuario

FECYT. (2001). Recursos Científicos. Recursos Científicos. https://www.fecyt.es/es/recurso/recursos-cientificos

Fiscalía General del Estado. (2015). Los delitos informáticos van desde el fraude hasta el espionaje. https://www.fiscalia.gob.ec/los-delitos-informaticos-van-desde-el-fraude-hasta-el-espionaje/

Grazioli, S. (2004). Where did they go wrong? An analysis of the failure of knowledgeable Internet consumers to detect deception over the internet. Group Decision and Negotiation, 13(2), 149–172. https://doi.org/10.1023/B:GRUP.0000021839.04093.5d

Heartfield, R., & Loukas, G. (2018). Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. Computers & Security. https://doi.org/10.1016/j.cose.2018.02.020

Hjørland, B. (2010). Letter to the Editor: Answer to Professor Szostak (concept theory). Journal of the American Society for Information Science & Technology, 61(5), 1078–1079. https://doi.org/10.1002/asi

Instituto Nacional de Estadística y Censos INEC. (2015). Resumen Ejecutivo. Módulo de Tecnologías de La Información y La Comunicación - TIC de Las Encuestas de Manufactura y Minería, Comercio Interno y Servicios 2015, 1–12.

Ivaturi, K., & Janczewski, L. (2014). Journal of Global Information Social Engineering Preparedness of Online Banks: An Asia-Pacific Perspective. December. https://doi.org/10.1080/1097198X.2013.10845647

Jagatic, B. T. N., Johnson, N. A., & Jakobsson, M. (2007). Social Phisihing. 50(10).

Kevin D. Mitnick, William L. Simon, S. W. (2003). THE ART OF DECEPTION: Controlling the human element of security (1st ed.). Wiley Publishing, Inc. https://doi.org/112147

Kitchenham, B., & Charters, S. (2007). Guidelines for performing Systematic Literature Reviews in SE. Guidelines for Performing Systematic Literature Reviews in SE, 1–44. https://userpages.uni-koblenz.de/%7B~%7Dlaemmel/esecourse/slides/slr.pdf

Kritzinger, E., & Von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. Computers and Security, 29(8), 840–847. https://doi.org/10.1016/j.cose.2010.08.001

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and Applications; Elsevier Ltd. https://doi.org/10.1016/j.jisa.2014.09.005

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. Computers and Security, 25(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008

Liu, X. (2013). Full-Text Citation Analysis: A New Method to Enhance. Journal of the American Society for Information Science and Technology, 64(July), 1852–1863. https://doi.org/10.1002/asi

Makridakis, A., Athanasopoulos, E., Antonatos, S., Antoniades, D., Ioannidis, S., & Markatos, E. P. (2010). Understanding the Behavior of Malicious Applications in Social Networks. October, 14–19.

Manterola, C., & Otzen, T. (2015). Bias in Clinical Research. International Journal of Morphology, 33(3), 1156–1164. https://doi.org/10.4067/S0717-95022015000300056

Mao, J. (2019). Phishing page detection via learning classifiers from page layout feature.

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social Engineering Attack Examples, Templates and Scenarios. Computers & Security. https://doi.org/10.1016/j.cose.2016.03.004

Mózo, B. S. (2017). Ingeniería Social el Arte del Haking Personal. In Journal of Chemical Information and Modeling (Vol. 53, Issue 9). https://doi.org/10.1017/CBO9781107415324.004

Noyce, R. N., & Hoff, M. E. (1981). A History of Microprocessor Development at Intel. IEEE Micro, 1(1), 8–21. https://doi.org/10.1109/MM.1981.290812

Pluas, N., & Jazm, G. (2020). MAESTRÍA EN AUDITORÍA DE TECNOLOGÍAS DE LA INFORMACIÓN.

Salahdine, F. (2019). Social Engineering Attacks: A Survey as. https://doi.org/10.3390/fi11040089

Sancho-Hirare, C. (2017). Ciberseguridad. Presentación del dossier. URVIO, Revista Latinoamericana de Estudios de Seguridad, 20, 8–15. https://scielo.conicyt.cl/pdf/eure/v31n93/art04.pdf

Servicio Ecuatoriano de Normalización INEN. (2017). Tecnologías de la Información y Comunicación Contenido. Norma Técnica Ecuatoriana. Tecnologías de La Información - Técnicas de Seguridad - Código de Práctica Para Los Controles de Seguridad de La Información (ISO/IEC 27002:2013 + Cor1.: 2014 + Cor.2: 2015, IDT) (2). Quito, Pichincha, Ecuador: Servicio Ecuatoria.

Tetri, P., & Vuorinen, J. (2013). Dissecting social engineering. Behaviour and Information Technology, 32(10), 1014–1023. https://doi.org/10.1080/0144929X.2013.763860

Tsakalidis, G., Vergidis, K., Petridou, S., & Vlachopoulou, M. (2019). A cybercrime incident architecture with adaptive response policy. Computers and Security, 83, 22–37. https://doi.org/10.1016/j.cose.2019.01.011

Xiang, G., Hong, J., Rose, C. P., & Cranor, L. (2011). CANTINA+: A feature-rich machine learning framework for detecting phishing web sites. ACM Transactions on Information and System Security, 14(2), 1–28. https://doi.org/10.1145/2019599.201960

ANEXO A: DESCRIPCIÓN GENERAL

Tabla 1
Ecuación de búsqueda en *Web of Science*

DESCRIPCIÓN
(AU= cialdini r. AND PY= b. AND SO= 2001 influence sci practi.) OR (AU= huber markus AND PY= 2009 AND SO= 2009 international conference on computational science and engineering (cse)) OR (AU= irani d AND PY= 2011 AND SO= lect notes comput sc) OR (AU= jagatic tn AND PY= 2007 AND SO= commun acm) OR (AU= mitnick k. AND PY= d AND SO= 2002 art deception contro.) OR (AU= abraham s AND PY= 2010 AND SO= technol soc) OR (AU= algarni a AND PY= 2013 AND SO= int conf internet p508) OR (AU= mitnick k. AND PY= d. AND SO= 2001 art deception contro.) OR (AU= sheng s AND PY= 2010 AND SO= chi2010: proceedings of the 28th annual chi conference on human factors incomputing systems vols 1-4 p373.) OR (AU= hadnagy c. AND PY= 2010 AND SO= social eng art human.) OR (AU= brody rg AND PY= 2012 AND SO= int j account inf ma) OR (AU= downs js AND PY= 2007 AND SO= p ant work groups 2 p37) OR (AU= heartfield r AND PY= 2015 AND SO= acm comput surv) OR (AU= workman m AND PY= 2008 AND SO= j am soc inf sci tec) OR (AU= krombholz k AND PY= 2015 AND SO= j inf secur appl) OR (AU= bullee jwh AND PY= 2015 AND SO= j exp criminol) OR (AU= cohen j. AND PY= 1977 AND SO= stat power anal beha.) OR (AU= grazioli s AND PY= 2004 AND SO= group decis negot) OR (AU= d'arcy j AND PY= 2009 AND SO= inform syst res) OR (AU= arachchilage g. AND PY= n. AND SO= a. 2012 int j e learning sec) OR (AU= atkins b. AND PY= 2013 AND SO= open j social sci) OR (AU= bakhshi taimur AND PY= 2009 AND SO= information management \& computer security) OR (AU= colwill carl AND PY= 2009 AND SO= information security technical report) OR (AU= halevi t. AND PY= 2015 AND SO= spear phishing wild.) OR (AU= heartfield r. AND PY= 2013 AND SO= computer inform sci p343.) OR (AU= hong j AND PY= 2012 AND SO= commun acm) OR (AU= kirlappos i AND PY= 2012 AND SO= ieee secur priv) OR (AU= kritzinger e AND PY= 2010 AND SO= comput secur) OR (AU= kruger ha AND PY= 2006 AND SO= comput secur) OR (AU= lu l AND PY= 2010 AND SO= proceedings of the 17th acm conference on computer and communications security (ccs'10)) OR (AU= madlmayr g AND PY= 2008 AND SO= ares 2008: proceedings of the third international conference on availability security and reliability p642) OR (AU= sheng s. AND PY= 2007 AND SO= p 3 s us priv sec p88) OR (AU= tetri p AND PY= 2013 AND SO= behav inform technol) OR (AU= webroot 2013 AND PY= webr AND SO= real tim ant se.) OR (AU= xiang g AND PY= 2011 AND SO= acm t inform syst se)

ANEXO B: CO-CITACIÓN

Tabla 2
Estudios no incluidos en el análisis

NÚMERO DE CLUSTER	NÚMERO DE PAPER	RAZÓN
1	1	Tesis doctoral
1	2	Tesis doctoral
1	3	Tesis doctoral
1	5	Capítulo de libro
1	6	Carta editorial
1	7	Carta editorial
1	8	Capítulo de libro
1	9	Tesis doctoral
1	10	Tesis doctoral
1	11	Tesis doctoral
1	12	Carta editorial
1	13	Carta editorial
1	14	Revisión
1	17	Capítulo de libro
2	19	Revisión
2	20	Capítulo de libro
2	21	Capítulo de libro
2	22	Tesis doctoral
2	23	Tesis doctoral
2	24	Tesis doctoral
2	25	Capítulo de libro
2	30	Capítulo de libro
2	31	Capítulo de libro
2	32	Carta editorial
2	34	Carta editorial

Tabla 3
Artículos de investigación incluidos en el análisis

ID	TÍTULO PAPER	CLUSTER	AÑO PUBLICADO	CITADO	REVISTA	No REF	PAIS REGIÓN	TIPO INVESTIGACIÓN
1	Social phishing (4)	1	2007	379	Communications of the ACM	11	Estados Unidos	Descriptiva
2	Advanced social engineering attacks (15)	1	2015	59	Journal of information security and applications	48	Australia	Exploratoria
3	The persuasion and security awareness experiment: reducing the success of social engineering attacks (16)	1	2015	18	Journal of experimental criminology	60	Países Bajos	Descriptiva
4	Where did they go wrong? An analysis of the failure of knowledgeable Internet consumers to detect deception over the Internet (18)	1	2004	45	Group decision and negotiation	49	Estados Unidos	Descriptiva
5	The State of Phishing Attacks (26)	2	2012	140	Communications of the ACM	39	Estados Unidos	Explicativa
6	Security Education against Phishing: A Modest Proposal for a Major Rethink (27)	2	2012	44	IEEE security & privacy	15	Inglaterra	Descriptiva
7	Cyber security for home users: A new way of protection through awareness enforcement (28)	2	2010	42	Computers & security	21	Inglaterra	Explicativa
8	A prototype for assessing information security awareness (29)	2	2006	99	Computers & security	24	Australia	Descriptiva
9	Dissecting social engineering (33)	2	2013	27	Behavior & information technology	34	Finlandia	Explicativa

ID	TÍTULO PAPER	CLUSTER	AÑO PUBLICADO	CITADO	REVISTA	No REF	PAIS REGIÓN	TIPO INVESTIGACIÓN
10	CANTINA+: A Feature-Rich Machine Learning Framework for Detecting Phishing Web Sites (35)	2	2011	167	ACM transactions on information and system security	26	Estados Unidos	Descriptiva

ANEXO C: ACOPLAMIENTO

Tabla 4
Estudios no incluidos en el análisis

NÚMERO DE CLUSTER	NÚMERO DE PAPER	RAZÓN
1	2	REVISIÓN
1	3	REVISIÓN
2	20	REVISIÓN
2	21	REVISIÓN
3	27	REVISIÓN CRÍTICA
4	19	REVISIÓN CRÍTICA

Tabla 5
Artículos de investigación incluidos en el análisis

ID	TÍTULO PAPER	CLUSTER	AÑO PUBLICADO	CITADO	REVISTA	No REF	PAIS REGIÓN	TIPO INVESTIGACIÓN
1	A cybercrime incident architecture with adaptive response policy	2	2019	2	Computers & security	64	Europa	Explicativa
2	Phishing page detection via learning classifiers from page layout feature	2	2019	5	Eurasip journal on wireless communications and networking	29	China	Descriptiva
3	Phishing attempts among the dark triad: Patterns of attack and vulnerability	2	2018	5	Computers in human behavior	42	Estados unidos	Descriptiva
4	A taxonomy of cyber-physical threats and impact in the smart home	2	2018	14	Computers & security	159	Inglaterra	Explicativa
5	Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework.	2	2018	8	Computers & security	57	Inglaterra	Descriptiva
6	Finite state machine for the social engineering attack detection model: SEADM	1	2018	1	SAIEE Africa research	25	Sudáfrica	Explicativa
7	Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model	2	2018	4	MDPI (multidisciplinary digital publishing institute)	32	Oceanía	Explicativa
8	Self-control, organizational context, and rational choice in Internet abuses at work	2	2018	9	Information & management	66	Estados Unidos	Descriptiva

ID	TÍTULO PAPER	CLUSTER	AÑO PUBLICADO	CITADO	REVISTA	No REF	PAIS REGIÓN	TIPO INVESTIGACIÓN
9	Social engineering in cybersecurity: The evolution of a concept	2	2018	18	Computers & security	147	Estados Unidos	Exploratoria
10	Taxonomy of mobile users' security awareness	2	2018	8	Computers & security	55	Israel	Explicativa
11	User characteristics that influence judgment of social engineering attacks in social networks	2	2018	12	Human-centric computing and information sciences	49	Reino Unido	Descriptiva
12	Mitigation Strategies for Unintentional Insider Threats on Information Leaks	2	2018	2	Science and engineering research support society	42	Asia	Exploratoria
13	RoFa: A Robust and Flexible Fine-Grained Access Control Scheme for Mobile Cloud and IoT based Medical Monitoring	1	2018	3	Fundamenta informaticae	31	China	Explicativa
14	On the anatomy of social engineering attacks, A literature-based dissection of successful attacks	1	2018	2	Journal of investigative psychology and offender profiling	69	Alemania	Descriptiva
15	An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook	2	2017	4	european journal of information systems	147	Australia	Descriptiva
16	Panning for gold: Automatically analyzing online social engineering attack surfaces	1	2017	2	Computers & security	32	Reino Unido	Descriptiva
17	Priming and warnings are not effective to prevent social engineering attacks	2	2017	24	Computers in human behavior	128	Países Bajos	Descriptiva

ID	TÍTULO PAPER	CLUSTER	AÑO PUBLICADO	CITADO	REVISTA	No REF	PAIS REGIÓN	TIPO INVESTIGACIÓN
18	Social engineering attack examples, templates and scenarios	1	2016	16	Computers & security	59	Sudáfrica	Explicativa
19	You Are Probably Not the Weakest Link: Towards Practical Prediction of Susceptibility to Semantic Social Engineering Attacks	2	2016	9	IEEE access	74	Inglaterra	Descriptiva
20	An information security risk-driven investment model for analyzing human factors	1	2016	4	Information and computer security	28	Reino Unido	Exploratoria
21	A Taxonomy of Attacks and a Survey of Defense Mechanisms for Semantic Social Engineering Attacks	2	2015	21	ACM computing surveys	185	Reino Unido	Exploratoria
22	Advanced social engineering attacks	1	2015	59	Journal of information security and applications	48	Austria	Exploratoria
23	The persuasion and security awareness experiment: reducing the success of social engineering attacks	1	2015	18	Journal of experimental criminology	60	Países Bajos	Descriptiva
24	Online Disclosure of Personally Identifiable Information with Strangers: Effects of Public and Private Sharing	1	2014	1	Interacting with computers	46	Portugal	Descriptiva
25	Social Engineering Preparedness of Online Banks: An Asia-Pacific Perspective	2	2013	3	Journal of global information technology management	58	Inglaterra	Exploratoria

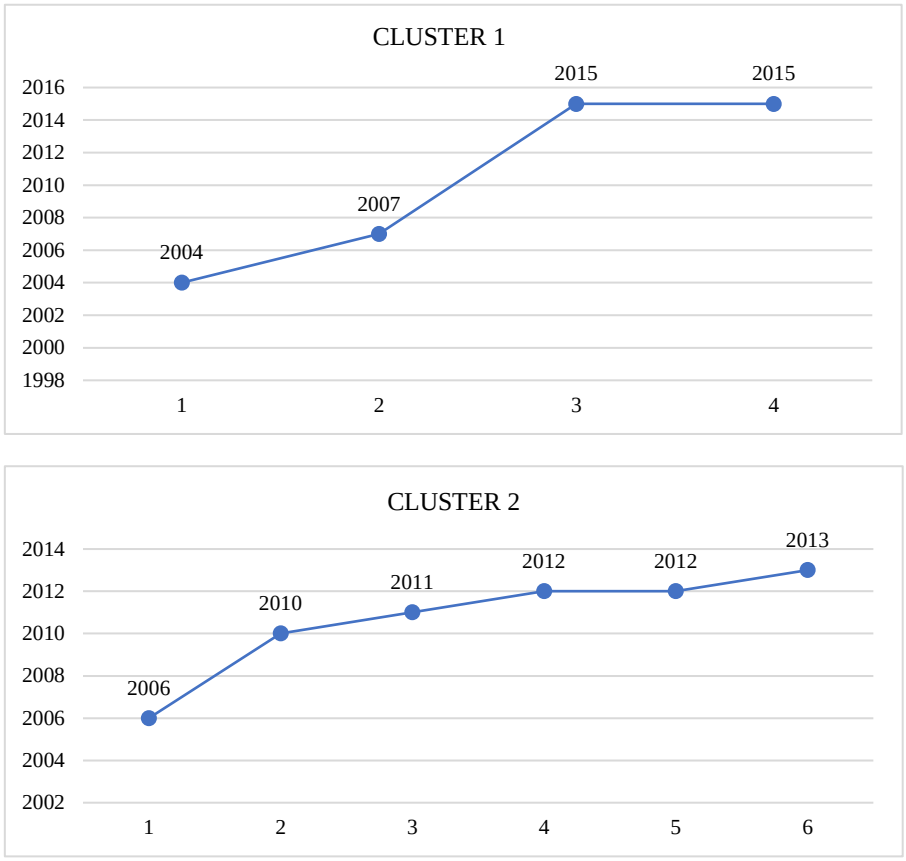


Figura A1. *Cantidad de artículos por año y clúster.*

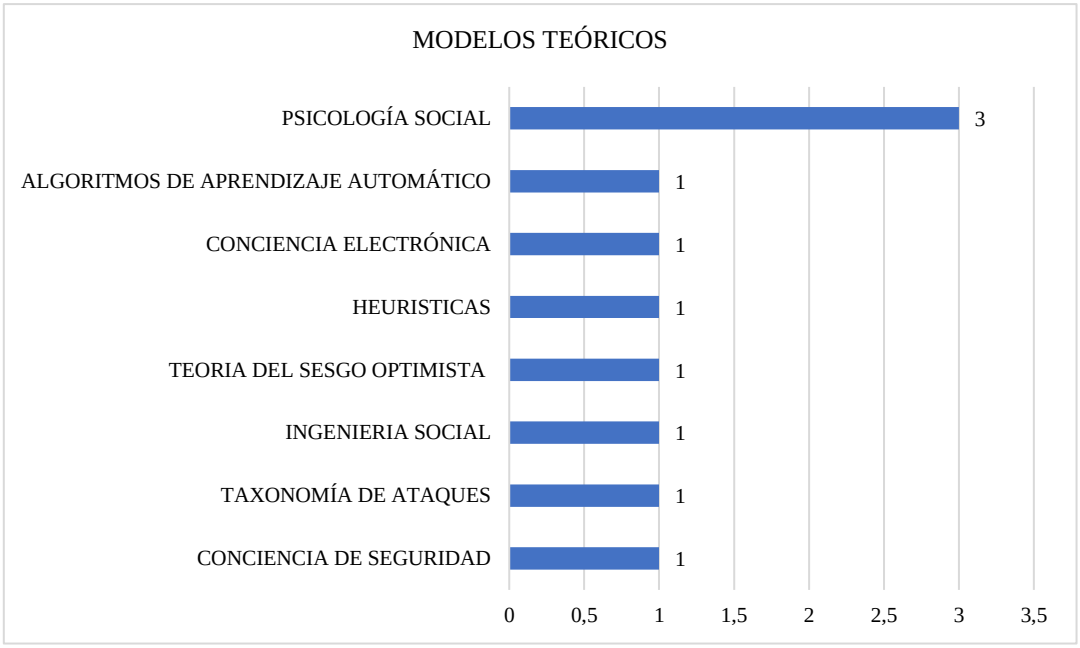


Figura A2. *Modelos teóricos aplicados en los estudios de investigación.*

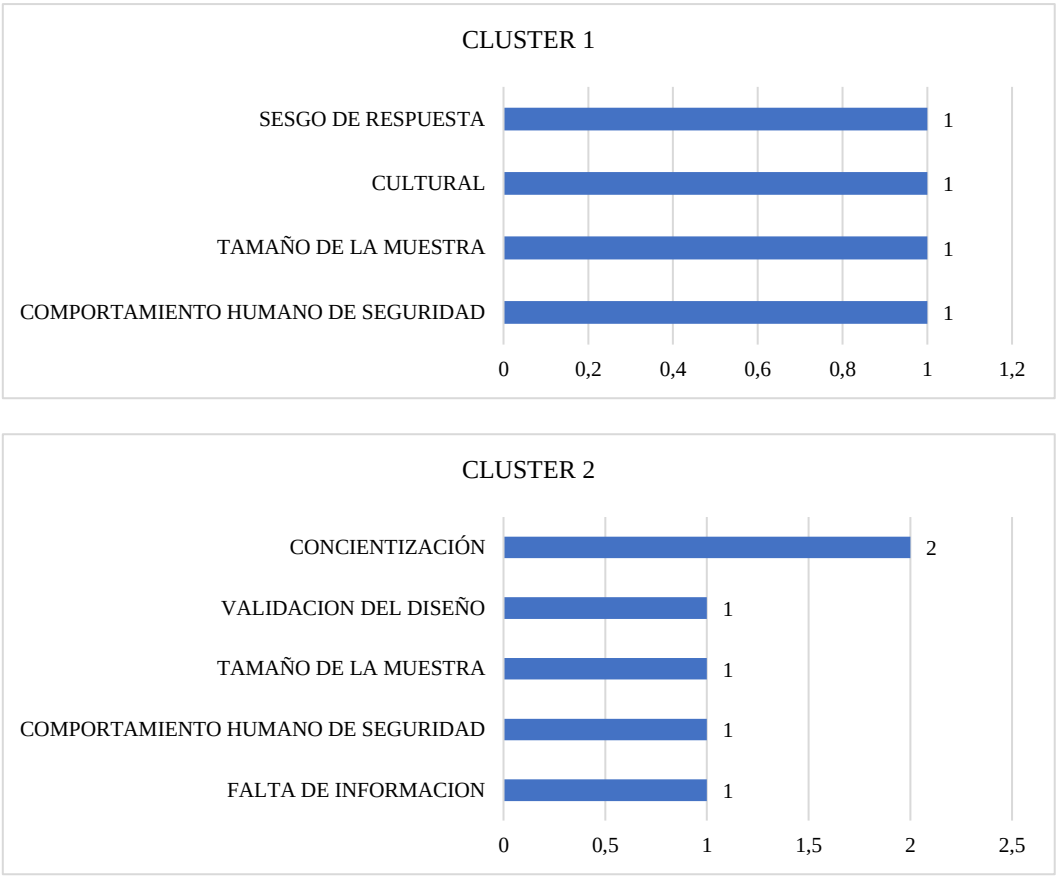


Figura A3. *Limitaciones en los estudios de investigación por clúster.*

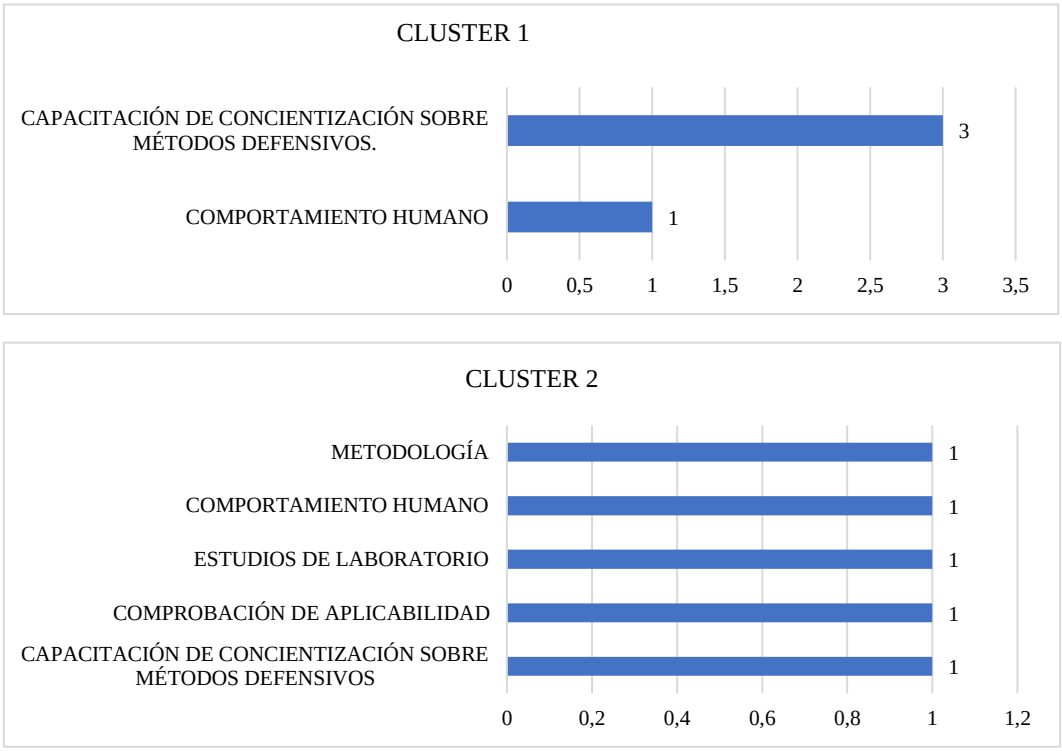


Figura A4. *Futuras investigaciones por clúster.*

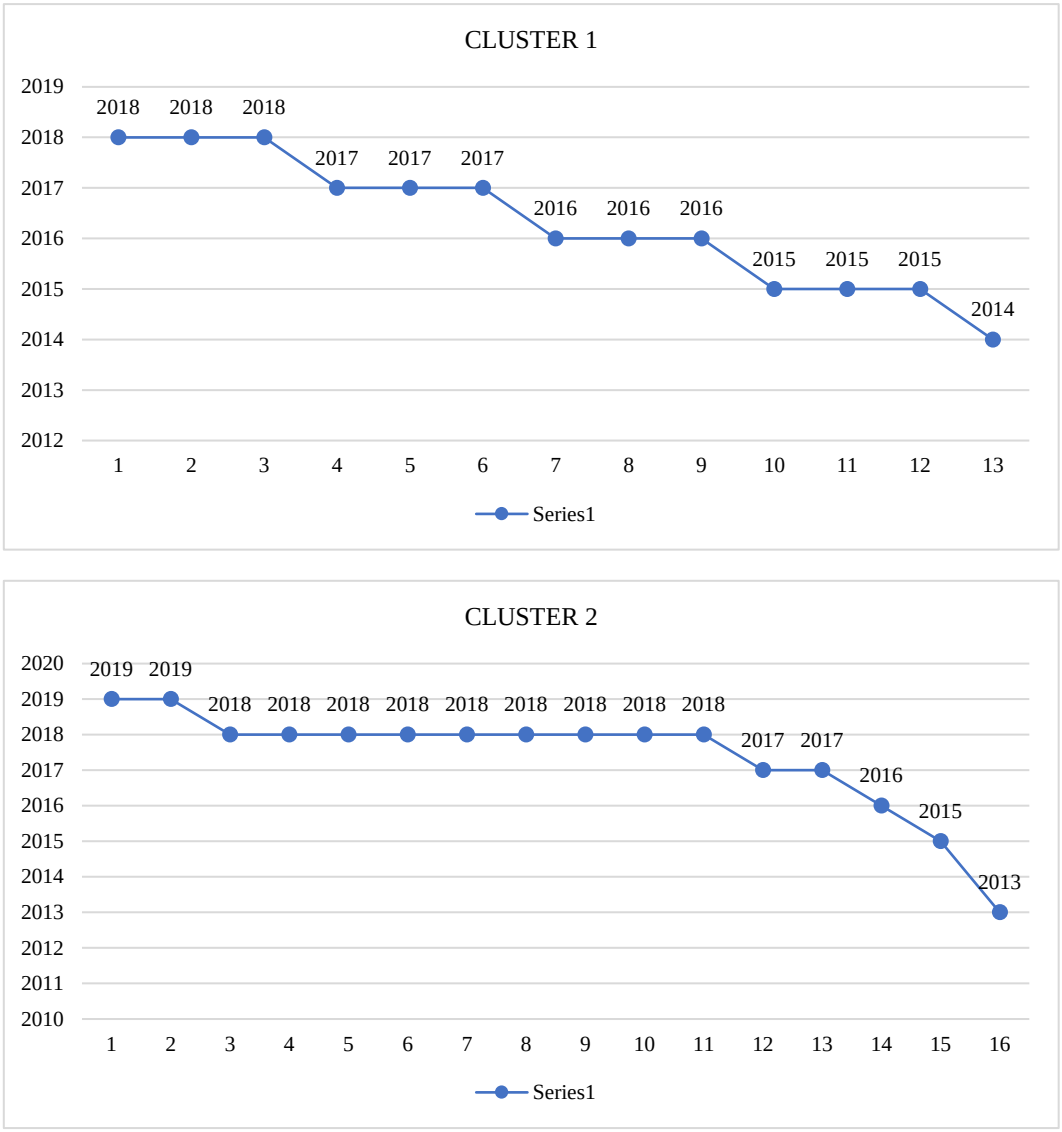


Figura A5. *Cantidad de artículos por año y clúster.*

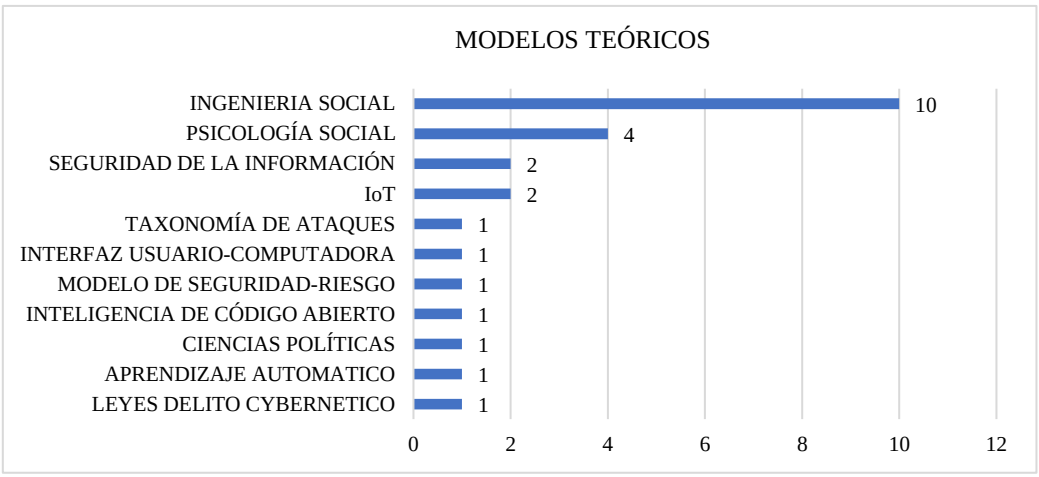
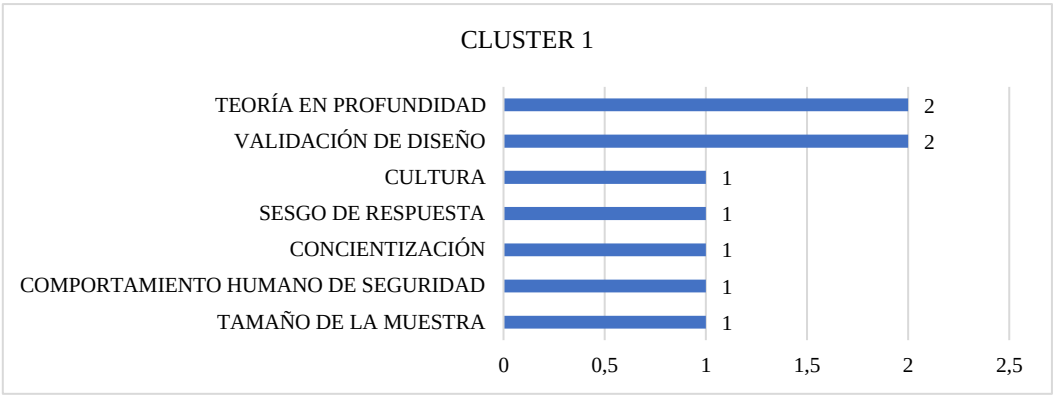


Figura A6. *Teorías aplicadas en los estudios de investigación.*



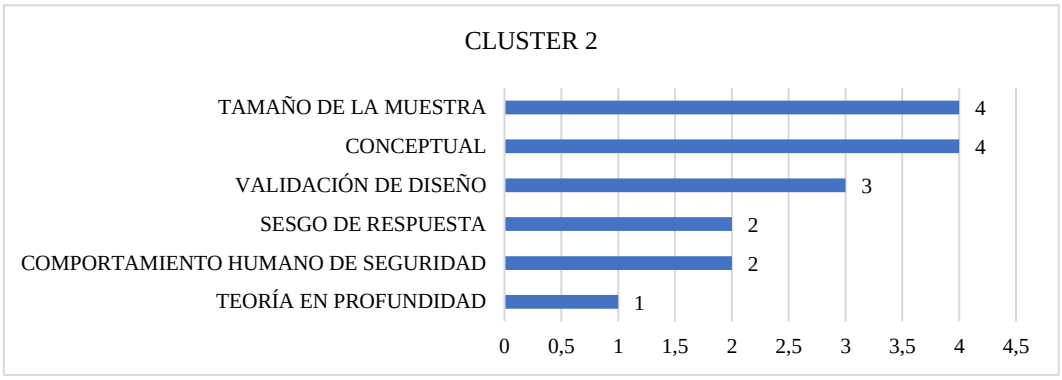
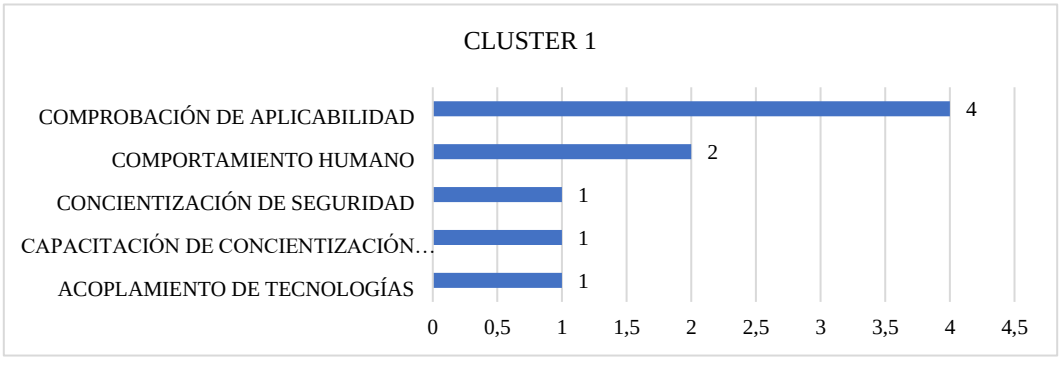


Figura A7. *Limitaciones por clúster*.



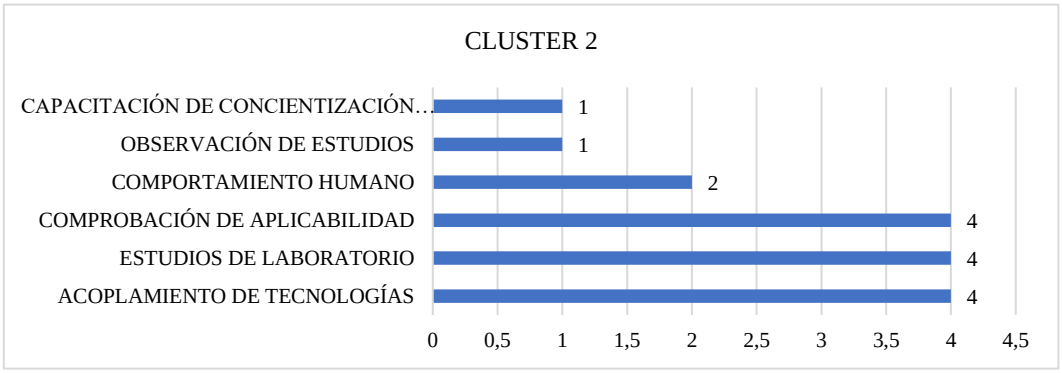


Figura A8. *Futuras investigaciones por clúster.*

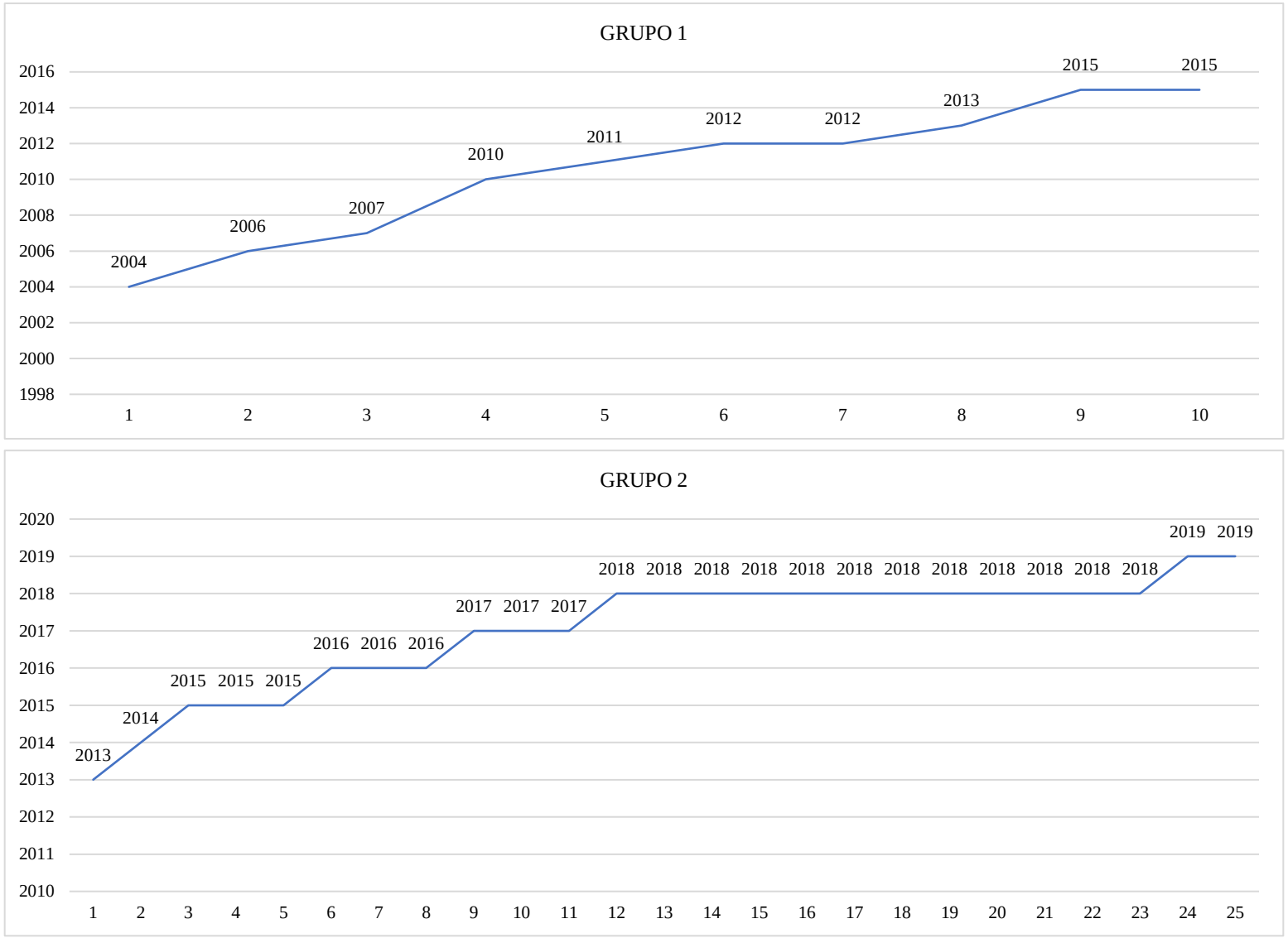


Figura B1. *Cantidad total de investigaciones por año.*

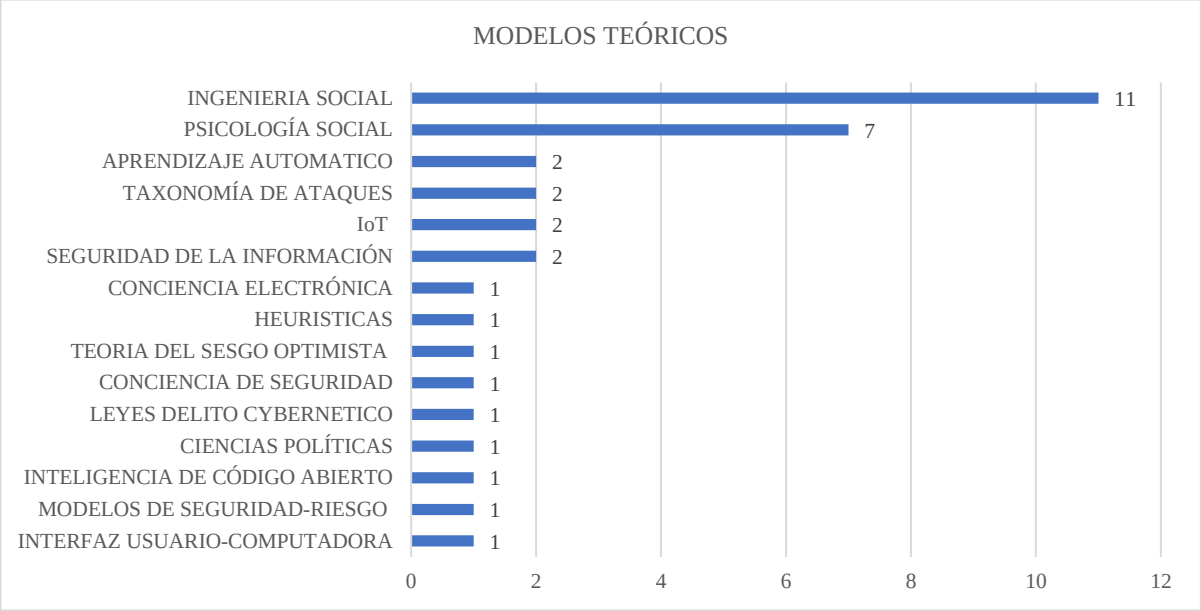


Figura B2. *Cantidad de modelos teóricos.*

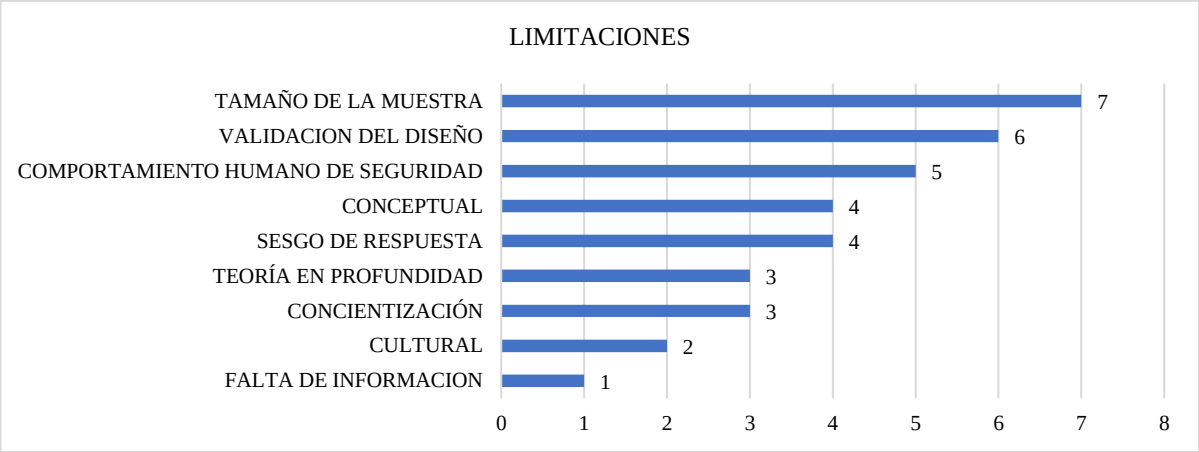


Figura B3. *Cantidad de análisis de limitaciones.*

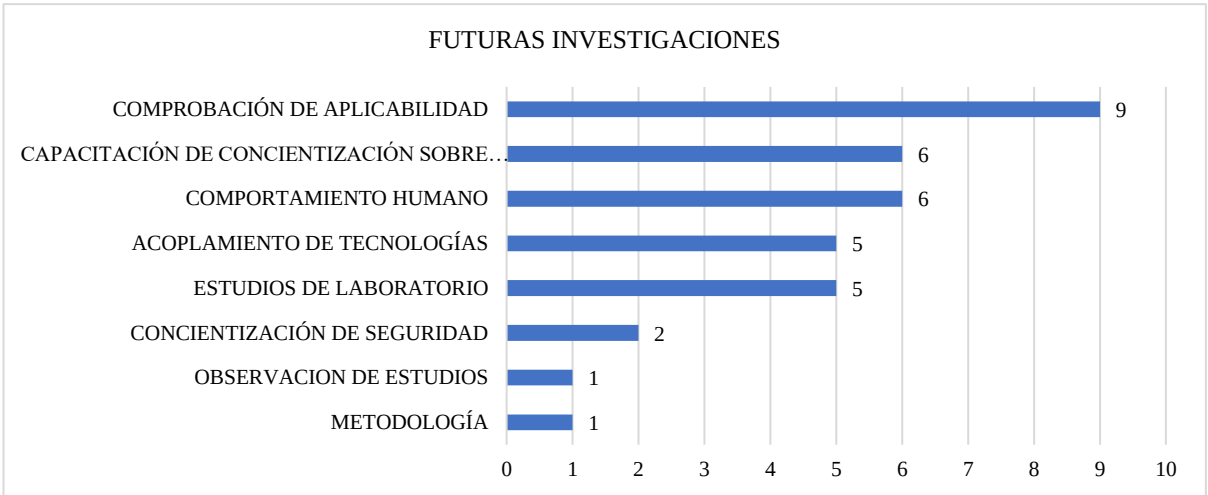


Figura B4. *Investigaciones Futuras.*