La_SEI School of Economic Intelligence & International Relations
Escuela de Inteligencia Económica y RRII
Universidad Autónoma de Madrid

2022 Volumen 4, nº 2, pp., 15-30

ISSN 2659-9791

- DRAFTS OF ECONOMIC INTELLIGENCE -

PERSONALIDAD EN INGENIERÍA SOCIAL: ¿QUÉ RASGOS SON MÁS VULNERABLES?

Sánchez Margolles, Sofía*

Resumen

El ser humano es el elemento más débil de un sistema de seguridad. La ingeniería social tiene como objetivo la explotación de las vulnerabilidades humanas, como la personalidad, para obtener información confidencial. El presente ensayo pretende comprender si hay ciertos individuos, de acuerdo con sus rasgos y perfiles de personalidad, que sean más vulnerables a los ataques sociales, para lo que se realiza un análisis de la bibliografía disponible. Los resultados son divididos en un perfil de susceptibilidad general y una vulnerabilidad específica según el contenido del ataque. Se concluye que los resultados obtenidos son aplicables a diferentes ámbitos de seguridad de la información, aunque se requiere más investigación respecto a la vulnerabilidad según el contenido del ataque.

Palabras clave: Vulnerabilidad, rasgos, ataques sociales, *phishing*, persuasión.

Abstract

Humans are the weakest element in a security system. Social engineering´s objective is the exploitation of human vulnerabilities, such as personality, to obtain privileged information. The present work intends to understand if there are certain individuals with a higher vulnerability to social attacks according to their personality traits and profiles, for which a literature review of the topic is conducted. The results are divided into a general susceptibility profile and a specific vulnerability regarding the content of the attack. It is concluded that the results obtained can be applied to different aspects of information security, although there is still a need for further research concerning vulnerability with regard to the content of the attacks.

Key words: *Vulnerability, personality traits, social attacks, phishing, persuasion.*

1. Introducción

La información mueve el mundo. La mayoría de los actores dentro del panorama tecnológico en el que nos encontramos actualmente, ya sean empresas privadas, organismos públicos o los propios individuos, procuran proteger la información de la que disponen a la vez que buscan nuevas formas de acceder a la información de otros para así obtener una ventaja competitiva. La seguridad de esta información confidencial ha sido principalmente relegada al campo de la ingeniería informática, descuidando el aspecto humano. Este factor humano, intrínsecamente psicológico, es el eslabón más débil de un sistema de seguridad (Mitnick y Simon, 2005; Mouton et al., 2014; Scheeres, 2008), además del aspecto cuyo estudio más se ha descuidado en este ámbito (Hadnagy, 2010). Sin embargo, y pese a la importancia que tiene el factor humano en las pérdidas de información privilegiada (Zamorano, 2018), no existe una gran cantidad de investigaciones que, partiendo de la psicología, estudien el fenómeno de la ingeniería social.

* *Escuela de Inteligencia Económica (La_SEI). Universidad Autónoma de Madrid (Spain)* Correo de contacto: sofiasmargolles@gmail.com

La ingeniería social, también conocida como "ataques sociales" (Uebelacker y Quiel, 2014), es, en términos generales, un tipo de ciberataque en el que un individuo manipula ilegítima e inadvertidamente a otro con el objetivo de obtener la información confidencial de la que dispone. Debido a la naturaleza persuasiva de las técnicas de ingeniería social, y conociendo la relación entre vulnerabilidad a estrategias de persuasión y rasgos de personalidad (Sánchez-Muñoz et al., 2018), cabe preguntarse ¿son todos los individuos igualmente vulnerables a los ataques sociales? ¿O existen, en cambio, perfiles de personalidad caracterizados por una mayor susceptibilidad?

Conseguir una definición de personalidad aceptada por toda la comunidad científica no es especialmente sencillo (Colom Marañón, 2018). La Real Academia Española (s.f.) incluye hasta ocho definiciones del término, entre ellas "diferencia individual que constituye a cada persona y la distingue de otra". Al igual que ocurre con la ingeniería social, ante la dificultad de obtener una única definición de personalidad optamos por centrarnos en las características que la definen, siendo en este caso la consistencia (a través de diferentes situaciones) y la estabilidad (a través del tiempo) de la conducta (Colom Marañón, 2018).

Múltiples estudios han observado como las diferencias en personalidad influyen en la manera en la que un individuo reacciona ante ataques sociales, relacionando la vulnerabilidad a estos con rasgos pertenecientes a diferentes modelos de personalidad (por ejemplo: Curtis et al., 2018; Cusack y Adedokun, 2018). El efecto de estos rasgos también ha sido observado en la determinación de actitudes relacionadas con la seguridad de la información de forma más general, no limitada exclusivamente a los ataques sociales (Shropshire et al., 2006; Uffen et al., 2012).

Como ha sido mencionado previamente, los ataques sociales dirigidos se caracterizan por la selección de una víctima concreta (Bullée et al., 2018), proceso en el que los ingenieros analizan la personalidad de sus objetivos para diseñar ataques especialmente efectivos contra ellos (Cusack y Adedokun, 2018; Quiel, 2013; Uebelacker y Quiel, 2014). En esta fase cobra gran importancia la persuasión, definida como "un tipo particular de comunicación en la que el emisor tiene como propósito convencer al receptor para cambiar sus actitudes hacia un objeto determinado mediante la transmisión de un mensaje y, como consecuencia de ello, cambiar su conducta" (Blanco et al., 2017, p. 228). La personalidad es una de las variables a tener en cuenta a la hora de diseñar un intento persuasivo, ya que la efectividad de las técnicas empleadas dependerá en parte de los rasgos de personalidad de los receptores (Sánchez-Muñoz et al., 2018). Las relaciones entre persuasión y personalidad han sido estudiadas a nivel general (por ejemplo, Halttu y Oinas-Kukkonen, 2021; Sánchez-Muñoz et al., 2018) y, específicamente, en ingeniería social (Quiel, 2013; Uebelacker y Quiel, 2014).

Debido a la relevancia de los rasgos de personalidad como factor a considerar en la elección una víctima y en el diseño del contenido del ataque, múltiples estudios han analizado las relaciones entre los ataques sociales y la personalidad de los dos principales actores en la ingeniería social, aunque la literatura parece haberse centrado especialmente en el estudio de la personalidad de los individuos vulnerables a estos ataques, siendo escasas las investigaciones focalizadas en la personalidad de los ingenieros sociales (Steinmetz et al., 2021). Esto puede ser debido a que, como observaron Curtis et al. (2018), son los rasgos de personalidad de las víctimas y no los de los atacantes los que predicen el éxito de un ataque.

En definitiva, la ingeniería social es un fenómeno en el que la psicología, y especialmente el estudio de la personalidad, tiene mucho que aportar. Predecir la habilidad de los miembros de una organización para mantener las políticas de seguridad y, por consiguiente, resistir los ataques sociales resultará imposible si no entendemos la relación existente entre los individuos y la seguridad de la información (Shropshire et al., 2006).

1.1. Ingeniería Social

La ingeniería social es el término empleado para referirse al proceso de engañar a una persona para que lleve a cabo un comportamiento de manera no intencionada que pueda causar o aumentar la probabilidad de causar un daño futuro (Stewart y Dawson, 2018). Otros autores la han definido como el acto de manipular mediante el engaño a una persona para conseguir acceso a sistemas de seguridad o información confidencial sensible (Hadnagy, 2010; Mitnick y Simon, 2002). Hadnagy (2010) usa este término para hacer referencia no solo a la acción, sino también a las destrezas y a la ciencia de manipular a una persona para que lleve a cabo un comportamiento que puede o no beneficiarle en algún aspecto de su vida.

No hay una única definición universalmente aceptada. Sin embargo, al examinar la literatura existente podemos observar aspectos comunes que representan el fenómeno (Quiel, 2013). Una de las características principales de la ingeniería social es la diferenciación de dos actores principales: el atacante y la víctima u objetivo, cuya dinámica es una de las claves para entender la ingeniería social (Quiel, 2013). El atacante o ingeniero social tiene como objetivo conseguir información por medio de los miembros de una organización (Peltier, 2006), empleando la persuasión en el proceso

(Quiel, 2013). Las víctimas, en cambio, son personas relacionadas con la organización objetivo, seleccionadas especialmente por los atacantes (Button et al., 2009, p. 15).

El objetivo final de la ingeniería social como proceso sería ganar acceso a información confidencial o sistemas completos de seguridad (Quiel, 2013). Debido a esto, la ingeniería social ha sido principalmente estudiada en ingeniería informática (Quiel, 2013), ámbito en el que se emplea para referirse a un conjunto de engaños para comprometer sistemas de seguridad como, por ejemplo, el phishing (Hong, 2012; Steinmetz et al., 2021). Sin embargo, sería reduccionista considerar únicamente el aspecto informático dentro de este fenómeno. La ingeniería social se compone tanto de esta perspectiva tecnológica como de una psicológica, centrada en la dimensión emocional y cognitiva (Bezuidenhout et al., 2010). Mitnick (2002), considera que la máxima letalidad de este fenómeno se obtiene al mezclar la explotación de las personas con la de la tecnología.

Aunque se trate la ingeniería social como un todo, esta se compone de un proceso complejo en el que se distinguen diferentes fases (Mitnick y Simon, 2002), tipos (Bullée et al., 2018) y técnicas de ataque (Peltier, 2006; Quiel, 2013).

Mitnick y Simon (2002) distinguen cuatro etapas en el proceso de los ataques sociales: investigación sobre la persona objetivo, desarrollo del rapport y confianza, explotación de dicha confianza y uso de la información obtenida. Estas etapas son empleadas tanto en ataques dirigidos como en ataques de oportunidad (Bullée et al., 2018). En los primeros cobra mayor relevancia la selección de una víctima concreta, mientras que en los segundos un grupo es escogido para obtener tantas víctimas como sea posible (Cusack y Adedokun, 2018).

De acuerdo con la literatura previa, los ataques de ingeniería social pueden ocurrir con diversos métodos y en cualquier ocasión (Sedano Pinzón, 2019). Un ciberataque de esta índole puede llevarse a cabo en diversos escenarios, ya sea mediante las redes sociales y otras formas de tecnología en línea o cara a cara (Samani y McFarland, 2015, p. 3). Así pues, la ingeniería social no solo posee una dimensión online, sino también una offline (Cross, 2019) en la que se hace un uso preferente de las técnicas basadas en humanos, que requieren interacción directa con el objetivo (Peltier, 2006).

Los ingenieros sociales detectan las vulnerabilidades humanas y las explotan para conseguir su objetivo (Jain et al., 2016). Entre estas vulnerabilidades se han estudiado la tendencia a confiar en los demás (Jain et al., 2016; Scheeres, 2008), la impulsividad (Norris et al., 2019), la autoridad (Stewart, 2015), las emociones (Scheeres, 2008), o variables de persuasión como la reciprocidad y la similitud (Jones, 2004, p. 5). Uno de los factores que más contribuyen a la susceptibilidad a la ingeniería social, entendiendo susceptibilidad como una debilidad percibida a daños o ataques (Houghton, 2004, p. 6), son los rasgos de personalidad (Maurya, 2013).

1.2. Personalidad en Ataques Sociales

Conseguir una definición de personalidad aceptada por toda la comunidad científica no es especialmente sencillo (Colom Marañón, 2018). La Real Academia Española (s.f.) incluye hasta ocho definiciones del término, entre ellas "diferencia individual que constituye a cada persona y la distingue de otra". Al igual que ocurre con la ingeniería social, ante la dificultad de obtener una única definición de personalidad optamos por centrarnos en las características que la definen, siendo en este caso la consistencia (a través de diferentes situaciones) y la estabilidad (a través del tiempo) de la conducta (Colom Marañón, 2018).

Múltiples estudios han observado como las diferencias en personalidad influyen en la manera en la que un individuo reacciona ante ataques sociales, relacionando la vulnerabilidad a estos con rasgos pertenecientes a diferentes modelos de personalidad (por ejemplo: Curtis et al., 2018; Cusack y Adedokun, 2018). El efecto de estos rasgos también ha sido observado en la determinación de actitudes relacionadas con la seguridad de la información de forma más general, no limitada exclusivamente a los ataques sociales (Shropshire et al., 2006; Uffen et al., 2012).

Como ha sido mencionado previamente, los ataques sociales dirigidos se caracterizan por la selección de una víctima concreta (Bullée et al., 2018), proceso en el que los ingenieros analizan la personalidad de sus objetivos para diseñar ataques especialmente efectivos contra ellos (Cusack y Adedokun, 2018; Quiel, 2013; Uebelacker y Quiel, 2014). En esta fase cobra gran importancia la persuasión, definida como "un tipo particular de comunicación en la que el emisor tiene como propósito convencer al receptor para cambiar sus actitudes hacia un objeto determinado mediante la transmisión de un mensaje y, como consecuencia de ello, cambiar su conducta" (Blanco et al., 2017, p. 228). La personalidad es una de las variables a tener en cuenta a la hora de diseñar un intento persuasivo, ya que la efectividad de las técnicas empleadas dependerá en parte de los rasgos de personalidad de los receptores (Sánchez-Muñoz et al., 2018). Las relaciones entre persuasión y personalidad han sido estudiadas a nivel general (por ejemplo, Halttu y Oinas-Kukkonen, 2021; Sánchez-Muñoz et al., 2018) y, específicamente, en ingeniería social (Quiel, 2013; Uebelacker y Quiel, 2014).

Debido a la relevancia de los rasgos de personalidad como factor a considerar en la elección una víctima y en el diseño

del contenido del ataque, múltiples estudios han analizado las relaciones entre los ataques sociales y la personalidad de los dos principales actores en la ingeniería social, aunque la literatura parece haberse centrado especialmente en el estudio de la personalidad de los individuos vulnerables a estos ataques, siendo escasas las investigaciones focalizadas en la personalidad de los ingenieros sociales (Steinmetz et al., 2021). Esto puede ser debido a que, como observaron Curtis et al. (2018), son los rasgos de personalidad de las víctimas y no los de los atacantes los que predicen el éxito de un ataque.

En definitiva, la ingeniería social es un fenómeno en el que la psicología, y especialmente el estudio de la personalidad, tiene mucho que aportar. Predecir la habilidad de los miembros de una organización para mantener las políticas de seguridad y, por consiguiente, resistir los ataques sociales resultará imposible si no entendemos la relación existente entre los individuos y la seguridad de la información (Shropshire et al., 2006).

1.3. Consecuencias de la Ingeniería Social

Las consecuencias de una inadecuada prevención de los ataques sociales no solo implican una pérdida monetaria de miles de millones de dólares al año (Internet Crime Complaint Center [IC3], 2019, p. 14), sino también la pérdida de prestigio y credibilidad de las organizaciones (Bulgurcu et al., 2010). Además, no son solo las empresas privadas y agencias gubernamentales las que se ven afectadas por este riesgo, sino que este se extiende a universidades y otras instituciones académicas (Bakhshi y Papadaki, 2011), además de a los propios individuos (Hosenball y Strobel, 2013; Sedano Pinzón, 2019) al causarles daño a nivel psicológico y fisiológico, entre otros (Cross et al., 2016; Whitty y Buchanan, 2016).

Sin embargo, no se dispone un método universal de defensa ante los ataques sociales (Quiel, 2013), y los sistemas de prevención empleados en la actualidad no resultan eficaces (Junger et al., 2017). Asimismo, las técnicas de ingeniería social se han ido adaptando a lo largo de la historia a los avances tecnológicos (Sedano Pinzón, 2019), lo que reitera la importancia de considerar factores diferenciados de la tecnología en el estudio de este fenómeno, factores que nos aporten una sensación de estabilidad ante el avance constante del entorno digital. El factor humano es, como ya se ha mencionado antes, el más vulnerable (Mitnick y Simon, 2005; Mouton et al., 2014; Scheeres, 2008) y, por lo tanto, al que más atención deberíamos prestar a la hora de diseñar sistemas preventivos.

Hauser (2016) resalta la importancia de comprender la amenaza que implican los ataques sociales, ya que desconocer que estamos expuestos a un engaño de esta naturaleza aumenta la probabilidad de que nos convirtamos en su víctima (Bezuidenhout et al., 2010). La habilidad del objetivo de detectar y resistirse a estos engaños es uno de los factores esenciales para el éxito o fracaso de un ataque social (Quiel, 2013). Sin embargo, ni las empresas ni la educación superior parecen entrenar de manera adecuada a sus miembros para la detección de estos ataques (Hauser, 2016; Mitnick y Simon, 2002; Rotvold, 2008; Thornburgh, 2004). El impacto de estos ataques podría ser reducido si las organizaciones implementasen una estrategia comprensiva de la seguridad de la información (Jain et al., 2016), incluyendo en esta las características de personalidad relacionadas con la vulnerabilidad.

En conclusión, debido a la importancia del aspecto humano en la predicción de ataques de ingeniería social y, en concreto, de las características de personalidad de los objetivos vulnerables, cabe preguntarse ¿existe un perfil de personalidad que caracterice a las personas vulnerables a los ataques sociales?

1.4. Objetivos

El presente estudio tiene como objetivo general analizar la bibliografía existente acerca de las relaciones entre psicología de la personalidad e ingeniería social. Además, se distinguen dos objetivos específicos:

- Obtener un perfil de vulnerabilidad general a la ingeniería social según la personalidad de las víctimas.
- Explorar, de manera superficial, si existe una vulnerabilidad específica en función del contenido persuasivo del ataque en relación a los rasgos de personalidad.

Aunque un mayor riesgo no implica certeza de comisión (Zamorano, 2018), si desconocemos qué personas son más susceptibles de caer ante un ataque social y revelar información privilegiada no podremos predecir las fugas de información ni establecer medidas de protección adecuadas.

2. Metodología

2.1. Materiales

Los materiales empleados en esta revisión consisten un total de 42 publicaciones científicas. De estas, 23 provienen de la búsqueda bibliográfica inicial localizadas en las diferentes bases de datos y buscadores, y las 19 adicionales han sido encontradas en el contenido de estas publicaciones. Adicionalmente, se han empleado 19 publicaciones provenientes de artículos de revistas científicas, libros y capítulos

de libros sobre personalidad y persuasión para la integración efectiva de la información.

2.1. Procedimiento

Se ha realizado una búsqueda bibliográfica en múltiples bases de datos y buscadores. La fuente de la que más artículos provienen es Google Académico, aunque también se ha empleado otros buscadores (EBSCO) y diversas bases de datos (APA PsycInfo, APA PsycArticles, APA PsycBooks, PSICODOC, APA PsycTherapy, Psychology and Behavioral Sciences Collection, eBook Collection, OpenDissertations y MEDLINE). Además, se han realizado búsquedas específicas en Research Gate y Science Direct. En la Tabla 1 puede observarse un resumen del número de publicaciones recuperadas de cada fuente. Algunas de ellas pueden ser encontradas en varias fuentes, por lo que se han incluido únicamente en una de ellas.

Tabla 1. Origen de las publicaciones encontradas en la búsqueda

Fuente	Publicaciones iniciales	Publicaciones finales
Google Académico	27	16
Science Direct	4	2
EBSCO (APA PsycInfo, APA PsycArticles, etc.)	4	4
Research Gate	1	1
Referencias dentro de las publicaciones encontradas inicialmente	0	19
Total	36	42

Con la finalidad de que la información empleada en esta revisión sea lo más actual posible, se acotó la búsqueda a publicaciones realizadas a partir del año 2000. Otros filtros empleados en las diferentes fuentes se centraron en el idioma de las publicaciones (español e inglés) y en la disponibilidad de estas, ya que solo se hizo uso de aquellas publicadas abiertamente o a las que se podía acceder mediante la identificación de la Universidad Autónoma de Madrid.

Los términos de búsqueda han sido combinados entre sí y empleados en las diferentes fuentes mencionadas: *personality, profiling, personality framework, personality traits, social engineering, social engineering attacks, social engineers, phishing, vulnerability, persuasion*. Por último, aunque las búsquedas se han realizado principalmente en inglés, los términos también han sido introducidos en castellano para ampliar el alcance de dicha búsqueda.

Inicialmente se realizó una búsqueda exploratoria de la que se extrajeron un total de 36 artículos, de los cuales solo se han empleado 23 una vez realizado un cribado en el que se consideraron como criterios de selección el rigor metodológico y la obtención de resultados significativos en los estudios, el uso de variables de personalidad y técnicas de ataque pertenecientes o relacionadas directamente con de ingeniería social, y la pertinencia de estas referencias con el objetivo de este trabajo. Adicionalmente, para ampliar la revisión se ha realizado una búsqueda más específica centrada en la localización de aquellas referencias de interés localizadas en los propios artículos encontrados, obteniendo un total de 19 estudios que también fueron cribados previamente a su selección.

Por último, con el objetivo de integrar los resultados de manera efectiva, también se han empleado un total de 19 artículos y libros sobre personalidad y persuasión. Sin embargo, los filtros empleados en la búsqueda de publicaciones sobre ingeniería social no han sido aplicados a estas fuentes.

3. Resultados

Gran parte de los artículos encontrados en la búsqueda exploratoria inicial provenían de la disciplina de ingeniería informática y, pese a ofrecer un punto de vista relevante sobre la ingeniería social, no todos incluían variables de personalidad. De igual manera, se han encontrado estudios y revisiones de otros tipos de fraudes que comparten características con la ingeniería social. Para comprender el papel que cumple la personalidad en los ataques sociales, debemos entender el fenómeno en su totalidad por lo que, pese a no ser parte del núcleo central, estas referencias han sido empleadas para contextualizar el tema.

Gran parte de los estudios publicados sobre ingeniería social tratan un tipo de ataque online específico, el "phishing". No se han encontrado estudios que hagan un uso explícito de técnicas de ingeniería social cara a cara, lo que puede deberse a la dificultad y el coste de la realización de estudios en este tipo de escenarios.

Respecto a las metodologías de los estudios referenciados, también resultan dispares. Algunos de ellos emplean un diseño de carácter cuantitativo, usando instrumentos como

encuestas o cuestionarios. Sin embargo, otros artículos presentan metodologías cualitativas, empleando, entre otros, entrevistas. Además, se ha hecho uso de revisiones teóricas sobre la temática en cuestión y propuestas de modelos de vulnerabilidad basados en la literatura previa.

En este apartado se analizarán los diversos rasgos de personalidad relevantes a la hora de distinguir personas vulnerables a la ingeniería social después de una introducción acerca del rol de la psicología en los ataques sociales. Para ello, se explicarán además los modelos de personalidad más relevantes para la comprensión de los resultados. Se establecen dos tipos de vulnerabilidad: una general a los ataques de ingeniería social organizada siguiendo el modelo PEN de Eysenck (1970), y otra específica en función del contenido del ataque.

3.1. La Psicología en ataques sociales

La ingeniería social es un proceso analizado desde diferentes disciplinas científicas (Washo, 2021). Aunque la ingeniería informática ha mostrado interés en comprender los ataques sociales debido a su relación intrínseca con estos (Quiel, 2013), algunos autores defienden que el éxito de un ataque social depende principalmente de la psicología detrás del ataque (Snyder, 2015) enfatizando la importancia de la explotación de vulnerabilidades humanas en el proceso (Bezuidenhout et al., 2010), especialmente los rasgos de personalidad (Maurya, 2013).

Ante las diferentes características de los tipos de ataques de ingeniería social, algunos autores defienden la posibilidad de que los rasgos de personalidad relevantes en un tipo de ataque no sean equivalentes en otros estilos de ataque (Albladi y Weir, 2017). Sin embargo, los rasgos de personalidad se caracterizan por ser consistentes y estables (Colom Marañón, 2018), por lo que su influencia en la vulnerabilidad debería ser semejante a través de diferentes escenarios y técnicas de ataque.

Asimismo, la concienciación, el factor más prevalente en el diseño de medidas de prevención de ataques sociales, parece ser menos predictivo que la personalidad. Los individuos parecen mostrar una dificultad a la hora de pronosticar su comportamiento en seguridad de la información incluso cuando están concienciados y disponen de conocimiento sobre el tema (Guo et al., 2011; Halevi et al., 2013; Vishwanath et al., 2011). Yan et al. (2018) defienden que no es adecuado tratar al ser humano como el eslabón más débil a nivel general, sino que debería identificarse la vulnerabilidad individual empleando medidas cuantitativas, como la personalidad.

Otros autores reiteran la importancia de considerar otros factores psicológicos además de la personalidad en este ámbito, argumentando que los ataques dependen a su vez de las circunstancias y de la técnica de ataque (Cusack y Adedokun, 2018). También se han identificado una serie de variables moderadoras entre la personalidad y los ataques sociales, como el estado emocional y las motivaciones (Albladi y Weir, 2017; Cusack y Adedokun, 2018). Sin embargo, en otros estudios la personalidad ha sido considerada el factor mediador clave entre el mensaje del ataque y la experiencia en su detección (Norris et al., 2019).

Tal y como se ha observado, la literatura previa parece mostrar que la personalidad es un factor especialmente relevante en la predicción de susceptibilidad a ataques sociales.

3.2. Vulnerabilidad general a la Ingeniería Social

La mayoría de las publicaciones encontradas emplean el modelo Big Five (Costa y McCrae, 1985), considerado por algunos autores el modelo mejor adaptado al contexto de la seguridad informática (Shropshire et al., 2006; Uebelacker y Quiel, 2014). Este modelo resume la personalidad en cinco dimensiones: extraversión, cordialidad, neuroticismo, responsabilidad y apertura. Los extravertidos se caracterizarían por estar llenos de energía y ser entusiastas, los cordiales por ser altruistas y afectuosos, los neuróticos serían nerviosos y ansiosos, los responsables serían concienzudos y controlados, y finalmente aquellos con altos niveles de apertura serían originales y abiertos de mente. Sin embargo, no es el único modelo de personalidad existente. El modelo de Eysenck (1970), conocido como modelo PEN, a diferencia del de Costa y McCrae solo hace uso de tres factores de personalidad: extraversión, neuroticismo y psicoticismo. Los dos primeros serían equivalentes a sus homólogos del modelo Big Five, mientras que psicoticismo se relaciona de manera negativa con los rasgos cordialidad y responsabilidad (John, 1990; Aluja et al., 2002; Zuckerman et al., 1993). Adicionalmente, el rasgo de apertura del modelo Big Five correlaciona significativamente de manera positiva con el rasgo extraversión del modelo PEN (Aluja et al., 2002; Zuckerman et al., 1993). Gray (1981) establece una serie de modificaciones al modelo de Eysenck, identificando tres sistemas motivacionales de la personalidad basándose en las bases biológicas de los rasgos del PEN: el Sistema de Activación Conductual o BAS, el Sistema de Inhibición Conductual o BIS, y el sistema de Ataque-Huida o FFS. El BAS responde a señales de recompensa, favoreciendo las respuestas de aproximación hacia estas en caso de estar sobreactivado, lo que ha sido asociado con una alta extraversión y neuroticismo. El BIS reacciona ante señales de castigo, inhibiendo la actividad; su sobreactivación ha sido asociada a altas puntuaciones del rasgo neuroticismo junto con baja extraversión (introversión). Por último, el FFS, asociado al rasgo

psicoticismo, en caso de estar infraactivado (puntuaciones altas en psicoticismo) resultaría en una mayor posibilidad de respuestas de agresividad e impulsividad. Otro modelo de personalidad planteado es la Triada Oscura (Paulhus y Williams, 2002), que distingue tres rasgos: maquiavelismo (personalidad característicamente manipulativa), narcisismo (de carácter dominante y grandioso) y psicopatía (que incluye alta impulsividad y baja empatía).

Aunque a nivel teórico el PEN y el Big Five se presentan como dos modelos diferenciados, como se ha mencionado previamente múltiples estudios de metaanálisis han observado que ambos modelos están relacionados (por ejemplo: Aluja et al., 2002; Zuckerman et al., 1993). Es decir, cuando hablamos de extraversión partiendo del modelo Big Five, estaríamos haciendo referencia al mismo rasgo del modelo PEN. De igual manera, todos los rasgos de la Triada Oscura han sido relacionados con psicoticismo (Mohammadzadeh y Ashouri, 2018). Considerando esta equivalencia entre los diferentes modelos de personalidad, y aunque la amplia mayoría de los estudios encontrados se basan en el modelo Big Five, en este apartado se va a emplear el modelo de tres rasgos de Eysenck para organizar la información encontrada, no solo porque únicamente con estos tres rasgos una persona quedaría completamente descrita (Eysenck, 1970) y porque ninguno de los demás modelos "se muestra tan comprehensivo ni con tanta capacidad para generar hipótesis y predicciones como el PEN" (de Juan Espinosa y García Rodríguez, 2004), sino también porque ha sido considerado el modelo más útil para realizar perfiles de personalidad (Sánchez-Muñoz et al., 2018).

Por último, aunque para facilitar su comprensión y debido a la estructura metodológica de los estudios revisados en ocasiones se van a tratar los rasgos de personalidad como si fuesen independientes, es necesario remarcar que los individuos no somos un conjunto de rasgos aislados, sino que, aunque dependan de sistemas cerebrales diferenciados, estos interactúan y se influyen entre sí (de Juan Espinosa y García Rodríguez, 2004).

3.2.1. Neuroticismo

En una revisión teórica sobre el rol del neuroticismo en la susceptibilidad a ataques de phishing, López-Aguilar y Solanas (2021) afirman que los resultados no parecen ser concluyentes. Sin embargo, la mayoría de las publicaciones encuentran que aquellos individuos con un mayor nivel de neuroticismo parecen tener una menor vulnerabilidad a la ingeniería social (por ejemplo: Albladi y Weir, 2017; Cho et al., 2016; Frauenstein y Flowerday, 2020). Esta tendencia ha sido tomada como referencia en propuestas de modelos de vulnerabilidad a los ataques sociales (Quiel, 2013; Uebelacker y Quiel, 2014), y ha sido observada en otros aspectos de seguridad de la información, como el respeto de políticas de ciberseguridad (McBride et al., 2012, p. 11) o sensibilidad a la privacidad (Bansal et al., 2010). La explicación que desde la investigación se ha dado a este fenómeno se centra en el valor protector de la ansiedad. Los individuos altos en este rasgo, también denominado inestabilidad emocional, se caracterizan por ser ansiosos, tensos o tímidos de acuerdo con el modelo PEN (Eysenck, 1970). Las víctimas de ataques sociales con alto neuroticismo presentan una mayor ansiedad ante los ordenadores (Albladi y Weir, 2017; Frauenstein y Flowerday, 2020; Parrish et al., 2009), lo que puede deberse al miedo a que les tomen como responsables de posibles brechas de seguridad y tiene como consecuencia que estos pasen menos tiempo en internet (Weirich y Sasse, 2001).

Como se ha explicado previamente, este rasgo (especialmente al combinarse con bajos niveles de extraversión) está relacionado con una sobreactivación del BIS (Gray, 1981). Este sistema reacciona inhibiendo conductas cuando se percibe un posible castigo, por lo que es posible que al percibir un castigo (por ejemplo, descargarse un virus o ser reprendidos por un superior), los individuos altos en neuroticismo eviten involucrarse en los ataques (por ejemplo, no respondiendo a un email de phishing). Tal y como se menciona en Cho et al. (2016), Chauvin et al. (2007) observaron una relación directa entre neuroticismo y percepción de riesgo; además, se ha encontrado una relación inversa entre percepción de riesgo y vulnerabilidad a ataques de phishing (Halevi et al., 2015, p. 7), aunque este último estudio presenta algunas limitaciones. La baja vulnerabilidad de los altos en neuroticismo podría deberse a su alta percepción de riesgo percibido, que a su vez influye en la confianza, haciendo que desconfíen más de los atacantes (Albladi y Weir, 2017), aunque se requiere más investigación sobre esto.

Por otro lado, también existen estudios que parecen identificar una mayor vulnerabilidad de aquellos individuos que presentan valores más altos en este rasgo (por ejemplo: Halevi et al., 2013). Sin embargo, estos resultados parecen ser minoritarios, y suelen presentar limitaciones metodológicas. El estudio publicado por Halevi et al. (2013) es mencionado a lo largo de la literatura como una de las referencias de que el neuroticismo es un rasgo definitorio de la vulnerabilidad al phishing, pese a que en este estudio la relación con vulnerabilidad se observa solo en mujeres, cuya muestra es de únicamente 13 participantes. Aunque no podemos negar la existencia de estos resultados, debido a sus limitaciones no van a ser considerados como centrales; sin embargo, se va a ofrecer una posible explicación a los mismos.

En ninguno de los estudios encontrados se analizan los efectos de los rasgos cuando estos interactúan entre sí, aunque la literatura haya mostrado que, al combinarse, los rasgos tienen efectos únicos (de Juan Espinosa y García Rodríguez, 2004). La combinación de altos valores de neuroticismo y extraversión provoca una sobreactivación del BAS,

favoreciendo las respuestas impulsivas ante señales de recompensa (Gray, 1981). Se ha observado que, a menor control de impulsos, menor detección de ataques de phishing (Lawson et al., 2020). En el mismo estudio se observa que el control de impulsos correlaciona de manera negativa tanto con neuroticismo como con extraversión (Lawson et al., 2020). Por consiguiente, es posible que la susceptibilidad de los individuos con altas puntuaciones en neuroticismo se deba a una sobreactivación del BAS. En el estudio de Halevi et al. (2013), el contenido del ataque hace referencia a una recompensa, lo que podría explicar la supuesta susceptibilidad de los altos en neuroticismo, aunque como se ha comentado este estudio es muy limitado metodológicamente. Actualmente no parece haber una línea clara de investigación que profundice sobre esta hipótesis.

En conclusión, los resultados apuntan a que debido a la alta ansiedad de los altos en neuroticismo estos individuos son menos vulnerables a la ingeniería social, aunque no podemos ignorar las contradicciones en la literatura. Sin embargo, es posible que los resultados en contra de esta teoría sean una consecuencia de las interacciones entre rasgos, no consideradas en los estudios analizados.

3.2.2. Extraversión

A lo largo de la literatura se ha considerado a la extraversión como el factor más prevalente en la vulnerabilidad a los ataques sociales (Albladi y Weir, 2017; Anawar et al., 2019; Cusack y Adedokun, 2018; Lawson et al., 2020). Con respecto al rasgo apertura que, como se ha explicado anteriormente, correlaciona positivamente con el rasgo extraversión del modelo PEN (Aluja et al., 2002; Zuckerman et al., 1993), no parece haber una conclusión clara acerca de cómo influye en la susceptibilidad a los ataques (Albladi y Weir, 2017). Parece haber tres posibles explicaciones complementarias para la vulnerabilidad de los extravertidos: el sesgo de optimismo, el uso de redes sociales y la impulsividad.

Los individuos altos en extraversión presentan un sesgo de emocionalidad positiva (Johnson et al., 1999) relacionado con las rutas dopaminérgicas cerebrales (Gray, 1981), lo que les hace ser más optimistas que los introvertidos (Depue y Collins, 1999). El sesgo de optimismo ha sido relacionado con una tendencia a ignorar los riesgos online (Debatin et al., 2009), además de con una variedad de riesgos offline (Weinstein y Klein, 1996). Consecuentemente, aquellos individuos con un sesgo de optimismo mayor (los más extravertidos), presentarían una mayor vulnerabilidad. Además, los individuos más optimistas hacen un mayor uso de internet (Campbell et al., 2007), y la actividad en redes sociales está relacionada con una mayor victimización por ataques de phishing (Halevi et al., 2013) y ciberataques en general (Saridakis et al., 2016). Múltiples estudios han observado los extravertidos interactúan más en redes sociales (por ejemplo: Casado-Riera y Carbonell, 2018; Correa et al., 2010; Jenkins-Guarnieri et al., 2012). Es posible que, debido a que emplean más las redes sociales (otro de los posibles vectores de técnicas online como el phishing), los extravertidos se expongan más a los ataques.

Por otro lado, la impulsividad ha sido relacionada con una baja capacidad de detección de phishing (Lawson et al., 2020) y con una mayor susceptibilidad a estos ataques, especialmente frente a aquellos que prometen recompensas económicas (Chen et al., 2017). Norris et al. (2019) explica que la detección de ciberataques puede verse dificultada debido a las vulnerabilidades relacionadas con conductas guiadas por incentivos. Sin embargo, algunos estudios refieren que la relación entre susceptibilidad e impulsividad es menor de lo que se consideraba (Pattinson et al., 2011), aunque estos resultados son minoritarios. Lawson et al. (2020) observan que el rasgo extraversión correlaciona negativamente con control de impulsos, lo cual coincide con la teoría de Gray (1981); una alta extraversión implicaría niveles más altos de activación en el BAS, sistema que facilita conductas de aproximación ante señales de recompensa y está intrínsecamente relacionado con la impulsividad. Al observar los resultados que muestran una alta susceptibilidad de los extravertidos por su impulsividad y los incluidos en el apartado anterior sobre la posible vulnerabilidad de los altos en neuroticismo, cabe pensar que la susceptibilidad ante ataques que incluyan refuerzos se deba al BAS.

En suma, la literatura parece coincidir en que las altas puntuaciones en extraversión están relacionadas con una mayor susceptibilidad, lo que puede ser debido al sesgo de emocionalidad positiva de este rasgo, a que interactúan más en redes sociales o a su impulsividad con respecto a señales de refuerzo.

3.2.3. Psicoticismo

Los individuos con puntuaciones altas en psicoticismo se caracterizarían por ser fríos, agresivos, impulsivos y no empáticos (Eysenck, 1970), lo que estaría relacionado con un FFS infraactivado, representando una tendencia hacia las respuestas agresivas e impulsivas (Gray, 1981). Como se ha mostrado en apartados anteriores, este rasgo correlaciona de manera negativa con cordialidad y con responsabilidad (Aluja et al., 2002; John, 1990; Zuckerman et al., 1993) aunque por razones distintas. Una alta cordialidad representaría puntuaciones más bajas en la dimensión de agresividad del psicoticismo, mientras que puntuaciones altas en responsabilidad implicarían una menor capacidad de la dimensión de control de impulsos (Aluja et al., 2002; Zuckerman et al., 1993). Debido a las relaciones diferenciales de los dos rasgos del modelo Big Five con el psicoticismo, no resulta sorprendente encontrar resultados que muestren dos tipos de

influencias diferenciales en la susceptibilidad de este rasgo a la ingeniería social.

Cordialidad parece ser, junto con extraversión, el rasgo más relacionado con la vulnerabilidad a ataques sociales (Anawar et al., 2019; Cho et al., 2016; Darwish et al., 2012). Estos resultados pueden atribuirse a la alta empatía de los individuos altos en cordialidad, lo que les hace más vulnerables a la persuasión en general (Sălceanu, 2014), a su altruismo (Parrish et al., 2009), y a su mayor tendencia a confiar en los demás (Cho et al., 2016; Cusack y Adedokun, 2018). La creación de confianza, criterio clave en la fuga de información privilegiada (Weirich y Sasse, 2001), es una de las estrategias más empleadas por los ingenieros sociales (Steinmetz et al., 2021), y ha sido considerada una de las principales razones de la susceptibilidad a los ataques sociales (Jain et al., 2016). Cordialidad contiene un subrasgo de confianza (Weirich y Sasse, 2001; Workman, 2008) que, aunque no afecta a la alta capacidad de detección de los ataques sociales de los altos en cordialidad (Lawson et al., 2020), sí parece aumentar su susceptibilidad. En otras palabras, la vulnerabilidad de los altos en cordialidad no parece deberse a una falta de detección de los ataques, sino a una tendencia a confiar en el carácter benigno de los atacantes. Sin embargo, Albladi y Weir (2017) encontraron una relación negativa entre la susceptibilidad a ataques sociales y el rasgo cordialidad, relación que justifican por una posible tendencia a seguir las medidas de seguridad.

Por otro lado, los individuos con altos niveles de responsabilidad parecen ser menos vulnerables (Albladi y Weir, 2017; Anawar et al., 2019; Lawson et al., 2020), lo que puede deberse a su alto control de impulsos (Albladi y Weir, 2017). Se han observado casos en los que este rasgo se asociaba con una mayor vulnerabilidad, lo que parece ser debido a que el mensaje del ataque fue diseñado para ser especialmente persuasivo con este rasgo, haciendo referencia al orden y a la eficacia (Halevi et al., 2015, p. 7). Esta baja vulnerabilidad puede deberse a la relación de este rasgo con una actitud positiva sobre la seguridad de la información (Uffen et al., 2012) o a la suspicacia de los individuos altos en responsabilidad (Goel et al., 2017). La función de la suspicacia ha sido estudiada en relación con la vulnerabilidad a ingeniería social en otros estudios (Harrison et al., 2016), pero se requiere más investigación acerca de esta relación para obtener resultados concluyentes. Debido a la correlación entre este rasgo y control de impulsos (Aluja et al., 2002; Zuckerman et al., 1993) y a la importancia de la impulsividad en la vulnerabilidad a estos ataques (Lawson et al., 2020; Chen et al., 2017), es posible que la función protectora de una alta responsabilidad se deba a la baja impulsividad de los altos valores en este rasgo.

Los rasgos narcisismo y psicopatía, pertenecientes a la Triada Oscura (Paulhus y Williams, 2002) y relacionados positivamente con psicoticismo (Mohammadzadeh y Ashouri, 2018), también parecen aumentar la susceptibilidad debido a su carácter impulsivo (Curtis et al., 2018). Como se puede observar, la impulsividad está presente en varios rasgos y combinaciones de estos adoptando diferentes facetas, ya que no parece representar un rasgo unitario de la personalidad (Revelle, 1997). De nuevo, parece que la impulsividad tiene un rol clave en la susceptibilidad a la ingeniería social.

En resumen, el psicoticismo puede afectar de dos formas diferentes a la susceptibilidad. Por un lado, una baja puntuación en la dimensión de agresividad implicaría una mayor vulnerabilidad, debido a la tendencia de confiar en la gente, junto con una mayor empatía y altruismo. Por otro, altas puntuaciones en la dimensión de impulsividad aumentarían la susceptibilidad, lo que se observa no solo al estudiar el rasgo de responsabilidad, sino también otros como narcisismo o psicopatía.

3.3. Vulnerabilidad en función del Contenido

Aunque el enfoque más común en la literatura es buscar una susceptibilidad de carácter general basándose en el modelo Big Five, parece ser que el contenido de un ataque social influye en esta vulnerabilidad, pudiendo resultar más persuasivo para unos u otros perfiles (Pantic y Husain, 2018) ya que, aunque existan perfiles susceptibles de ser manipulados, si el atacante no es capaz de motivarles reduce la probabilidad de éxito del ataque (Cusack y Adedokun, 2018). Sin embargo, debido a que la persuasión no es la cuestión central de este estudio y al reducido número de investigaciones disponibles, este tema solo será analizado de manera superficial. Se ha mantenido el uso del modelo Big Five en este apartado debido a que el objetivo del mismo no es establecer un perfil, sino realizar una exploración somera.

La mayoría de la literatura acerca de la vulnerabilidad a la ingeniería social en función del contenido del mensaje persuasivo se basa en los principios de influencia de Cialdini (1993) debido a que son válidos y aplicables en este contexto para determinar el contenido del ataque (Scheeres, 2008). Cialdini (1993) determina seis principios que englobarían el contenido de todos los intentos persuasivos: autoridad (obediencia a autoridades), compromiso y coherencia (tendencia a ser consistente), reciprocidad (tendencia a devolver los favores que hemos recibido), validación social (tendencia a hacer lo que hacen los demás), simpatía (obedecemos más a la gente que nos gusta) y escasez (se considera más valioso aquello que es escaso).

3.3.1. Responsabilidad

Se ha propuesto que los mensajes más efectivos con los individuos con altas puntuaciones en responsabilidad no apelan a emociones (Pantic y Husain, 2018), sino a normas y políticas (Uebelacker y Quiel, 2014). Dentro de los principios de Cialdini (1993), parece que el más efectivo para estos receptores sería autoridad, aunque también parecen ser vulnerables a reciprocidad y compromiso y coherencia (Tiwari, 2020). Sin embargo, es posible que su susceptibilidad a cualquier mensaje dentro de un ataque social se vea reducida si existen protocolos de seguridad explícitos para afrontar estos ataques (Uebelacker y Quiel, 2014), lo que concuerda con la idea de que el entrenamiento en seguridad debería reducir especialmente la victimización de los altos en este rasgo (Parrish et al., 2009). Esto también podría deberse a que el mediador más relevante entre responsabilidad y vulnerabilidad es la competencia en temas de seguridad (Albladi y Weir, 2017).

3.3.2. Apertura

Aunque los resultados sobre la vulnerabilidad de las personas con altos niveles de Apertura no son especialmente claros, parece que su susceptibilidad aumentaría ante contenidos que estimulen su curiosidad (Pantic y Husain, 2018; Parrish et al., 2009). Uebelacker y Quiel (2014) proponen en su modelo que este rasgo tendrá, además, una relación con el principio de escasez debido a una posible percepción de reducción de libertad.

3.3.3. Extraversión

Como se ha visto en el apartado anterior, los extravertidos son, en general, los individuos más susceptibles junto con los altos en cordialidad. Esto puede observarse también al mirar la vulnerabilidad específica según el contenido del mensaje persuasivo, ya que estos individuos parecen ser susceptibles a una mayor cantidad de principios de influencia: validación social, simpatía, escasez, compromiso y coherencia, y autoridad (Lawson et al., 2020; Uebelacker y Quiel, 2014). Además, también parecen ser vulnerables a otras variables de persuasión, como a los elogios (Pantic y Husain, 2018) y a la urgencia temporal (Tiwari, 2020).

3.3.4. Cordialidad

Los resultados encontrados en la búsqueda acerca de este rasgo son altamente similares a los que se explicaron en el apartado de vulnerabilidad general, por lo que no se entrará en mucho detalle. El principio de influencia al que son más susceptibles los altos en cordialidad parece ser el de autoridad (Tiwari, 2020), aunque también se ha propuesto que serán más fácilmente atacados si se emplean los principios de reciprocidad, simpatía y aprobación social (Uebelacker y Quiel, 2014), o si se hace referencia a la bondad de la víctima en una búsqueda de ayuda (Pantic y Husain, 2018).

3.3.5. Neuroticismo

Aunque a nivel general parece que los individuos altos en neuroticismo presentan una menor vulnerabilidad, si en el ataque se hace referencia a contenidos amenazantes, especialmente por parte de una autoridad, su susceptibilidad aumenta (Pantic y Husain, 2018). Uebelacker y Quiel (2014) lo atribuyen al sistema motivacional de este rasgo, basado en "incertidumbre a amenazas". Es decir, es posible que, en caso de tener un BIS sobreactivado, incluir referencias a castigos reduzca el valor protector de la ansiedad y aumente la susceptibilidad a los ataques sociales.

4. Discusión

El presente estudio ha intentado dar una respuesta a la pregunta de si existen perfiles de personalidad que representen una mayor vulnerabilidad a la ingeniería social. La bibliografía analizada parece coincidir en que sí existen ciertos rasgos que aumentan, de manera general, la vulnerabilidad de un individuo a los ataques sociales. De acuerdo con el primer objetivo específico, los resultados desarrollados en el apartado anterior se resumen de acuerdo con los tres rasgos del modelo PEN para establecer un perfil de vulnerabilidad general:

- Un bajo neuroticismo aumentaría la vulnerabilidad debido a una menor ansiedad, que ejerce un rol de protección.
- Una alta extraversión implica mayor susceptibilidad, lo que puede deberse a una alta impulsividad, a una mayor interacción en redes sociales o a una tendencia a ignorar riesgos debido a su sesgo de emocionalidad positiva.
- El psicoticismo tiene una influencia dual: bajos niveles en la dimensión de agresividad estarían relacionados con una mayor tendencia a confiar en la gente, aumentando la vulnerabilidad; mientras que altos niveles en la dimensión de impulsividad aumentarían la susceptibilidad.

En resumen, una persona estable (bajo neuroticismo) y extravertida representaría el perfil más vulnerable, de acuerdo con la bibliografía. Esta vulnerabilidad aumentaría si la persona presenta una baja agresividad y una puntuación alta en la dimensión de impulsividad del psicoticismo. En general, y de manera transversal a los tres rasgos, parece que la impulsividad es la característica que más susceptible hace a un individuo a los ataques sociales.

Por otro lado, siguiendo el segundo objetivo específico se exploró la vulnerabilidad de cada rasgo en función del contenido del ataque y se observó que los diferentes perfiles de

personalidad pueden presentar una mayor vulnerabilidad si se emplea el contenido adecuado. Debido a la cantidad limitada de investigaciones de calidad que traten la relación entre vulnerabilidad según personalidad y contenido persuasivo del ataque, no ser van a realizar perfiles individuales de vulnerabilidad según el contenido concreto al que es susceptible cada rasgo. Sin embargo, esta representa una de las principales líneas futuras de estudio.

La bibliografía encontrada, pese a ser relativamente escasa, parece mostrar resultados concluyentes con respecto a la vulnerabilidad general a la ingeniería social. Aunque algunos de los estudios sobre esta temática no emplean una metodología apropiada, gran parte parece obtener resultados significativos empleando un buen diseño cuantitativo (por ejemplo, Albladi y Weir, 2017), por lo que las conclusiones sobre el perfil de vulnerabilidad general pueden ser aplicadas a nivel práctico. Sin embargo, no se puede afirmar lo mismo para los estudios sobre vulnerabilidad a contenidos específicos, ya que, aunque algunas de las publicaciones parecen mostrar resultados significativos (como Lawson et al., 2020) estas son bastante reducidas, por lo que antes de poder establecer perfiles de susceptibilidad concluyentes se debe ampliar esta línea de investigación, ya que incluir la persuasión como otra variable más aumenta la complejidad del fenómeno.

4.1. Fortalezas y limitaciones del estudio

Por un lado, la principal fortaleza de este estudio es que no consiste en un resumen de la bibliografía acerca de la relación entre personalidad e ingeniería social, sino que representa una integración de esta, basándose en teorías de personalidad comprobadas empíricamente para ofrecer una explicación a los resultados obtenidos. Además, se ha propuesto una síntesis de los rasgos con mayor susceptibilidad de acuerdo con el modelo PEN, con el objetivo de facilitar la aplicación de los resultados a la hora de perfilar individuos vulnerables. Sin embargo, las publicaciones disponibles actualmente no hacen referencia a ataques cara a cara, y aunque debido a la consistencia y estabilidad de los rasgos los resultados sobre ataques online deberían ser aplicables a otros escenarios offline, se requiere más investigación para comprobarlo. Es posible que existan otras publicaciones que hubieran resultado relevantes para la consecución de los objetivos, pero que no se haya podido acceder a ellas con los medios de los que se disponía.

Por otro lado, se podría destacar como una limitación presente en este estudio el carácter contradictorio de la literatura, debido principalmente a factores metodológicos. A su vez, en ninguno de los estudios encontrados se considera el efecto de los rasgos al ser combinados, lo que limita la validez de las conclusiones. Por último, y aunque la personalidad parece ser el mejor predictor de vulnerabilidad a los ataques sociales, es posible que los resultados sobre la susceptibilidad resulten incompletos al ignorar el efecto de otros posibles factores, como el procesamiento de información (Frauenstein y Flowerday, 2020), el proceso de toma de decisiones (Uebelacker y Quiel, 2014) o la probabilidad de elaboración (Harrison et al., 2016).

4.2. Aplicaciones y líneas futuras de estudio

Los resultados de este estudio pueden ser aplicados en la identificación de individuos vulnerables a la ingeniería social, lo que permitiría la detección de los eslabones más débiles en la seguridad de la información y el diseño de programas de prevención de ataques sociales basados en la personalidad específica de estos individuos vulnerables. Por otro lado, no es posible obviar la otra cara del uso de estos resultados, ya que estos facilitan la selección de personas vulnerables, pudiendo propiciar un mayor número de ataques efectivos. Esto nos lleva a una línea de investigación futura especialmente relevante, la búsqueda de estándares éticos, deontológicos y legales que regulen y limiten esta práctica.

Con el objetivo de obtener una mayor comprensión sobre la influencia de la personalidad, se debería además considerar la interacción entre rasgos a la hora de analizarlos como variables independientes, puesto que es posible que la contradicción observada entre publicaciones esté relacionada con este fenómeno. Otras líneas futuras de investigación incluirían comprobar si la susceptibilidad a ataques online es equivalente a otros contextos de la ingeniería social, especialmente aquellos cara a cara, y examinar el efecto de otras variables psicológicas como la probabilidad de elaboración. Por último, y puesto que la investigación parece mostrar diferentes grados de vulnerabilidad de acuerdo con el contenido persuasivo de los ataques sociales, es relevante estudiar en un futuro la relación entre contenido del mensaje persuasivo y susceptibilidad a la ingeniería social según la personalidad de los receptores.

5. Referencias

Albladi, S. M., y Weir, G. R. S. (2017, noviembre 23-24). *Personality traits and cyber-attack victimisation: Multiple mediation analysis* [Acta de congreso]. 2017 Internet of Things Business Models, Users, and Networks, Copenhague, Dinamarca. https://doi.org/10.1109/CTTE.2017.8260932

Aluja, A., García, O. y García, L. F. (2002). A comparative study of Zuckerman´s three structural models of personality through the NEO-PI-R, ZKPQ-III-R, EPR-RS, and Goldberg's 50-bipolar adjectives. *Personality and*

Individual Differences, 33(5), 713-725. https://doi.org/10.1016/S0191-8869(01)00186-6

Anawar, S., Kunasegaran, D. L., Mas´ud, M. Z., y Zakaria, N. A. (2019). Analysis of phishing susceptibility in a workplace: a big-five personality perspectives. *Journal of Engineering Science and Technology, 14*(5), 2865-2882. https://jestec.taylors.edu.my/Vol%2014%20issue%205%20October%202019/14_5_30.pdf

Bakhshi, T., y Papadaki, M. (2011). Social Engineering Vulnerabilities. En P. Dowland, y S. Furnell (*Eds.*). *Advances in Networks, Computing and Communications 6* (pp. 23-31). University of Plymouth School Of Computing, Communications And Electronics.

Bansal, G., Zahedi, F., y Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems, 49*(2), 138-150. https://doi.org/10.1016/j.dss.2010.01.010

Bezuidenhout, M., Mouton, F., y Venter, H. S. (2010, agosto 2-4). *Social engineering attack detection model: SEADM* [Acta de congreso]. 2010 Information Security for South Africa, Johannesburg, Sudáfrica. https://doi.org/10.1109/ISSA.2010.5588500

Blanco, A., Horcajo, J., y Sánchez, F. (2017). *Cognición social.* Pearson Educación.

Bulgurcu, B., Cavusoglu, H., y Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548. https://doi.org/10.2307/25750690

Bullée, J., Montoya, L., Pieters, W., Junger, M., y Hartel, P. H. (2018). On the anatomy of social engineering attacks- A literature-based dissection of successful attacks. *Journal of Investigative Psychology and Offender Profiling, 15*, 20-45. https://doi.org/10.1002/jip.1482

Button, M., Lewis, C., y Tapley, J. (2009). *Fraud typologies and victims of fraud*. National Fraud Authority. https://researchportal.port.ac.uk/en/publications/fraud-typologies-and-the-victims-of-fraud-literature-review

Campbell, J., Greenauer, N., Macaluso, K., y End, C. (2007). Unrealistic optimism in internet events. *Computers in Human Behavior, 23*(3), 1273-1284. https://doi.org/10.1016/j.chb.2004.12.005

Casado-Riera, C., y Carbonell, X. (2018). La influencia de la personalidad en el uso de Instagram. *Aloma, 36*(2), 23-31. https://doi.org/10.51698/aloma.2018.36.2.23-31

Chauvin, B., Hermand, D., y Mullet, E. (2007). Risk perception and personality facets. *Risk Analysis, 27*(1), 171-185. https://doi.org/10.1111/j.1539-6924.2006.00867.x

Chen, H., Beaudoin, C. E., y Hong, T. (2017). Securing online privacy: an empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior, 70*, 291-302. https://doi.org/10.1016/j.chb.2017.01.003

Cho, J. H., Cam, H., y Oltramari, A. (2016, marzo 21-25). *Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis* [Acta de congreso]. 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), San Diego, Estados Unidos. https://doi.org/10.1109/COGSIMA.2016.7497779

Cialdini, R. B. (1993). *Influence: Science and practice*. Harper Collins.

Colom Marañón, R. (2018). *Manual de psicología diferencial.* Ediciones Pirámide.

Correa, T., Hinsley, A. W., y Gil de Zúñiga, H. (2010). Who interacts on the Web?: The intersection of users' personality and social media use. *Computers in human behavior, 26*(2), 247-253. https://doi.org/10.1016/j.chb.2009.09.003

Costa, P. T., y McCrae, R. R. (1985). *The NEO Personality Inventory manual*. Psychological Assessment Resources.

Cross, C. (2019). Is online fraud just fraud? Examining the efficacy of the digital divide. *Journal of Criminological Research, Policy and Practice, 5*(2), 120-131. https://doi.org/10.1108/JCRPP-01-2019-0008

Cross, C., Richards, K., y Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends & Issues in Crime and Criminal Justice, 518*, 1-14. https://www.aic.gov.au/sites/default/files/2020-05/tandi518.pdf

Curtis, S. R., Rajivan, P., Jones, D. N., y Gonzalez, C. (2018). Phishing attempts among the dark triad: Patterns of attack and vulnerability. *Computers in Human Behavior, 87*, 174-182. https://doi.org/10.1016/j.chb.2018.05.037

Cusack, B., y Adedokun, K. (2018, enero 1). *The impact of personality traits on user's susceptibility to social engineering attacks* [Acta de congreso]. 16th Australian Information Security Management Conference, Perth, Australia. https://doi.org/10.25958/5C528FFA66693

Darwish, A., Zarka, A. E., y Aloul, F. (2012, diciembre 18-20). *Towards understanding phishing victims' profile* [Acta de congreso]. 2012 International Conference on Computer Systems and Industrial Informatics (ICCSII), Sharjah, Emiratos Árabes Unidos. https://doi.org/10.1109/ICCSII.2012.6454454

Debatin, B., Lovejoy, J. P., Horn, A., y Hughes, B. N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication, 15*(1), 83-108. https://doi.org/10.1111/j.1083-6101.2009.01494.x

Depue, R. A., y Collins, P. F. (1999). Neurobiology of the structure of personality: Dopamine, facilitation of incentive motivation, and extraversion. *Behavioral and Brain Sciences*, *22*(3), 491-517. https://doi.org/10.1017/S0140525X99002046

Eysenck, H. J. (1970). *The structure of human personality*. Methuen.

Frauenstein, E. D., y Flowerday, S. (2020). Susceptibility to phishing on social network sites: A personality information processing model. *Computers & Security, 94*, 1-18. https://doi.org/10.1016/j.cose.2020.101862

Goel, S., Williams, K., y Dincelli, E. (2017). Got Phished? Internet Security and Human Vulnerability. *Journal of the Association for Information Systems, 18*(1), 22-44. https://doi.org/10.17705/1jais.00447

Gray, J. A. (1981). A critique of Eysenck's theory of personality. En Eysenck, H. J. (*Ed.*). *A model for personality* (pp. 246-276). Springer.

Guo, K. H., Yuan, Y., Archer, N. P., y Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems, 28*(2), 203-236. https://doi.org/10.2753/mis0742-1222280208

Hadnagy, C. (2010). *Social engineering: The art of human hacking*. Wiley.

Halevi, T., Lewis, J., y Memon, N. (2013, mayo 13-17). *A Pilot Study of Cyber Security and Privacy Related Behavior and Personality Traits* [Acta de congreso]. 22nd International Conference on World Wide Web, Rio de Janeiro, Brasil. https://doi.org/10.1145/2487788.2488034

Halevi, T., Memon, N., y Nov, O. (2015). *Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks*. Social Science Research Network. http://dx.doi.org/10.2139/ssrn.2544742

Halttu, K., y Oinas-Kukkonen, H. (2021). Susceptibility to social influence strategies and persuasive system design: exploring the relationship. *Behaviour & Information Technology*, 1-22. https://doi.org/10.1080/0144929X.2021.1945685

Harrison, B., Vishwanath, A., y Rao, R. (2016, enero 5-8). *A User-Centered Approach to Phishing Susceptibility: The Role of a Suspicious Personality in Protecting Against Phishing* [Acta de congreso]. 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa, Estados Unidos. https://doi.org/10.1109/HICSS.2016.696

Hauser, D. (2016, mayo 19-20). *Social Engineering Awareness in Business and Academia* [Acta de congreso]. Eleventh Midwest Association for Information Systems Conference, Milwaukee, Estados Unidos. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1007&context=mwais2016

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74-81. https://doi.org/10.1145/2063176.2063197

Hosenball, M., y Strobel, W. (2013, 8 de noviembre). *Exclusive: Snowden persuaded other NSA workers to give up passwords*. Reuters. https://www.reuters.com/article/net-us-usa-security-snowden-idUSBRE9A703020131108

Houghton, P. (2004). *Potential System Vulnerabilities of a Network-Enabled Force* [Informe nº11]. Defense Science and Technology Laboratory. https://apps.dtic.mil/dtic/tr/fulltext/u2/a466659.pdf

Internet Crime Complaint Center [IC3] (2019). *2018 Internet Crime Report*. https://www.ic3.gov/Media/PDF/AnnualReport/2018_IC3Report.pdf.

Jain, A., Tailang, H., Goswami, H., Dutta, S., Sankhla, M. S., y Kumar, R. (2016). Social Engineering: Hacking a Human Being through Technology. *IOSR Journal of Computer Engineering, 18*(5), 94-100. https://www.researchgate.net/publication/309234725_Social_Engineering_Hacking_a_Human_Being_through_Technology

Jenkins-Guarnieri, M. A., Wright, S. L., y Hudiburgh, L. M. (2012). The relationships among attachment style, personality traits, interpersonal competency, and Facebook use. *Journal of Applied Developmental Psychology, 33*(6), 294-301. https://doi.org/10.1016/j.appdev.2012.08.001

John, O. P. (1990). The Big Five Factor Taxonomy: Dimensions of Personality in the Natural Language and in Questionaires. En L. Pervin (*Ed.*). *Handbook of Personality: Theory and Research* (pp. 66-100). Guilford Press.

Johnson, D. L., Wiebe, J. S., Gold, S. M., Andreasen, N. C., Hichwa, R. D., Watkins, G. L., y Boles Ponto, L. L. (1999). Cerebral blood flow and personality: a positron emission tomography study. *The American Journal of Psychiatry*, *156*(2), 252-257. https://ajp.psychiatryonline.org/doi/10.1176/ajp.156.2.252

Jones, C. (2004). *Social Engineering: Understanding and Auditing.* SANS Institute. https://sansorg.egnyte.com/dl/jkIn15cfNb

De Juan, M., y García, L. F. (2004). *Nuestra personalidad. En qué y por qué somos diferentes*. Biblioteca Nueva.

Junger, M., Montoya, L., y Overink, F.J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behaviour, 66*, 75-87. https://doi.org/10.1016/j.chb.2016.09.012

Lawson, P., Pearson, C. J., Crowson, A., y Mayhorn, C. B. (2020). Email phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy. *Applied Ergonomics, 86*, 113-122. https://doi.org/10.1016/j.apergo.2020.103084

López-Aguilar, P., y Solanas, A. (2021, julio 12-16). *Human Susceptibility to Phishing Attacks Based on Personality Traits: The Role of Neuroticism* [Acta de congreso]. 2016 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, España. https://doi.org/10.1109/COMPSAC51774.2021.00192

Maurya, R. (2013). *Social Engineering: Manipulating the Human*. Scorpio Net Security Services.

McBride, M., Carter, L., y Warkentin, M. (2012). *Exploring the Role of Individual Employee Characteristics and Personality on Employee Compliance with Cybersecurity Policies*. Institute for Homeland Security Solutions. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.453.3551&rep=rep1&type=pdf#:~:text=More%20Open%20individuals%20are%20less%20likely%20to%20violate%20cybersecurity%20policies.&text=More%20Extroverted%20individuals%20are%20more%20likely%20to%20violate%20cybersecurity%20policies.&text=More%20Neurotic%20individuals%20are%20less%20likely%20to%20violate%20cybersecurity%20policies

Mitnick, K. (2002, 14 de octubre). *How to Hack People*. BBC News Online. http://news.bbc.co.uk/2/hi/technology/2320121.stm

Mitnick, K. D., y Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. Wiley.

Mitnick, K. D., y Simon, W. L. (2005). *The Art of Intrusion: the Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*. Wiley.

Mohammadzadeh, A., y Ashouri, A. (2018). Comparison of Personality Correlates of Machiavellianism, Narcissism and Psychopathy (Dark Triad of Personality) in Three Factor Personality Model. *Iranian Journal of Psychiatry and Clinical Psychology, 24*(1), 44-55. https://www.sid.ir/en/Journal/ViewPaper.aspx?ID=574536

Mouton, F., Malan, M. M., Leenen, L., y Venter, H. S. (2014, agosto 13-14). *Social engineering attack framework* [Acta de congreso]. 2014 Information Security for South Africa, Pretoria, Sudáfrica. https://doi.org/10.1109/ISSA.2014.6950510

Norris, G., Brookes, A., y Dowell, D. (2019). The Psychology of Internet Fraud Victimisation: a Systematic Review. *Journal of Police and Criminal Psychology, 34*(3), 231-245. https://doi.org/10.1007/s11896-019-09334-5

Pantic, N., y Husain, M. (2018, diciembre 10-13). *A Decision Support System for Personality Based Phishing Susceptibility Analysis* [Acta de congreso]. 2018 IEEE International Conference on Big Data (Big Data), Seattle, Estados Unidos. https://doi.org/10.1109/BigData.2018.8622555

Parrish, J. L., Bailey, J. L., y Courtney, J. F. (2009). *A Personality Based Model for Determining Susceptibility to Phishing Attacks.* Academia.edu. http://www.swdsi.org/swdsi2009/Papers/9J05.pdf

Pattinson, M. R., Jerram, C., Parsons, K., McCormac, A., y Butavicius, M. A. (2011, julio 7-8). *Managing phishing emails: a scenario-based experiment* [Acta de congreso]. Fifth International Symposium on Human Aspects of the Information Security & Assurance (HAISA 2011), Londres, Reino Unido. https://www.semanticscholar.org/paper/Managing-Phishing-Emails%3A-A-Scenario-Based-Pattinson-Jerram/91c76694abecfc0dee4fb072038844778d42ad80

Paulhus, D. L., y Williams, K. M. (2002). The Dark Triad of personality: narcissism, Machiavellianism, and psychopathy. *Journal of Research in Personality, 36*(6), 556-563. https://doi.org/10.1016/S0092-6566(02)00505-6

Peltier, T. R. (2006). Social engineering: Concepts and solutions. *Information Security Journal, 15*(5), 13. https://doi.org/10.1201/1086.1065898X/46353.15.4.20060901/95427.3

Quiel, S. (2013). *Social Engineering in the Context of Cialdini's Psychology of Persuasion and Personality Traits* [Tesis de grado, Technische Universität Hamburg]. https://tore.tuhh.de/handle/11420/1126.

Real Academia Española. (s.f.). Personalidad. En *Diccionario de la lengua española*. Recuperado el 26 de marzo de 2022, de https://dle.rae.es/personalidad

Revelle, W. (1997). Extraversion and Impulsivity. The lost dimension? En H. Nybord (*Ed.*). *The scientific study of human nature: Tribute to Hans J. Eysenck at eighty* (pp. 189-213). Elsevier.

Rotvold, G. (2008). How to create a security culture in your organization: a recent study reveals the importance of assessment, incident response procedures, and social engineering testing in improving security awareness program. *Information Management Journal, 42*(6), 32- 38. https://go.gale.com/ps/i.do?id=GALE%7CA189486076&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=15352897&p=AONE&sw=w&userGroupName=anon%7Ef7751722

Sălceanu, C. (2014). Personality factors and resistance to the manipulation of advertising. *Procedia-Social and Behavioral Sciences, 127*, 5-9. https://doi.org/10.1016/j.sbspro.2014.03.202

Samani, R., y McFarland, C. (2015). *Ataques al sistema operativo humano*. Intel Security. https://nanopdf.com/download/ataques-al-sistema-operativo-humano_pdf

Sánchez-Muñoz, I., Calcerrada Alcazar, M. L., González Álvarez, J. L., y De Juan Espinosa, M. (2018). Persuasión y Personalidad. El receptor en la comunicación persuasiva. *Behavior & Law Journal, 4*(1), 9-20. https://doi.org/10.47442/blj.v4.i1.48

Saridakis, G., Benson, V., Ezingeard, J. N., y Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change*, *102,* 320-330. https://doi.org/10.1016/j.techfore.2015.08.012

Scheeres, J. W. (2008). *Establishing the Human Firewall: Reducing an Individual's Vulnerability to Social Engineering Attacks* [Tesis de master, Air Force Institute of Technology]. https://www.semanticscholar.org/paper/Establishing-the-Human-Firewall%3A-Reducing-an-toScheeres/a2d3f4340b7db6f9d162adb53826060e294eb446

Sedano Pinzón, J. J. (2019). *La ingeniería social, el antes y el ahora de un problema global* [Trabajo de monografía, Universidad Nacional Abierta y a Distancia]. https://repository.unad.edu.co/bitstream/handle/10596/28152/%20%09jaime.sedano.pdf?sequence=1&isAllowed=y

Shropshire, J., Warkentin, M., Johnston, A., y Schmidt, M. (2006, enero 4-6). *Personality and IT security: An application of the five-factor model* [Acta de congreso]. Twelfth Americas Conference on Information Systems (AMCIS 2006), Acapulco, México. https://aisel.aisnet.org/amcis2006/415/

Snyder, C. (2015). *Handling Human Hacking: Creating a Comprehensive Defensive Strategy Against Modern Social Engineering* [Tesis de honor, Liberty University]. https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,uid&db=ddu&AN=731F775E914DB8DE&lang=es&site=ehost-live&scope=site

Steinmetz, K. F., Pimentel, A., y Goe, W. R. (2021). Performing social engineering: A qualitative study of information security deceptions. *Computers in Human Behavior, 124*, 1-11. https://doi.org/10.1016/j.chb.2021.106930

Stewart, J. H. (2015). *Social engineering deception susceptibility: Modification of personality traits susceptible to social engineering manipulation to acquire information through attack and exploitation* [Tesis de doctorado, Colorado Technical University]. https://www.proquest.com/openview/65afc1823b2f3205235292f80fa07368/1?pq-origsite=gscholar&cbl=18750

Stewart, J., y Dawson, M. (2018). How the modification of personality traits leaves one vulnerable to manipulation in social engineering*? International Journal of Information Privacy, Security and Integrity, 3*(3), 187-208. https://doi.org/10.1504/IJIPSI.2018.10013213

Thornburgh, T. (2004, octubre 8). *Social engineering: the dark art* [Acta de congreso]. 1st annual conference on Information security curriculum development, Kennesaw, Estados Unidos. https://doi.org/10.1145/1059524.1059554

Tiwari, P. (2020). *Exploring Phishing Susceptibility Attributable to Authority, Urgency, Risk Perception and Human Factors* [Tesis de master, Purdue University]. https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,url,uid&db=ddu&AN=C95C38763884E9C5&lang=es&site=ehost-live&scope=site

Uebelacker, S., y Quiel, S. (2014, julio 18). *The Social Engineering Personality Framework* [Acta de congreso]. 2014 Workshop on Socio-Technical Aspects in Security and

Trust, Viena, Austria. https://doi.org/10.1109/STAST.2014.12

Uffen, J., Guhr, N., y Breitner, M. H. (2012, diciembre 16-19). *Personality traits and information security management: An empirical study of information security executives* [Acta de congreso]. Thirty Third International Conference on Information Systems (ICIS 2012), Orlando, Estados Unidos. https://aisel.aisnet.org/icis2012/proceedings/ISSecurity/5/

Vishwanath, A., Herath, T., Chen, R., Wang, J., y Rao, H.R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems, 51*(3), 576-586. https://doi.org/10.1016/j.dss.2011.03.002

Washo, A. H. (2021). An interdisciplinary view of social engineering: A call to action for research. *Computers in Human Behavior Reports, 4*, 1-8. https://doi.org/10.1016/j.chbr.2021.100126

Weinstein, N. D., y Klein, W. M. (1996). Unrealistic Optimism: Present and Future. *Journal of Social and Clinical Psychology, 15*(1), 1-8. https://doi.org/10.1521/jscp.1996.15.1.1

Weirich, D., y. Sasse, M. A. (2001, septiembre 10-13). *Pretty good persuasion: a first step towards effective password security in the real world* [Acta de congreso]. New Security Paradigms Workshop 2001 (NSPW01), Cloudcroft, Estados Unidos. https://doi.org/10.1145/508171.508195

Whitty, M. T., y Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims - both financial and non-financial. *Criminology and Criminal Justice, 16*(2), 176-194. https://doi.org/10.1177/1748895815603773

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology, 59*(4), 66-674. https://doi.org/10.1002/asi.20779

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., y Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? *Computers in Human Behavior, 84*, 375-382. https://doi.org/10.1016/j.chb.2018.02.019

Zamorano Salardón, A. (2018). El factor humano en la fuga de información privilegiada y su relación con la personalidad. *Drafts of Economic Intelligence, 1*(2), 11-22. https://escuela-inteligencia-economica-uam.com/drafts-volumen-1-2018-2019/

Zuckerman, M., Kuhlman, D., Teta, P., Joireman, J., y Kraft, M. (1993). A Comparison of Three Structural Models for Personality: The Big Three, the Big Five, and the Alternative Five. *Journal of Personality and Social Psychology, 65*(4), 757-768. https://doi.org/10.1037/0022-3514.65.4.757