Grado de vulnerabilidad del factor humano en los sistemas de seguridad de la información

Quilachamín Untuña, Alexis Javier

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Trabajo de titulación previo a la obtención del título de Ingeniero en Tecnologías de la Información

Ing. Fuertes Díaz, Walter Marcelo, PhD.

01 de marzo de 2023

Revisión de plagio

Document Information

Analyzed document	Tesis_QuilachaminAlexis.pdf (D159774985)
Submitted	3/1/2023 11:42:00 AM
Submitted by	Ramiro Delgado
Submitter email	pg.docenterdr@uniandes.edu.ec
Similarity	1%
Analysis address	pg.docenterdr.unia@analysis.urkund.com

Sources included in the report

W	URL: https://neuroquotient.com/indicador-mbti-indicador-de-tipos-psicologicos-de-myers-briggs-herra... Fetched: 3/1/2023 11:42:00 AM	1
SA	**TESIS_INGSOCIAL_Version-Final 7 sept 21.docx** Document TESIS_INGSOCIAL_Version-Final 7 sept 21.docx (D112195818)	4
SA	**Chris_tesis_2nov.doc** Document Chris_tesis_2nov.doc (D58246889)	1
W	URL: https://www.lisainstitute.com/blogs/blog/diferencia-ciberseguridad-seguridad-informatica-segur... Fetched: 3/1/2023 11:43:00 AM	1
W	URL: https://socialsci.libretexts.org/Bookshelves/Psychology/Book%253A_Personality_Theory_in_a_Cult... Fetched: 3/1/2023 11:43:00 AM	1
SA	**M5.254_20221_PEC 3 - Cu les ser n mis datos?_18585711.txt** Document M5.254_20221_PEC 3 - Cu les ser n mis datos?_18585711.txt (D151911480)	1

Entire Document

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Certificación

Certifico que el trabajo de titulación: **"Grado de vulnerabilidad del factor humano en los sistemas de seguridad de la información"** fue realizado por el señor Quilachamín Untuña Alexis Javier; el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Sangolquí, 01 de marzo de 2023

WALTER MARCELO FUERTES DIAZ

Ing. Fuertes Díaz, Walter Marcelo, PhD.

C.C.: 1707017701

Responsabilidad de Autoría

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Responsabilidad de Autoría

Yo, **Quilachamín Untuña Alexis Javier**, con cédula de ciudadanía N.º 172535435-9, declaro que el contenido, ideas y trabajo de titulación: **"Grado de vulnerabilidad del factor humano en los sistemas de seguridad de la información"**, es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 01 de Marzo de 2023

Quilachamín Untuña Alexis Javier

C.C.: 1725354359

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Autorización de Publicación

Yo, **Quilachamín Untuña Alexis Javier**, con cédula de ciudadanía N.º 172535435-9, autorizo a la Universidad de las Fuerzas Armadas ESPE a publicar el trabajo de titulación: **"Grado de vulnerabilidad del factor humano en los sistemas de seguridad de la información"** en el Repositorio Institucional, cuyo contenido, ideas y criterios expuestos son de mi responsabilidad.

Sangolquí, 01 de Marzo de 2023

Quilachamín Untuña Alexis Javier

C.C.: 1725354359

Dedicatoria

Este trabajo es dedicado a mis padres Mirian y Cristóbal, quienes han sido el motor de mi vida y me han dado el ejemplo de sacrificio y calidad. Los amo demasiado.

Quilachamín Untuña Alexis Javier

Agradecimientos

A Mirian; mi madre, quien ha sido la persona que estuvo incondicionalmente a mi lado para no rendirme en ninguna circunstancia, siendo mi motor en cada paso.

A Cristóbal; mi padre, la persona que nunca ha dejado que me falte nada para continuar con mis estudios y mis actividades en general.

A los ingenieros Walter M. Fuertes D. y Mario B. Ron E., que me ha brindado su valioso tiempo, apoyo y conocimiento para el desarrollo de este trabajo. Por otra parte, agradezco a mis profesores que han tenido la voluntad de brindar su conocimiento a cada uno de sus alumnos y formarnos como personas de bien.

A la gloriosa Universidad de las Fuerzas Armadas ESPE, que forja profesionales de excelencia para un mejor futuro de nuestro Ecuador.

Quilachamín Untuña Alexis Javier

Índice de contenidos

Índice de Tablas

Índice de Figuras

Resumen

Dentro de los sistemas de información de una organización se puede aplicar múltiples métodos y controles técnicos que permitan garantizar la confidencialidad, integridad y disponibilidad de la seguridad de la información, sin embargo, en ocasiones no se toma en cuenta al eslabón más débil de los sistemas informáticos, las personas. Generalmente no se analiza a los seres humanos desde el aspecto psicológico el cual es un punto clave para que un delincuente informático pueda aprovechar y aplicar técnicas de ingeniería social para vulnerar los sistemas que tienen a cargo las posibles víctimas.

Por ello se ha generado un modelo de evaluación de personalidad en base a cuestionario para determinar el grado de vulnerabilidad del factor humano, este modelo ha sido definido en base a la investigación teórica y científica que comprende los aspectos psicológicos más relevantes de las personas para analizar los rasgos humanos presentes en cada individuo, estas características humanas son apertura a la experiencia, conciencia, extraversión, amabilidad, neuroticismo y honestidad / humildad y han sido definidas tomando como referencia al Modelo de los cinco grandes rasgos de personalidad, Modelo de Indicadores de Tipo de Myers-Briggs y el modelo HEXACO, los cuales son ampliamente utilizados y validados por la comunidad científica.

El modelo definido utiliza la escala de Likert para obtener los resultados del cuestionario, el cuál fue aplicado en una muestra poblacional correspondiente a docentes y estudiantes del Departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE en su campus Matriz. Los resultados generados por el modelo indican que el 89.09% de los evaluados tienen un grado de vulnerabilidad leve para convertirse en víctimas de ingeniería social y que el neuroticismo está más presente en estudiantes que en profesores con un 33.4% de diferencia.

Palabras clave: rasgos de personalidad, vulnerabilidad, factor humano, sistemas de información.

Abstract

Within the information systems of an organization, multiple methods and technical controls can be applied to guarantee the confidentiality, integrity and availability of information security, however, sometimes the weakest link in the systems is not taken into account. computers, people. Generally, human beings are not analyzed from the psychological aspect, which is a key point for a computer criminal to take advantage of and apply social engineering techniques to violate the systems that potential victims are in charge of.

For this reason, a personality evaluation model has been generated based on a questionnaire to determine the degree of vulnerability of the human factor, this model has been defined based on theoretical and scientific research that includes the most relevant psychological aspects of people to analyze. the human traits present in each individual, these human characteristics are openness to experience, conscientiousness, extraversion, agreeableness, neuroticism and honesty / humility and have been defined taking as reference the Model of the big five personality traits, Model of Type Indicators of Myers-Briggs and the HEXACO model, which are widely used and validated by the scientific community.

The defined model uses the Likert scale to obtain the results of the questionnaire, which was applied in a population sample corresponding to teachers and students of the Department of Computer Sciences of the University of the Armed Forces ESPE on its main campus. The results generated by the model indicate that 89.09% of those evaluated have a slight degree of vulnerability to become victims of social engineering and that neuroticism is more present in students than in teachers with a difference of 33.4%.

Key words: personality traits, vulnerability, human factor, information systems.

Capítulo I

Introducción

Dentro de una organización, su sistema información está conformado por tres componentes que son: hardware, software y recursos humanos, los cuales funcionan en conjunto para llevar a cabo las operaciones exitosas de la institución. Actualmente, la seguridad de la información en las organizaciones es un tema que ha conseguido un nivel de criticidad alto por el cual se desarrollan medidas técnicas y administrativas con el fin de reducir los riesgos que podrían acarrear las violaciones en los sistemas de información (Revnivykh & Fedotov, 2015). Por esta razón es que las vulnerabilidades en las tecnologías de la información representan un riesgo para preservar los tres principios de la seguridad de la información: confiabilidad, integridad y disponibilidad.

Como lo indican Conteh y Royer (2016): “La seguridad de una organización es tan fuerte como su componente más débil”. Dentro de los sistemas de información, las personas son denominadas como el eslabón o componente más débil (Conteh & Royer, 2016; Kennison & Chan-Tin, 2022), puesto que son fáciles de manipular ya que están sujetas a emociones que en ciertos casos evaden acciones lógicas. Esta debilidad psicológica juega con el comportamiento de la persona de desear algún tipo de aceptación, afecto o beneficio aprovechándose del deseo humano de ayudar al resto (Conteh & Royer, 2016) y pueden ser aprovechadas por individuos malintencionados al utilizar ataques de baja naturaleza técnica como la ingeniería social.

En base a lo mencionado, es importante analizar el comportamiento del factor humano en los sistemas de información para determinar su vulnerabilidad y modelar una herramienta que medirá el grado de vulnerabilidad que podría tener una persona que represente un riesgo en una organización o que constituya una amenaza a la seguridad de la información; para este caso particular, la herramienta va a ser aplicada al personal que forma parte del Departamento de Ciencias de la Computación (DCCO) de la Universidad de

las Fuerzas Armadas ESPE (UFA-ESPE) en su campus Matriz ubicado en Ecuador, provincia de Pichincha en el cantón Rumiñahui.

Planteamiento del problema

Generalmente, las organizaciones aplican múltiples evaluaciones, controles y soluciones para mitigar las brechas de seguridad que están presentes en sus sistemas; sin embargo, la mayoría de las prácticas utilizadas son netamente técnicas por lo que no consideran la franja de riesgos en los que intervienen las personas que manejan los sistemas de información.

La UFA-ESPE tiene a su disposición distintas medidas y controles para preservar la seguridad física de sus instalaciones y la seguridad de la información, sin embargo, no existe una herramienta que permita evaluar la esencia de las personas para clasificarlas como individuos que puedan o no representar una amenaza para la precautelar la disponibilidad, integridad y confidencialidad de la información, servicios y sistemas informáticos, más aun al considerar que la población de interés pertenece al área de computación e informática.

Aunque los usuarios de un equipo o sistema informático tengan buen dominio sobre las herramientas que manejan y que los equipos de seguridad de la información mantengan controles rigurosos sobre su infraestructura, no se puede dejar a un lado el hecho de que cada persona puede representar un riesgo de seguridad de la información al ser vulnerables ataques de ingeniería social, cuya incidencia ha incrementado por la llegada de la pandemia causada por COVID-19, esta vulnerabilidad puede ser aprovechada al depender de la personalidad que un individuo posea, el último aspecto mencionado no es evaluado técnicamente, sino más bien con instrumentos psicológicos que modelan la personalidad humana.

Justificación

Como se mencionó anteriormente, las organizaciones aplican distintos métodos técnicos, sin embargo, no se aplican otras medidas no técnicas que permitan evaluar la vulnerabilidad de las personas para ser víctimas de ingeniería social, que es el principal método de ataque que se aprovecha de las características personales de los seres humanos.

Es por esta razón que se pretende investigar, comprender y sintetizar la información disponible sobre los rasgos de personalidad que modelan el comportamiento de las personas y su relación con la vulnerabilidad que tienen las mismas para llegar a convertirse víctimas de ataques de ingeniería social que puedan comprometer los principios de seguridad de la información de una organización.

Además, se definirá una herramienta y un modelo de evaluación para determinar el grado de vulnerabilidad que tienen las personas para que un ataque de ingeniería social sea efectivo, esto se lo realizará al tomar en cuenta las cualidades psicológicas que presenta cada individuo; con esto, la UFA-ESPE tendrá a su disposición un modelo de evaluación de vulnerabilidades humanas con respecto a seguridad de la información, este modelo tiene definidas sus bases psicológicas con respaldo de profesionales en psicología.

Objetivos

Objetivo general

Analizar el comportamiento del factor humano en los sistemas de seguridad de la información, con el objeto de determinar sus vulnerabilidades y desarrollar mecanismos e instrumentos que permitan medir el grado y tipo de vulnerabilidad que podría tener una persona que gestione, desarrolle, instale, administre o utilice un sistema de información y que podría generar un riesgo para la organización o constituirse en una amenaza a la seguridad del sistema de información.

Objetivos específicos

- Establecer el estado del arte utilizando la Guía metodológica de Bárbara Kitchenham para identificar los trabajos relacionados, las teorías y el marco teórico referencial que fundamente este estudio.
- Definir las amenazas relacionadas con el comportamiento humano para describir la forma en que los atacantes pueden actuar y aprovecharse se las debilidades de las personas.
- Determinar las características psicológicas de las personas investigando modelos de personalidad válidos con el fin de conocer los rasgos humanos que favorecen a la victimización por delitos informáticos.
- Desarrollar un instrumento que permita medir el grado de vulnerabilidad que podría tener una persona que gestione, desarrolle, instale, administre o utilice un sistema de información.

Alcance

Para la investigación se pretende determinar el estado del arte referido a las características relacionadas a los rasgos de personalidad del factor humano en los sistemas de seguridad de la información, con el objeto de determinar sus vulnerabilidades y desarrollar mecanismos e instrumentos en base a cuestionarios psicológicos que permitan medir el grado y tipo de vulnerabilidad que podría tener una persona que gestione, desarrolle, instale, administre o utilice un sistema de información y que podría generar un riesgo para la organización o constituirse en una amenaza a la seguridad del sistema de información. La aplicación del estudio se realizará en la Universidad de las Fuerzas Armadas ESPE; en su campus Matriz, al personal docente y de estudiantes que forman parte del Departamento de Ciencias de la Computación.

Resultados esperados

El presente trabajo pretende determinar cuáles son las características de personalidad del ser humano que atenten a la seguridad de la información de una

organización y que un atacante pueda tomar ventaja para hacer efectivo un ataque de ingeniería social.

Con base a lo anterior, se propone definir un instrumento para medir; conforme a sus rasgos de personalidad, que tan vulnerables son las personas para que se conviertan en una amenaza a la seguridad de la información. En base a esto, se definirá una escala con la cual se clasificará a los individuos en distintos grupos de vulnerabilidad. Con esto, las organizaciones podrán tomar en cuenta controles y medidas adicionales con las cuales reducir la posibilidad de ocurrencia de un incidente de seguridad.

Capítulo II

Fundamentación teórica y estado del arte

Fundamentación teórica

Para el desarrollo de este trabajo es fundamental tener el conocimiento de los conceptos principales relacionados a la seguridad de la información, activos de información, las vulnerabilidades en el factor humano, los ataques que pueden aprovechar estas vulnerabilidades; además, las características psicológicas y comportamiento de las personas y la relación que puede existir para que un atacante pueda aprovechar estas características y concretar un ataque de ingeniería social.

Seguridad informática

De forma general, al hablar de seguridad su significado hace referencia a la ausencia de peligro, afectación o cualquier riesgo en determinada situación; aunque en la realidad, no hay una inexistencia absoluta de riesgos, sin ellos no existiría la seguridad (Equipo de GWC, s.f.).

Refiriéndose a las tecnologías de la información, la seguridad informática se describe como la disciplina que opera sobre la infraestructura y sistemas informáticos, que tiene por objetivo protegerlos, al tratar de preservar la integridad y privacidad de la información que es contenida y procesada en dicha infraestructura, por lo que es un componente táctico y operacional de seguridad para garantizar las operaciones de una organización (Equipo de ISOTools Excellence, 2017).

Seguridad de la información

La información de una organización es procesada, almacenada y transmitida de manera electrónica, física o verbalmente (Equipo de LISA Institute, 2021).

La seguridad de la información es un campo más amplio, el cual se encarga de proteger los datos e información que una organización genera, esto se logra al implementar medidas y políticas que garanticen el tratamiento adecuado de la información (Equipo de LISA Institute, 2021).

En seguridad de la información se evalúa vulnerabilidades, amenazas y riesgos que están presentes en el entorno y que se relacionan con los activos de una institución, con lo cual se definen medidas preventivas y reactivas para proteger los datos que se encuentren en una base de datos, un archivador e incluso en las personas pertenecientes a una organización, con el objetivo de precautelar la confidencialidad, integridad y disponibilidad de los datos.

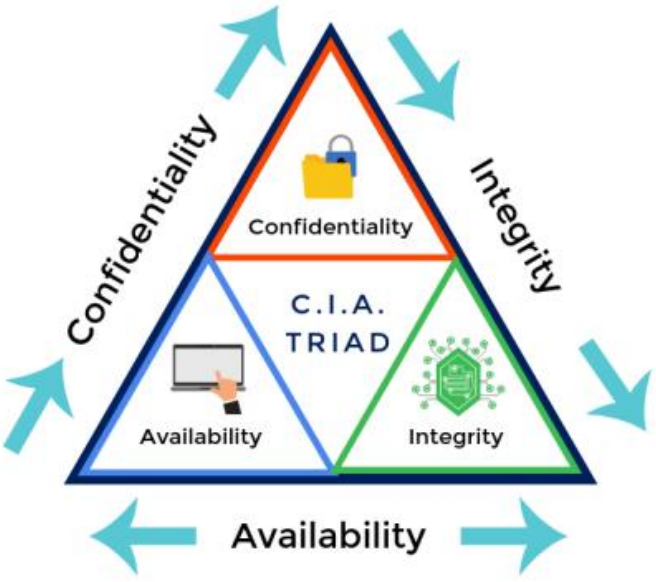
Principios de seguridad de la información

Con el fin de proteger la información ante amenazas tanto internas como externas, es importante tomar en cuenta los denominados principios o pilares de la seguridad de la información, que son: confidencialidad, integridad y disponibilidad Figura 1.

Estos principios son definidos en base a la necesidad que se genera para acceder a la información y su valor. Si alguno de estos principios se ve comprometido, la información perderá seguridad.

Figura 1

Principios de seguridad de la información.



En el caso que falte alguno de estos principios, una organización se verá expuesta a ataques que afecte a los recursos económicos, informáticos, humanos e incluso la reputación de la empresa (Romero Castro, y otros, 2018).

A continuación, se describe cada uno de los principios fundamentales en seguridad de la información.

Confidencialidad. Este principio se refiere a que la información debe ser accesible únicamente por usuarios que sean autorizados, con lo cual un sistema o usuario únicamente accederá a los recursos a los que tenga permisos (Romero Castro, y otros, 2018). Para cumplir este principio, se recurre a las siguientes acciones:

- **Autenticación de usuarios:** sirve para que el usuario se identifique y comprobar que quién accede, es quien dice ser.
- **Gestión de roles y privilegios:** es utilizado para que los usuarios únicamente accedan a la información que se le ha autorizado y únicamente con los permisos necesarios; ya sean, de lectura o escritura.
- **Cifrado de información:** la información almacenada o transmitida es convertido de un formato legible a uno no legible, y puede ser aplicada a información que esté o no autorizada y solamente con un sistema de contraseñas se puede extraer el contenido original de los datos.

La información puede ser de carácter confidencial no solo por tener un alto valor para una organización, sino también a que dicha información puede estar bajo el amparo de la legislación de cada país.

Integridad. El segundo principio responde a que la información no se va a perder ni será alterada de manera errónea al momento de su uso. La manipulación de datos puede desencadenar eventos sucesivos para una posterior toma de decisiones equivocadas, por lo cual se debe tomar en cuenta lo siguiente:

- Monitorear y controlar el tráfico de red ante intrusiones.
- Implantar políticas de auditoría para registrar los eventos ocurridos con los datos.
- Definir sistemas de control de cambios para comprobar la modificación de la información.

- Mantener copias de seguridad para restaurar la información original si ha existido manipulación o pérdida de la misma.

Disponibilidad. El último principio fundamental es aplicado para la información o los sistemas sean accesibles en cualquier momento que un usuario autorizado desee acceder. Para garantizar este principio, se puede implementar políticas de control, como:

- Acuerdo de nivel de servicio con proveedores de servicios.
- Balanceadores de carga para minimizar el impacto ante la pérdida de servicios.
- Respaldos de los datos para su restauración.
- Recursos alternos para cuando los principales fallen.

Al aplicar de manera adecuada estos tres principios se tendrá información y sistemas seguros, los cuales serán accedidos en cualquier momento por personas autorizadas y que; a lo largo de su uso, será información consistente.

Además de la inversión en aspectos tecnológicos, las organizaciones deben asignar recursos económicos para la enseñanza de seguridad de la información a los usuarios (Teruel, 2021), dado que una parte de los incidentes de seguridad resultan exitosos al aprovecharse del error humano.

Activos de información

Los activos de información son un conjunto de elementos que tienen valor para una organización y que debe protegerlos (Equipo de REDVOISS, 2021) para que cumpla los objetivos de negocio, retorne la inversión realizada y genere ganancias. Dentro de los activos de información se incluyen activos tangibles e intangibles que al verse comprometidos generan pérdidas económicas, de reputación, entre otras (Equipo de Black Swan Security, 2020).

Tipos de activos de información

Como se mencionó anteriormente, los activos de información se encuentran en forma tangible o intangible.

Activos tangibles. Los activos que se encuentran en esta clasificación están representados de forma física. Dentro de estos activos se pueden mencionar los siguientes:

- Equipos tecnológicos para almacenamiento de datos.
- Equipos informáticos como smartphones, tablets, computadoras o servidores.
- Infraestructura de comunicación y transmisión de datos.
- Bienes inmuebles en donde reside la organización.
- Contenedores de información como: armarios, archivadores, cajas fuertes, centros de datos, entre otros.
- Las personas que generan y utilizan la información dentro de una organización.

Activos Intangibles. Estos activos no pueden ser percibidos físicamente, por lo que tienen una naturaleza inmaterial. A continuación, se define un listado de algunos ejemplos de esta clase de activos.

- Datos que son almacenados, utilizados y modificados.
- Aplicaciones y programas para generar y manipular datos.
- Sistemas operativos y sus licencias respectivas.
- Copias de seguridad de los datos.
- Suministro eléctrico, servicio telefónico y de internet.
- Imagen, confianza y reputación de la organización.

Vulnerabilidades en la seguridad de la información

En el contexto de informática, una vulnerabilidad es considerada como un fallo o debilidad que tiene un sistema de información el cual pone en riesgo la seguridad del mismo. Se puede decir que es una brecha la cual puede ser producida por una incorrecta configuración, falta de controles en los procesos o un diseño deficiente (Equipo de AMBIT, 2020).

Las vulnerabilidades en un sistema son las principales razones por las cuales una organización se puede ver expuesta a ataques informáticos; los cuales, violan los principios de confidencialidad, integridad y disponibilidad de los sistemas y la información.

En toda infraestructura informática de las empresas existe; aunque mínimo, algún error en su diseño, estructura o código los cuales pueden generar alguna vulnerabilidad que pueda ser aprovechada como una puerta para sufrir ataques informáticos por atacantes, tanto externos como internos, a estos últimos se los debe prestar mayor atención, dado que son individuos que tienen; de alguna manera, acceso directo a la información.

Dado que el presente trabajo se enfoca en el factor humano, los siguientes temas serán abordados en torno a este aspecto para no desviar la atención y seguir el curso de la investigación.

Vulnerabilidades en el factor humano

Según lo expuesto por Cortez Pinto (2013), la vulnerabilidad humana responde a la exposición de las personas a un ataque con el que se roba datos confidenciales para obtener acceso a un sistema de información y concretar ataques hacia los mismos. Esta vulnerabilidad es uno de los puntos más importantes de este estudio, ya que influye y da paso a un entendimiento más completo del comportamiento de las personas que podrían violar la seguridad de los sistemas informáticos.

Debido al exponencial crecimiento en el uso de los servicios en línea tales como comercio, salud, educación, entre otros, las transacciones y el número de ataques informáticos también han tenido una tendencia incremental de ocurrencias (Benavides-Astudillo, y otros, 2022). De acuerdo con Anaya (2021), los equipos de seguridad de la información han enfocado sus esfuerzos para proteger a los usuarios en entornos remotos, los cuales se ven expuestos a ciberataques.

Dado que en 2020 los ciberdelincuentes tuvieron éxito en efectivizar ataques, sus esfuerzos van a ser orientados a usuarios individuales con técnicas más elaboradas para extraer credenciales e información crítica para afectar a una empresa.

Por otra parte, Arroyo Siruela (2021) menciona que una de cada cinco brechas de seguridad es originada por un empleado que realizó alguna acción de forma inconsciente. Se debe prestar cierto cuidado en el factor humano, dado que las personas son elementos fundamentales en cada proceso de una organización.

Andrade, Cazares, & Fuertes (2021) indican que con la llegada de la pandemia por COVID-19 las vulnerabilidades en el factor humano han aumentado debido a la aparición de noticias falsas, puesto que generan fatiga cognitiva sobre la forma en que las personas procesan esa información y podría cambiar la percepción de lo que consideran verídico o información falsa.

El factor humano como el eslabón más débil

Dado que las personas son las encargadas de administrar y utilizar cualquier sistema de información, los individuos serán considerados como uno de los componentes en la cadena de seguridad. Conteh & Royer (2016) mencionan que las personas son el eslabón más débil de esta cadena. Suelen ocurrir descuidos que, por falta de información o exceso de confianza, generan múltiples oportunidades para comprometer la seguridad en los sistemas al momento de instalar software malicioso o revelar información confidencial (Equipo de Aprender compartiendo, 2017).

Los empleados dentro de una organización pueden convertirse en un problema, dado que la pérdida de datos puede originarse por imprevistos, ignorancia o el deseo de encajar con sus compañeros.

Pueden existir empleados malintencionados que por ambición o descontento dan paso; con mayor facilidad, a ataques informáticos, ya que tienen acceso a los equipos e información sensible que puede perjudicar a la empresa con graves consecuencias de reputación y económicas.

Cortez Pinto (2013) indica que analizar las causas de la vulnerabilidad en el factor humano responde a los principios definidos por Kevin Mitnick, los cuales son:

- Todos queremos ayudar.
- La primera acción es de confiar en otra persona.
- Nos gusta que nos elogien.
- No nos gusta decir no.

En base a estos principios, generalmente las vulnerabilidades se ven atraídas por la falta de capacitación de las personas sobre los potenciales inconvenientes y perjuicios a los que exponen a una empresa o incluso a sí mismos.

Existen múltiples ataques informáticos que aprovechan las vulnerabilidades existentes en los activos de información.

Para la pertinencia de este trabajo se tiene en cuenta un grupo de ataques que son el principal vector que atenta a la seguridad de la información y se aprovecha de las vulnerabilidades humanas, a este tipo de ataques se los denomina como Ataques de Ingeniería social.

Ingeniería social en ataques informáticos

Desde de una perspectiva bíblica e histórica, la ingeniería social puede ser apreciada en el libro de Génesis; en donde, el diablo en forma de serpiente manipuló a Eva para que coma el fruto del árbol prohibido. Otro hecho histórico que se pone de ejemplo es el denominado Caballo de Troya. La ingeniería social existe desde que el ser humano aprendió formas de manipulación y persuasión (Borkovich & Skovira, 2019).

El término de ingeniería social tiene múltiples definiciones en términos de ciencias políticas y sociales. En torno a la seguridad, la ingeniería social hace referencia a ser una herramienta con la que se engaña a las personas para que actúen de alguna forma o renuncien a algo que de otro modo no lo harían, esto se consigue mediante trucos psicológicos (Conteh & Royer, 2016).

En su libro, Mitnick & Simon (2002); dentro del contexto de informática, definen a la ingeniería social como una técnica que “utiliza la influencia y la persuasión para engañar a las personas convenciéndolas de que un atacante es alguien que no es, o mediante manipulación. Como resultado, el atacante es capaz de aprovecharse de las personas para obtener información con o sin el uso de la tecnología”.

Figura 2

Ejemplificación de ingeniería social.

¿Qué son los ataques de ingeniería social?

Al referirse en el ámbito de la seguridad informática, los ataques de ingeniería social son definidos como un tipo de ataque en el cual un atacante se aprovecha de las vulnerabilidades de las personas mediante aspectos psicológicos como la influencia, el engaño, la persuasión, la inducción y manipulación (Figura 2); esto, con el fin de obtener información confidencial, sabotear un sistema de información, obtener credenciales de acceso, esto lo consigue al violar los principios de confidencialidad, integridad y disponibilidad de los servicios y la información (Wang, Zhu, & Sun, 2021).

Stergiou (2013) hace una recopilación de definiciones que múltiples autores definen como ingeniería social, con lo cual rescatan los siguientes enunciados:

- Es una técnica que explota la vulnerabilidad humana.
- Es el arte de explotar el eslabón más débil de los sistemas de seguridad de la información.
- Obtiene cierta cantidad de información para más tarde utilizarla en un ataque técnico.

La ingeniería social se enfoca en romper las barreras de seguridad que tenga un sistema informático, sin la necesidad de combatir contra los controles técnicos, como firewalls o software antivirus.

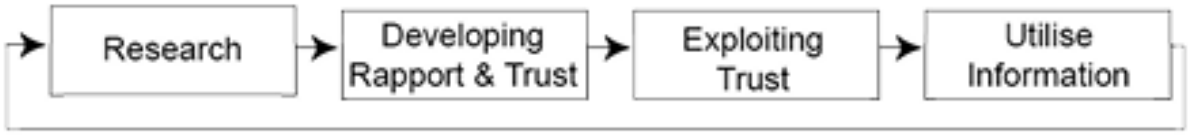
Aunque una organización tenga las tecnologías más actuales de seguridad y que sus colaboradores sigan las mejores prácticas, ambos van a ser completamente vulnerables (Mitnick & Simon, 2002). El factor humano es un componente inevitable y vulnerable que también es denominado como una amenaza universal (Wang, Zhu, & Sun, 2021).

Existen múltiples ataques de ingeniería social que los atacantes utilizan para manipular a los usuarios y pedir datos confidenciales, para luego infectar sus equipos con software malicioso, abrir páginas web fraudulentas o actuar de una forma en particular, esto se logra al engañar al individuo haciéndole pensar que es algo confiable y seguro.

En Figura 3 se puede observar el ciclo de operación de un ataque de ingeniería social según el trabajo realizado por Kevin Mitnick.

Figura 3

Ciclo de ataque de ingeniería social de Kevin Mitnick.



A continuación, se explicará de forma breve cada una de las etapas del ciclo mostrado anteriormente:

- **Investigación:** es el proceso para reunir información de varias formas sobre la potencial víctima, para que se adapte una estrategia de ataque.
- **Desarrollo de la relación y confianza:** se basa en utilizar información privilegiada, al suplantar una identidad haciéndose pasar por personas conocidas por la víctima o una autoridad.
- **Explotación de la confianza:** el atacante abusa del vínculo generado anteriormente para obtener información confidencial o que la víctima realice alguna acción en particular.
- **Utilización de información:** con la información proporcionada, el atacante podrá continuar con otros pasos la cumplir con su objetivo final (Mouton, Malan, Leenen, & Venter, 2014).

Tipos de ataques informáticos que utilizan ingeniería social

En esta sección se describen algunos de los principales ataques informáticos que utilizan técnicas de ingeniería social.

- **Phishing:** el atacante; disfrazado de una entidad de confianza, se contacta por algún medio electrónico con una víctima para obtener información o hacer que realice una acción, el principal medio de comunicación utilizado es el correo electrónico, en el cual se adjunta enlaces a páginas web similares a un sitio oficial de una organización, pidiéndole que verifique datos privados sensibles (Banco Pichincha, 2020). Esta forma de ataque varía de acuerdo con el medio que el atacante se contacte, en base a esto, se tiene:
    - **Vishing:** es una estafa mediante llamadas telefónicas o de VoIP. Generalmente, el atacante solicita información confidencial sobre número de tarjetas o credenciales al utilizar manipulación en torno a empatía o miedo.
    - **Smishing:** este ataque utiliza mensajes de texto o mensajería instantánea para remitir a la víctima enlaces de sitios web fraudulentos para instalar software malicioso en su dispositivo o solicitar datos confidenciales.

      Por el objetivo de ataque también se tiene el spear phishing, se enfoca a una víctima en particular, a diferencia del phishing que se dirige a un público en general. El atacante necesita recopilar información más a detalle de la víctima para planificar su ataque.
- **Pretexting:** el atacante se hace pasar por una autoridad legítima y para engañar a sus víctimas crea escenarios al inventar historias o pretextos convincentes para que provean información o acceso (Perallis Security, s.f.).

- **Dumpster diving:** es la técnica que busca información sensible en la basura de las compañías o los colaboradores con lo cual perjudicar un sistema o a un usuario en particular (Krombholz, Hobel, Huber, & Weippl, 2014).
- **Shoulder surfing:** se basa en espiar el teclado o la pantalla de un individuo para obtener algún tipo de información con el que pueda perjudicar al individuo, en ocasiones el usuario malintencionado puede obtener credenciales de acceso a los sistemas (Krombholz, Hobel, Huber, & Weippl, 2014).
- **Ingeniería social inversa:** es un tipo de ataque en el que el atacante y su víctima llegan a crear una relación, el atacante crea una situación en que la víctima requiere ayuda y el atacante se presenta como su solución a cambio de obtener información confidencial (Krombholz, Hobel, Huber, & Weippl, 2014).
- **Baiting:** los atacantes dejan un dispositivo electrónico en un sitio accesible para todos, para que algún individuo lo recoja y conecte a su computadora, al conectarlo en el equipo se podría infectar con software malicioso (Bodnar, 2022).
- **Scareware:** los atacantes cargan ventanas emergentes en sitios web los cuales notifican a las potenciales víctimas que su dispositivo tiene algún tipo y que al hacer clic en la ventana eliminará el virus informático, al caer en este engaño, la ventana puede redirigir a un sitio malicioso o instalar software no deseado sin que el usuario se dé cuenta (Bodnar, 2022).

Estos ataques pueden ser utilizados por los atacantes tomando como ventaja la necesidad de que las personas utilicen las redes sociales para recibir, crear y compartir información. El victimario tratará de aprovechar este escenario para persuadir y manipular a una víctima para convencerla de una idea o acción a realizar (Andrade, Cazares, & Fuertes, 2021).

De forma similar, Fuertes y otros (2022) aclaran que las personas publican mayor cantidad de información a cada momento, que puede ser utilizada por los criminales con el

objetivo de crear cebos o anzuelos que resulten llamativos para las potenciales víctimas y que revelen información de carácter crítico y confidencial.

La vulnerabilidad a los ataques de ingeniería social está basada en el comportamiento e impulsos humanos, además de características de personalidad, por esta razón es importante comprender los aspectos psicológicos en ingeniería social, con el fin de educar a los individuos para concientizar sobre la identificación y defensa de estos tipos de ataques.

Rasgos de personalidad del ser humano

Como lo exponen Erbasi, Caliskan, & Akdeniz (2022), los rasgos de personalidad son un importante tópico de investigación en el campo de la psicología. Es por ello que su estudio está relacionado a distintos campos de la ciencia.

Así mismo, dentro de múltiples estudios empíricos los rasgos de personalidad son un elemento que modela la conducta y el comportamiento de las personas. Se trata de cualidades distintivas y propias de cada persona y aunque existen varios tipos de personalidades, cada persona es única y por ende su personalidad también lo es (Ruiz Mitjana, 2019).

Por esta razón, la personalidad se puede definir como un conjunto de características estables y funcionales, que están presentes en las personas desde su nacimiento y que además son adquiridas en cada situación a lo largo de la vida de cada individuo, en conjunto definen la conducta o comportamiento de cada individuo en distintas situaciones (Ruiz Mitjana, 2019).

Además, la personalidad del ser humano viene determinada por múltiples rasgos psíquicos, morfológicos y fisiológicos que se interrelacionan.

Montañez, Golob, & Xu (2020) mencionan que la personalidad de la gente es relativamente consistente a lo largo del tiempo y las circunstancias, dado que los pensamientos, sentimientos y su comportamiento son dependientes del entorno en que se encuentren y las situaciones que hayan afrontado conforme envejecen.

Componentes de la personalidad

La personalidad de los seres humanos tiene dos componentes fundamentales que son: el temperamento y el carácter.

Temperamento. Este elemento es adquirido desde el nacimiento dado que lo poseen por herencia genética que define varios rasgos y cualidades fisiológicas en el cuerpo del individuo. El temperamento es una característica al natural que se afina y determina la personalidad de una persona.

Carácter. Este componente es adquirido en base al día a día de la persona, el cuál llega a ser más cambiante. Es influenciado por las vivencias, educación, entorno de crecimiento y la cultura en la que el individuo haya vivido. Al ser una característica volátil; cualquier experiencia que la persona haya tenido hará que su comportamiento sea variante. Con el pasar del tiempo el carácter puede acentuarse de forma positiva con lo que la persona madura y crece emocionalmente, por el contrario, si es de forma negativa, el individuo puede llegar a sufrir y traumatizarse (Equipo de Psicología y vida, 2013).

Modelos de personalidad

Para determinar los rasgos de personalidad de la gente existen múltiples modelos aceptados por la comunidad científica, dentro de los cuales se encuentran el Modelo de los Cinco Grandes o Modelo de los Cinco Factores (FFM) el cual fue definido por los investigadores Robert McCrae y Paul Costa (Kelland, 2020), por otra parte, se tiene el modelo de Indicadores de Tipo de Myers-Briggs (MBTI) y el modelo HEXACO, el cual es una variante del FFM.

Modelo de los Cinco Grandes Rasgos de Personalidad

El propósito de este modelo es identificar los principales rasgos de personalidad que tiene cada individuo. El modelo está compuesto por cinco rasgos de personalidad distintos que son:

- Apertura a la experiencia → Openness to experience.
- Conciencia → Conscientiousness.

- Extraversión → Extraversion.
- Amabilidad → Agreeableness.
- Neuroticismo → Neuroticism.

A continuación, se describe cada uno de los rasgos de personalidad del Modelo FFM en base a la literatura encontrada para este fin.

Apertura a la experiencia. Este rasgo hace referencia a la intención que una persona tiene una mentalidad abierta a aprender e interactuar con nuevas experiencias e ideas; así mismo, acepta las distintas creencias que tienen sus semejantes. Los individuos que tienen un mayor nivel de apertura sienten apreciación positiva por el arte, dado que tienen una mayor imaginación y curiosidad por aventuras (Papatsaroucha, Nikoloudakis, Kefaloukis, Pallis, & Markakis, 2021). Por el contrario de quienes obtuvieron un nivel inferior, se sienten cómodos con su rutina y no sienten deseo por experimentar nuevas cosas.

Conciencia. También hace referencia a escrupulosidad, el rasgo de personalidad en cuestión es asociado a la honestidad, confianza, respeto (Papatsaroucha, Nikoloudakis, Kefaloukis, Pallis, & Markakis, 2021), autocontrol y orden, lo cual hace que las personas sean confiables y trabajadoras (Halevi, Lewis, & Memon, 2013).

A pesar de ello, un alto nivel de conciencia se puede interpretar como exceso de trabajo y obsesión por la limpieza (Halevi, Lewis, & Memon, 2013).

Extraversión. Está relacionado con habilidades sociales, por lo que se adaptan con facilidad al estar en grandes grupos de personas, esto lo logran al ser entusiastas, amigables, comunicativos y enérgicos. Las personas con bajo nivel de extraversión son denominadas introvertidas, lo cual hace que sean más reservadas y están cómodas en grupos pequeños (Halevi, Lewis, & Memon, 2013).

Amabilidad. Las personas con este rasgo son consideradas agradables dado que tienen la voluntad de ayudar al resto y creen en la reciprocidad, ya que tienen en cuenta el lado bueno de los demás (Halevi, Lewis, & Memon, 2013). Aquellas personas con un nivel bajo en este rasgo, son denominadas como competitivas y egocéntricas.

Neuroticismo. Este rasgo es característico de personas que tienden a experimentar sentimientos negativos como culpa, tristeza, miedo, asco e ira (Papatsaroucha, Nikoloudakis, Kefaloukis, Pallis, & Markakis, 2021). Al tener puntuaciones bajas, los individuos tienen estabilidad emocional; de lo contrario, no suelen tener pensamientos racionales y tampoco controlan sus impulsos ni el estrés.

En Tabla 1 se puede observar una clasificación de las características de los rasgos de personalidad que depende de un puntaje alto o bajo para cada rasgo.

Tabla 1

Resumen de las características de cada rasgo de personalidad

Rasgo	Puntuación alta	Puntuación baja
Apertura a la experiencia	Curioso, imaginativo, intelectual	Rutinario, escéptico, conservador
Conciencia	Organizado, fiable, minucioso	Negligente, no fiable, descuidado, Desorganizado, propenso a adicción
Extraversión	Activo, asertivo, locuaz, extrovertido, activo, curioso	Distante, tranquilo, precavido, reservado
Amabilidad	Confiado, amistoso, empático, afable, obediente	Hostil, antipático, egoísta, desconfiado
Neuroticismo	Malhumorado, nervioso, temperamental, estresado	Emocionalmente estable, tranquilo, seguro

Indicadores de Tipo Myers-Briggs (MBTI)

Este modelo de personalidad fue creado por Katharine Cook Briggs y su hija Isabel Briggs Myers. Su modelo fue basado en una investigación teórica realizada por Carl Jung sobre Tipos psicológicos que fue publicado en 1921. Carl Jung indica que las distintas formas de ser y la conducta de las personas son basadas en la percepción y el juicio, lo cual determina su comportamiento y toma de decisiones (Calbet, 2017).

En este modelo se plantean cuatro grandes grupos para determinar la personalidad de un individuo, estos rasgos son:

- **Extraversión/intraversión:** las personas se diferencian por la forma en que se desenvuelven en su entorno.
- **Sentido/Intuición:** determina la manera en que los individuos recopilan o consiguen información o conocimiento.
- **Pensamiento/Sentimiento:** indica la manera en que los seres humanos toman decisiones o emiten juicios de una situación en particular.
- **Juicio/Percepción:** este rasgo define la manera en que las personas eligen seguir o cambiar el rumbo de sus vidas.

En Figura 4 se puede observar las características que tiene cada rasgo de personalidad del modelo MBTI.

Figura 4

Rasgos de personalidad del MBTI.

Modelo de personalidad HEXACO

El modelo de personalidad HEXACO fue diseñado por los investigadores Kibeom Lee y Michael Ashton. Las bases teóricas de este modelo son fundamentadas en el Modelo de los cinco factores de Paul Costa y Robert McCrae.

Su nombre es derivado de las siglas en inglés de cada rasgo de personalidad que lo componen. HEXACO es considerado como uno de las principales herramientas para

determinar el los rasgos de personalidad y el comportamiento de las personas. Algunos estudios se enfocaron en determinar la personalidad de profesionales académicos.

Este modelo se está conformado por seis rasgos de personalidad dominantes en las personas, dentro de estos se encuentra: Honestidad/Humildad, Emocionalidad, Extraversión, Amabilidad, Conciencia y Apertura a la experiencia (van Winsen, 2020).

Según van Winsen (2020) los autores de HEXACO indican que este modelo tiene un desempeño superior a diferencia del modelo de cinco factores, debido a que integra el rasgo de Honestidad/Humildad el cual permite determinar comportamientos inmorales y de auto-mejora. En el mismo trabajo se menciona que en al integrar este rasgo se capturan características de integridad y egoísmo.

A continuación, se describe el comportamiento de las personas en base a una puntuación alta o baja en cada rasgo de personalidad.

Honestidad / humildad. Al tener un puntaje alto en este rasgo, una persona evita manipular al resto, tiene pocas intenciones de romper reglas, no sienten tener privilegios por su estatus social ni tampoco están interesados en lujos y riquezas. Por el contrario; con un puntaje bajo, son capaces de violar normas por obtener beneficios personales, están interesados en ser aprobados socialmente y tener ganancias materiales (Lee & Ashton, s.f.).

Emocionalidad. Las personas con un alto nivel de emocionalidad suelen tener miedo a peligros físicos, lo cual conlleva a tener ansiedad. Además, se preocupan por ayudar a sus semejantes, son empáticos y sentimentales. Al tener un nivel bajo de emocionalidad no sienten desánimo por un daño físico, son despreocupados ante situaciones de estrés y se cohíben en expresar sus preocupaciones. Son emocionalmente distantes (Lee & Ashton, s.f.).

Extraversión. Con una escala alta de extraversión, las personas se sienten cómodas en desenvolverse en grupos de personas, además que disfrutan las interacciones sociales y experimentan entusiasmo y energía. Por otro lado, con un nivel bajo de este rasgo, los individuos son impopulares y sienten incomodidad al ser el centro de atención

social, no cooperan en actividades sociales, no son tan optimistas ni animadas (Lee & Ashton, s.f.).

Amabilidad. Cuando tienen un puntaje alto, las personas suelen perdonar errores de los demás, son indulgentes, son comprometidos y colaboradores, además controlan de buena manera su temperamento. Por otro lado, al tener un puntaje bajo van a guardar rencor a quienes les han perjudicado, son fuertemente críticos con las falencias del resto y se cierran a ideas contrarias a su punto de vista (Lee & Ashton, s.f.).

Conciencia. Con una puntación alta, las personas trabajan de manera disciplinada para cumplir objetivos, buscan precisión y eficiencia para sus actividades; además, son cuidadosos en tomar decisiones. Por el contrario, las personas con puntuaciones bajas son despreocupadas por el orden y horarios, además que evitan tareas desafiantes, si algún trabajo presenta errores son conformistas y toman decisiones por impulso o sin reflexionar en las consecuencias de su falta de ética y moralidad (Lee & Ashton, s.f.).

Apertura a la experiencia. Las personas con puntuación alta son buenos apreciadores del arte y la naturaleza, se interesan por aumentar su conocimiento, son imaginativos y se interesan por pensamiento y personas inusuales. Por otro lado, quienes tienen un bajo nivel de este rasgo, no se impresionan con el arte y tienen poca curiosidad por cosas nuevas, no son creativos y se sienten desinteresados por ideas nuevas o inusuales (Lee & Ashton, s.f.).

Estado del Arte

Para el presente trabajo se ha realizado la búsqueda de información que haga referencia a la relación existente entre los rasgos de personalidad y la vulnerabilidad del factor humano a ataques de ingeniería social en el contexto de la seguridad de la información de una organización.

Para la recopilación de información importante relacionada al tema se hará uso de la guía metodológica propuesta por Kitchenham y otros (2009) para ello se ha considerado las etapas de definición de las preguntas de investigación, búsqueda de artículos relevantes,

selección de estudios primarios, análisis de resúmenes y palabras clave y mapeo de los estudios primarios seleccionados.

Planteamiento de la revisión de literatura preliminar

Esta revisión de literatura tiene por objetivo determinar los parámetros apropiados para desarrollar el estado del arte, por lo que se realiza:

Definición de las preguntas de investigación. El presente trabajo pretende identificar y determinar los rasgos de personalidad principales que influyen en el comportamiento humano para determinar qué tan vulnerable es una persona para ser víctima de ataques de ingeniería social, bajo esta premisa se define la siguiente pregunta: ¿Cuáles son los rasgos o características de personalidad relacionados con la facilidad de que un ataque de ingeniería social sea efectivo? Bajo esta pregunta se resumirá la información disponible que vincula ciertos aspectos psicológicos que definen a una persona y el arte de la explotación de vulnerabilidades de la psicología humana.

Búsqueda de artículos relevantes. En esta etapa se definieron los principales términos para la obtención de artículos científicos relacionados al tema del presente trabajo. Para ello se ha hecho uso del motor de búsqueda de documentos académicos Google Scholar, en el cual se ha hecho uso de la siguiente cadena de búsqueda: ("personal characteristics" OR "behavior" OR "personality traits") AND ("threat" OR "vulnerability" OR "risk") AND ("social engineering") AND ("information systems" OR "cybersecurity"); donde, el conector OR permite buscar términos similares y AND posibilita enlazar términos distintos.

En esta etapa se definió los criterios de inclusión, exclusión y calidad de los artículos que deben tener los resultados de la búsqueda realizada para ser considerados como artículos válidos. Para este paso se seleccionaron trabajos que cumplan con los siguientes criterios de inclusión:

- Trabajos cuyo título contenga al menos dos términos distintos presentes en la cadena de búsqueda.

- Trabajos que utilicen los rasgos de personalidad para evaluar la vulnerabilidad en la seguridad de la información.
- Trabajos que fueron desarrollados entre 2013 y 2022.
- Trabajos publicados en idioma inglés.
- Trabajos disponibles en texto completo.

Así mismo, se descartó los trabajos que cumplan con al menos un criterio de exclusión de los expuestos a continuación:

- Trabajos cuyo título se mencione uno o ningún término de los definidos en la cadena de búsqueda.
- Trabajos publicados antes de 2013.
- Trabajos publicados en un idioma distinto al inglés.
- Trabajos donde se expongan definiciones de los términos de la cadena de búsqueda.

Resultado de la selección de estudios primarios. Una vez obtenidos los artículos que cumplan con los criterios de inclusión y exclusión mencionados anteriormente, se tuvo un total de 75 artículos preliminarmente aptos. De los cuales se eliminaron siete duplicados. Posteriormente, se hizo la lectura completa de los resúmenes, donde se descartaron 56 por no tener relación cercana al tema del presente trabajo y de los artículos restantes se hizo la lectura completa, con lo cual se obtuvo un total de siete artículos considerados como aptos para establecer el estado del arte.

Resumen de estudios primarios

A Pilot Study of Cyber Security and Privacy Related Behavior and Personality Traits (Halevi, Lewis, & Memon, 2013)**.** Este estudio evalúa la relación existente entre los 5 grandes rasgos de personalidad y la respuesta a correos electrónicos de phishing. Además, los autores examinan en qué medida estos aspectos se involucran con el comportamiento en Facebook.

Los autores encontraron que existe una correlación alta entre el neuroticismo y las mujeres vulnerables a phishing. Así mismo, determinaron que las personas que navegan en Internet con mayor frecuencia aumentan su conciencia sobre las amenazas y riesgos en línea. El neuroticismo fue directamente relacionado a la adicción a Internet y que dicha adicción es inversamente correlacionada con la conciencia.

Por último, encontraron que la apertura está relacionada a la cantidad y tipo de publicaciones que las personas realizan y a una configuración de privacidad débil con restricciones limitadas, los resultados indican que quienes publican mayor cantidad información en Facebook tienen mayor riesgo de que su información sea filtrada; disfrutan el uso de la aplicación, sin embargo, no toman en cuenta el riesgo de su comportamiento.

Social Engineering in the Context of Cialdini psychology of persuasion and personality traits (Quiel, 2013)**.** El trabajo en mención toma en cuenta los principales rasgos de personalidad y su relación con los principios de persuasión propuestos en la psicología de Cialdini. El autor indica que, hasta la fecha de publicación de su trabajo, la relación entre los rasgos de personalidad y la ingeniería social ha sido examinada de forma general, por lo cual en el propone un modelo que asocia cada rasgo de personalidad con uno o más principios de persuasión.

Para el caso del rasgo de conciencia, la vulnerabilidad a la ingeniería social se ve incrementada frente al principio de autoridad, reciprocidad y compromiso – coherencia, para el resto de principios se define una baja o nula vulnerabilidad. La simpatía y aprobación social pueden aprovechar la extroversión de las personas y que al buscar nuevas emociones en cosas que no se posee, puede ser emocionante para el individuo, lo que se vincula al principio de escasez. En personas con el rasgo de amabilidad influye la autoridad, reciprocidad, simpatía y aprobación social, el atacante aprovecha la naturaleza confiada, el apoyo que puede brindar y la bondad de la potencial víctima.

La apertura está relacionada a adquirir conocimiento libremente, lo que reduce la vulnerabilidad a ingeniería social ya que se asocia a experiencia y competencia tecnológica. El neuroticismo; en general, no representa un rasgo que pueda ser asociado a algún principio de persuasión que incremente la vulnerabilidad de las personas, dado que los individuos con este rasgo asumen las intenciones del peor lado de los demás en cualquier circunstancia, la ansiedad informática actúa como barrera ante posibles ataques.

Big Five Personality Traits of Cybercrime Victims (Weijer & Leukfeldt, 2017)**.** Los autores del artículo realizan un análisis de regresión logística para evaluar la relación entre los cinco principales rasgos de personalidad y tres grupos de víctimas. Indican que estos rasgos no se asocian específicamente a la victimización por ciberdelincuencia, sino más bien, con la delincuencia en general.

Determinaron que las personas más conscientes son aquellas que tienen un riesgo menor de ser víctimas de ciberdelincuencia, de forma similar, las personas con mayor estabilidad emocional tienen esta tendencia. Por otro lado, las personas abiertas a la experiencia tienen una probabilidad mayor de ser víctimas de cibercrimen por medio de hacking o infección por virus. Con el uso de otras características demográficas como la edad y el género, los resultados indican que los hombres y personas jóvenes son más propensas en ser víctimas de cibercrimen, a diferencia de las mujeres y personas mayores.

Los autores concluyeron que la estabilidad emocional es el único rasgo de personalidad que puede predecir significativamente la victimización por ciberdelincuencia, y que quienes son emocionalmente estables, tienen menor probabilidad de convertirse en víctimas. Dado que el estudio se llevó a cabo en Holanda, los autores indican que los resultados expuestos en su trabajo no pueden generalizar la realidad de otros países.

The impact of personality traits on user's susceptibility to social engineering attacks (Cusack & Adedokun, 2018)**.** En este trabajo, los autores utilizan el modelo de las cinco grandes personalidades. Los participantes en este estudio son personas que fueron

víctimas de ingeniería social y que entendieron la esencia de estos ataques. Uno de los participantes indica que el éxito de un ataque de ingeniería social tiene como factor motivante una relación confiable, el amor o el sentido del humor, esto se relaciona con el rasgo de amabilidad y extroversión. Otro participante indica que la presión de la autoridad, la facilidad y comodidad lo hicieron víctima de ingeniería social, esto se relaciona a la amabilidad y conciencia.

Por último, un individuo señala que el dinero, la curiosidad y la retroalimentación de otras personas fueron razón para que sea atacado por ingeniería social, eso se relaciona a la apertura, extroversión y amabilidad. Los autores encontraron que las personas con un nivel alto de amabilidad y extroversión son propensas a ser vulnerables a ataques de ingeniería social, aunque el éxito de este no solo depende de los rasgos de personalidad, sino también de la circunstancia en la que se encuentre la persona y de la técnica que utiliza el atacante.

Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods (Wang, Zhu, & Sun, 2021). Este artículo propone un modelo conceptual sobre la manera en que los atacantes utilizan ingeniería social para aprovechar las vulnerabilidades en cognición y conocimiento, hábito y comportamiento, sentimientos y emociones, naturaleza humana, rasgos de personalidad y carácter del individuo. En el trabajo en mención se analizan 16 escenarios en de ataques de ingeniería social.

En la mayoría de los escenarios analizados se encuentra al menos uno de los cinco grandes rasgos de personalidad que han sido aprovechados para vulnerar la seguridad de la información. En el escenario 16 utiliza un ataque de ingeniería social inversa, en donde se envía un correo electrónico de un remitente que impersona a un operador de soporte técnico, el cual solicita la contraseña a un usuario nuevo para conocer si la contraseña es débil o fuerte, dado que el usuario trata de ser amable y colaborador, accede a entregar la

contraseña convirtiéndose en víctima del ataque, en su personalidad también intervienen aspectos de incredulidad, juicio intuitivo e inexperiencia.

Para cumplir con su objetivo, el atacante utilizó los principios de persuasión de Cialdini, con lo cual se vincula los rasgos de personalidad con la persuasión para el éxito del ataque.

A Framework Based on Personality Traits to Identify Vulnerabilities to Social Engineering Attacks (Benavides-Astudillo, y otros, 2022)**.** Este estudio propone un marco de trabajo en el que se evalúan los rasgos de personalidad basados en base al Modelo de 5 Factores para identificar que tan vulnerable es una persona a ser víctima de ingeniería social.

En el trabajo en cuestión se indica que las personas con alto nivel de extroversión, amabilidad, neuroticismo y apertura pueden ser víctimas potenciales a sufrir un ataque, por otra parte, un nivel bajo de conciencia denota un alto nivel de vulnerabilidad. Para su estudio utilizaron un cuestionario de 42 preguntas. El resultado fue que, dentro de la muestra poblacional evaluada, la mayoría de las personas que son altamente vulnerables a ingeniería social son aquellas que tienen los rasgos de apertura, amabilidad y conciencia.

Human elements impacting risky habits in cybersecurity (Majumdar & Ramteke, 2022)**.** El desarrollo de este trabajo abarca distintos elementos humanos que ponen en riesgo a la ciberseguridad, dentro de estos elementos se encuentran los rasgos de personalidad. Los autores mencionan que; de forma directa o indirecta, estos rasgos influyen en el comportamiento de ciberseguridad de un individuo.

Utilizan una encuesta basada en el modelo de los cinco grandes rasgos de personalidad, al utilizar análisis estadístico concluyen que existe un impacto significante cuando intervienen algunos factores situacionales. Por ejemplo, las personas con alto nivel de neuroticismo tienen menor probabilidad de pasar por alto las políticas de seguridad definidas para seguridad de la información, ya que evalúan si confiar o no en un individuo o

indicación, por el contrario de individuos que obtuvieron un puntaje alto en extroversión quienes violarían dichas políticas de seguridad.

Así mismo, los autores indican que la personalidad de las personas se relaciona a la situación en la que se encuentren en el momento de un potencial ataque, como el caso de la presión del tiempo hace que los individuos puedan tomar decisiones apresuradas y riesgosas.

Resumen general y conclusión del estado del arte

Resumen general. Para la revisión de literatura, se ha tomado como referencia el modelo de propuesto por Kitchenham y otros (2009) con lo cual se ha definido la pregunta de investigación relacionada a los rasgos de personalidad de las personas que pueden ser convertirlos en individuos vulnerables a ataques de ingeniería social en el contexto de la seguridad de la información.

Con la pregunta de investigación planteada se obtienen siete artículos representativos que cumplen con todos los criterios de inclusión y exclusión descritos anteriormente. De estos artículos se realiza un resumen de los aspectos importantes que dan respuesta a la pregunta de investigación definida.

Conclusión del estado del arte. De los trabajos utilizados para el estado del arte; es importante resaltar que, para los rasgos de personalidad que definen el comportamiento de las personas el modelo que tienen mayor uso y aprobación es el denominado Modelo de los cinco factores, también conocido como Modelo de los cinco grandes rasgos de personalidad, y que se relacionan directa o indirectamente para que un ataque de ingeniería social llegue a concretarse, los atacantes analizan a su víctima y se aprovechan de las vulnerabilidades que puedan presentar.

Además de las vulnerabilidades que pueden reflejarse en el comportamiento de las personas, algunos autores mencionan que un ataque de ingeniería social de cualquier tipo será exitoso al depender de la situación en la que se encuentre la víctima.

Así pues, la tasa de éxito de dichos ataques puede incrementarse si se toman en cuenta otros factores demográficos tales como género, edad, nivel académico, lugar de residencia, entre otros.

Para finalizar, los autores de los trabajos expuestos en el Resumen de estudios primarios, coinciden en que las medidas técnicas para salvaguardar la seguridad y privacidad de la información no son suficientes y que los aportes realizados en sus investigaciones pueden servir como referencia para que se tome en cuenta la forma en que funciona la ingeniería social para aprovechar las vulnerabilidades del factor humano, con lo cual las organizaciones podrán definir medidas alternativas de prevención de ataques.

Capítulo III

Desarrollo metodológico e investigación de campo

Definición de los rasgos de personalidad pertinentes al estudio

De acuerdo con el grado que una persona posee de un cierto rasgo o indicador, hace que un individuo sea susceptible a ataques basados en ingeniería social, esto en base a algunos métodos de persuasión.

Los rasgos de personalidad y su relación con ataques de ingeniería social

Como se mencionó anteriormente, las organizaciones realizan todos los esfuerzos técnicos posibles para mitigar los riesgos de seguridad en sus sistemas, sin embargo, estas medidas resultan deficientes ante las vulnerabilidades en el factor humano (Richardson, Lemoine, Stephens, & Waller, 2020).

En su artículo de investigación, Uebelacker & Quiel (2014) han determinado que existe una relación directa entre el FFM y la ingeniería social con lo cual diseñaron un Modelo de Personalidad de la Ingeniería Social. En base a esto, los autores definen bajo qué rasgo de personalidad los individuos son considerados vulnerables o no a ingeniería social.

Apertura a la experiencia. De acuerdo a la técnica que un atacante utilice, este rasgo es un indicador de que una persona es vulnerable a un ataque, dado que son curiosas, perspicaces y con gran interés en cosas nuevas (Uebelacker & Quiel, 2014). Quienes tengan niveles altos de este rasgo, toman a la ligera los problemas de privacidad ya que subestiman el riesgo al que podrían estar expuestos y son individuos propensos a violar políticas de seguridad informática.

Conciencia. Las personas con niveles altos de este rasgo tienden a apegarse a las reglas definidas, con lo cual Uebelacker & Quiel (2014) indican que son vulnerables a ingeniería social ante un ataque que manipule a sus víctimas por medio de autoridad, la reciprocidad y el compromiso con otros. Wang, Zhu, & Sun (2021) coinciden con esta premisa al mencionar que las personas son vulnerables cuando se usan mecanismos de

persuasión, obediencia a la autoridad, normas de responsabilidad social, el compromiso y la coherencia. La vulnerabilidad incrementa si el entorno del compromiso es público.

Extraversión. La gente extrovertida representa un mayor riesgo a la seguridad de la información, dado que tienen mayor probabilidad de violar las políticas de seguridad informática, por lo que llegan a desobedecer estas normas para cumplir solicitudes que puede ser maliciosas. En los trabajos investigados por Uebelacker & Quiel (2014), encontraron evidencia que los empleados que no revelaron sus contraseñas son personas introvertidas y solitarias. Las personas se vuelven vulnerables a ingeniería social si el atacante usa mecanismos de similitud, agrado, ayuda y construcción de relaciones sociales.

Amabilidad. Es el rasgo más asociado al phishing. La vulnerabilidad de las personas radica en la confianza, altruismo y compromiso que tienen (Uebelacker & Quiel, 2014). Al confiar en el resto, se despreocupan sobre la invasión de su privacidad. Al utilizar manipulación que implique autoridad, reciprocidad, simpatía y aprobación social, se espera una mayor vulnerabilidad dado que pretenden alcanzar el bien para todos. Así mismo, Wang, Zhu, & Sun (2021) mencionan que estas personas actúan de forma crédula, lo que es aprovechado por los atacantes al utilizar los mecanismos mencionados anteriormente.

Neuroticismo. Una persona que tenga un nivel alto de neuroticismo tiene menor probabilidad de ser vulnerables a ataques de ingeniería social, dado que se comportan de forma paranoica y no divulgan información personal, esto se debe al miedo de ser el responsable; directo o indirecto, de una violación de seguridad, por lo que son precavidos a problemas de privacidad (Uebelacker & Quiel, 2014). Quiel (2013) menciona que la ansiedad informática y pensar que todas las personas tienen intenciones malas en cualquier momento puede generar una barrera para que un ataque de ingeniería social se concrete.

En el trabajo realizado por Papatsaroucha, Nikoloudakis, Kefaloukis, Pallis, & Markakis (2021) indican que los investigadores Cullen y Armitage definieron una metodología para evaluar la vulnerabilidad de las personas en base a los Indicadores de Myers-Briggs. En su investigación cada persona tuvo un rasgo en particular, con lo cual determinaron lo siguiente:

- Las personas extrovertidas llegaron a ser más susceptibles al principio de relación cercana.
- El perfil que toma decisiones en base a su sentido o intuición fue más susceptible al compromiso que tienen con personas de su círculo o que lo simulan.
- Quienes se basan al pensamiento y sentimiento, su percepción a la detección de ingeniería social se vio comprometida por la autoridad por parte de sus superiores y aprobación social con sus semejantes.
- Las personas que tienen un perfil en base a su juicio y percepción tienden a ser vulnerables a la persuasión mediante reciprocidad y distracción.

Por otra parte, el modelo HEXACO, el cual está basado en el modelo de los cinco rasgos de personalidad (Cieciuch & Strus, 2021), sin embargo, no se incluye al neuroticismo; si no, se toma en cuenta a la Honestidad/Humildad y la Emocionalidad como rasgos de personalidad principales para este modelo. En su investigación, determinan que los individuos con alto grado de conciencia y amabilidad tienen un comportamiento más seguro en entornos de Internet; y que, por lo tanto, disminuye la probabilidad de ser víctimas de crímenes informáticos.

Dentro del trabajo de maestría de van Winsen (2020) de los resultados obtenidos pudo determinar que las personas quienes tuvieron una puntuación alta en conciencia, amabilidad y emocionalidad tienen un comportamiento más seguro en entornos en línea. Además, los individuos con una puntuación alta en apertura a la experiencia, honestidad/humildad y extraversión, son sujetos que se comportan de una manera no tan segura en ambientes de Internet.

Definición del modelo ecléctico de rasgos significativos de personalidad

El método ecléctico aplicado para este trabajo es utilizado para recopilar y fusionar los puntos más importantes para seleccionar los rasgos de personalidad que hacen vulnerables a los individuos a ataques de ingeniería social. Por esta razón, se han

seleccionado tres de los modelos de personalidad más importantes que están relacionados a la seguridad de la información y la vulnerabilidad de las personas.

Como se observa en **Tabla *2*** se ha extraído los rasgos, características e indicadores de personalidad de cada modelo descrito anteriormente y que tienen relación directa e indirecta a la vulnerabilidad de ingeniería social.

Tabla 2

Rasgos e indicadores de personalidad asociados a ingeniería social

Modelo de los 5 Factores	**Indicadores Myers-Briggs**	**Modelo HEXACO**
Apertura a la experiencia	Sentido/Intuición	Apertura a la experiencia
Conciencia	Juicio/Percepción	Conciencia
Extraversión	Extraversión/Introversión	Extraversión
Amabilidad	Pensamiento/Sentimiento	Amabilidad
Neuroticismo		Emocionalidad
		Honestidad/Humildad

En definitiva, los rasgos de personalidad cumplen un rol importante al momento de determinar el comportamiento en seguridad informática y la vulnerabilidad que pueden presentar las personas para convertirse en una amenaza y potencial riesgo a la seguridad de la información. No obstante, la vulnerabilidad a un ataque podrá cambiar al depender de la circunstancia en que la persona se encuentre, el entorno, su edad, género, cultura, nacionalidad, creencias y nivel académico, entro otros aspectos; lo cual, puede interferir en el grado de vulnerabilidad que tenga una persona y la probabilidad de que los ataques de ingeniería social lleguen a ser exitosos.

Al dejar a un lado estos aspectos para futuros trabajos, se ha determinado los siguientes rasgos de personalidad que servirán para determinar la vulnerabilidad de las personas en entornos de seguridad informática, estos rasgos han sido obtenidos de los tres modelos presentados en Tabla 2, la selección de los rasgos se realizó por su aparición repetida y la semejanza que existe entre los modelos.

A continuación, en **Tabla *3*** se presenta una clasificación de los rasgos de personalidad y el grado en que son vulnerables a ingeniería social, se ha utilizado una categorización por semáforo; en donde, el color verde indica un nivel bajo de vulnerabilidad, el color amarillo determina que la persona es medianamente vulnerable y el color rojo define que un individuo es altamente vulnerable a ser víctima de ingeniería social.

Tabla 3

Categorización de rasgos de personalidad según su grado de vulnerabilidad

Rasgo	Bajo	Medio	Alto
Apertura a la experiencia	Personas reservadas, no suelen actualizar sus conocimientos sobre ataques informáticos. Tienen menor competencia informática.	Aceptan y están abiertos a aprender nuevas cosas sin dejar aislado su comportamiento conservativo.	Personas son curiosas y suelen despreocuparse por su privacidad. Subestiman el riesgo al que se pueden exponer. Pueden violar políticas se seguridad.
Conciencia	Son susceptibles cuando una autoridad le da alguna indicación y más aún cuando el compromiso se lo realiza en público. No les interesa violar las reglas establecidas.	Son personas que pueden llegar a cometer errores, no obstante, mantienen sus valores y acciones constantes. Asumen las consecuencias de sus actos.	Se apegan a las reglas definidas, por lo que respetarán los estándares y procedimientos de seguridad. Son personas responsables.
Extraversión	Individuos introvertidos que no socializan y no comparten con grandes grupos de personas. Pueden mantener segura la información privada.	Mantienen un comportamiento reservado en cualquier situación, no obstante, si algo o alguien llama su atención pueden establecer una conversación más larga de normal.	Pueden violar reglas de seguridad por cumplir peticiones de otras personas. Al ser sociables, llegan a compartir información que puede ser confidencial. Son vulnerables a la autoridad, compromiso y aprobación social.
Amabilidad	Son personas que tienen un comportamiento hostil y egoísta. No son condescendientes ante las peticiones de sus semejantes y tampoco ofrecerán su ayuda.	Tienen un equilibrio de su bondad y la precaución. Pueden ayudar a los demás solo si es necesario, siempre y cuando determinen las consecuencias que podrían aparecer.	Son personas crédulas. Por tener aprobación social pueden realizar acciones sin importar si deben pasar por alto las normas de seguridad definidas. No sospechan de las malas intenciones que

Rasgo	Bajo	Medio	Alto
			pueda tener otra persona.
Neuroticismo	Pueden pasar por alto las políticas de seguridad informática. Son vulnerables cuando una autoridad le ordena que realice alguna acción, ya que se sienten en la obligación de cumplir órdenes.	Generalmente mantienen la calma en distintas situaciones, sin embargo, pueden romper su estabilidad cuando se sienten obligados a realizar algo.	Toman en cuenta las malas intenciones de las personas. La ansiedad informática hace que las personas con un puntaje alto, actúen de manera precavida por las consecuencias que puede acarrear su accionar.
Honestidad / humildad	Pueden cometer actos inmorales, ya sea por malicia o por una ganancia personal. Romperán normas de seguridad establecidas.	Pueden ser víctimas ya que son optimistas en la honestidad o del comportamiento correcto de los demás.	Personas escrupulosas que actuarán de manera correcta sin saltarse pasos para vulnerar la seguridad. Tienen un comportamiento justo en cualquier situación.

De los tres modelos de rasgos de personalidad no se mencionan algunos debido a que en la teoría disponible se hace referencia a que algunos rasgos son semejantes entre sí, como es el caso de Amabilidad y Extraversión, que en el modelo HEXACO se indica que ambos rasgos expresan la intensidad del comportamiento social.

De forma similar ocurre con el neuroticismo y la extraversión, que son considerados como energizantes de conducta humana. Dentro del modelo, la emocionalidad de HEXACO no se presenta ya que no existe relación directa con la victimización de personas en el ámbito de seguridad de la información, esto no ocurre para el escenario de victimización por otros delitos comunes.

Además, según lo mencionan Papatsaroucha, Nikoloudakis, Kefaloukis, Pallis, & Markakis (2021), el Sentimiento / Pensamiento está directamente asociado o es un símil del

rasgo de Amabilidad presente en el FFM, es por esta razón que tampoco se incluye en el modelo propuesto en el presente trabajo.

Definición del instrumento de evaluación

Para el cumplir con los objetivos de este trabajo, se pretende evaluar la vulnerabilidad de las personas mediante un cuestionario de personalidad, este instrumento es diseñado para recabar información de una persona en particular. Según lo expuesto por García Muñoz (2003) cuando un cuestionario es innecesariamente extenso, las personas evaluadas pueden sentirse cansadas y hace que tengan un rechazo para completarlo, con lo cual se puede obtener una evaluación incompleta o inconsistente, así mismo, menciona que el tiempo necesario para terminar completamente la evaluación puede variar entre 30 minutos y una hora.

La definición del número de preguntas que son necesarias puede variar en función de la complejidad de la misma, para el caso de cuestionarios utilizados en psicología, se encontró que se puede utilizar entre 40 a 50 preguntas distribuidas entre todas las variables de interés, esto ayuda a garantizar que se puede obtener datos concisos sin generar cansancio en la persona evaluada (Coindreau, 2022).

Los investigadores Donnellan, Oswald, Baird & Lucas (2006) diseñaron un cuestionario compuesto por 20 preguntas para determinar la personalidad en base al Modelo de los Cinco Factores. Con este cuestionario demostraron que en un tiempo menor se puede tener resultados similares a los cuestionarios con mayor cantidad de preguntas. En el mismo trabajo mencionan que existe un cuestionario de diez preguntas que; según los autores, es difícil tener consistencia de resultados al evaluar cada personalidad únicamente con dos preguntas por cada rasgo.

Por lo mencionado anteriormente, en base a la duración que puede tener un cuestionario, la cantidad de preguntas y el tiempo estimado para responder cada pregunta,

se ha planteado utilizar 42 preguntas y cada pregunta puede demorar hasta 20 segundos en ser contestada, con lo que se tiene lo siguiente:

$$Duración\ del\ test = \#\ de\ preguntas * Tiempo\ de\ respuesta$$

Al reemplazar los valores se calcula el tiempo estimado para completar el test.

$$Duración\ del\ test = 42 * 20\ s$$

$$Duración\ del\ test = 840\ s$$

$$Duración\ del\ test = 840\ s * \frac{1\ m}{60\ s}$$

$$Duración\ del\ test = 14\ m$$

La cantidad de preguntas que se utilizará responde a la necesidad de tener un adecuado modelamiento de cada personalidad al tener un resultado más detallado y conciso.

La duración para completar el cuestionario para evaluar los rasgos de personalidad podría durar aproximadamente 14 minutos, a este tiempo se le añade 3 minutos para que la persona que será evaluada lea las indicaciones generales del cuestionario y que responda algunas preguntas de carácter personal e institucional, con lo cual se obtiene que, para completar la evaluación, la persona lo podrá hacer en aproximadamente 17 minutos.

De acuerdo con los rasgos de personalidad expuestos en Tabla 3 se ha investigado la disponibilidad existente de distintos cuestionarios y su escala de medición para determinar un puntaje que determinará la personalidad de cada individuo y para finalmente definir el grado de vulnerabilidad que esta persona tiene para ser víctima de ingeniería social.

El banco de preguntas obtenido fue del resultado de comparar los ítems definidos en distintos cuestionarios utilizados en investigaciones previas. Los cuestionarios utilizados para esta actividad son:

- BFI Personality Trait Scale
- NEO5-20
- Ten-Item Personality Inventory-(TIPI)
- 20-Item Mini-IPIP
- HEXACO-PI

De los cuestionarios mencionados anteriormente se han extraído sus ítems, se ha agrupado cada uno de acuerdo con el rasgo de personalidad que evalúan y la similitud existente entre sí por último se ha definido un listado de preguntas que serán utilizadas como herramienta de evaluación. El banco de preguntas categorizado por rasgo de personalidad se puede observar en Tabla 4.

Tabla 4

Banco de preguntas recopilado de cuestionarios de personalidad

Rasgo de personalidad	Tipo de valoración	Pregunta
Apertura a la experiencia	N	¿Tiene buena imaginación? Le resulta fácil pensar en cosas útiles y nuevas
	N	¿Le gusta pensar en ideas abstractas o poco convencionales? (Ideas en base al análisis minucioso de las situaciones)
	N	¿Es creativo/a?
	R	¿Cree que el arte es aburrido?
	N	¿Se siente atraído/a con ideas nuevas; ya sean, propias o ajenas? (Le llama la atención las ideas innovadoras de otros)
	R	¿Le desagrada tener conversaciones complejas? (Conversaciones que abarcan temas políticos, sociales, científicos, psicológicos, entre otros)
	R	¿Prefiere que su trabajo sea rutinario? (Realizar siempre las mismas actividades sin ningún cambio)
Conciencia	N	¿Termina las actividades que comienza?
	N	¿Pone toda su atención para realizar alguna actividad? (Estar concentrado)
	R	¿Olvida poner las cosas en su lugar?
	N	¿Lleva a cabo sus planes? (Empieza los planes que tiene pendientes)
	R	¿Cree que suele arruinar las cosas, ya sean personales o profesionales?
	N	¿Cree que es un/a trabajador/a confiable?
	R	¿Se distrae fácilmente?
Extraversión	R	¿Es una persona callada?

Rasgo de personalidad	Tipo de valoración	Pregunta
Amabilidad	R	¿Es tranquilo/a o reservado/a?
	N	¿Cree que es el alma de la fiesta?
	N	¿Genera entusiasmo en otros/as?
	R	¿Se mantiene distante de otras personas?
	R	¿Le resulta difícil presentarse cuando conoce a alguien nuevo?
	R	¿No disfrutaría de un trabajo que requiera mucha interacción social?
	R	¿Suele contradecir a los demás?
	N	¿Ayuda a las personas sin esperar nada a cambio?
	R	¿Comienza discusiones / peleas con los demás?
	R	¿No le interesa los problemas de los demás?
	R	¿Es descortés con otros/as?
	N	¿Siente empatía por las emociones de los demás?
	N	¿Respeta a las personas?
Neuroticismo	N	¿A menudo se siente triste o deprimido/a?
	R	¿Se siente tranquilo/a, aunque esté en situaciones de alta presión?
	N	¿Se pone nervios/a o ansioso/a con facilidad?
	N	¿Se preocupa mucho en cualquier situación?
	N	¿Tiene cambios de humor frecuentes?
	R	¿Rara vez se enoja?
	N	¿Se frustra con facilidad?
Honestidad/humildad	R	Robaría dinero si supiera que nunca va a ser descubierto
	R	¿Quisiera ganar mucho dinero, aunque sea de forma deshonesta?
	N	¿No aceptaría un soborno, aunque fuera muy cuantioso? (El soborno tiene un gran valor económico)
	R	¿Le gustaría vivir en un lugar muy caro y de clase alta?
	R	¿Quisiera que lo vieran conduciendo un auto muy caro?
	R	¿Cree que se merece más respeto que los demás?
	N	Si quisiera algo de alguien ¿se reiría de sus chistes, aunque no causen gracia?

Definición de matriz de priorización de rasgos de personalidad

Debido a que el conjunto de rasgos de personalidad forma el comportamiento de los individuos y cada uno puede ser el detonante diferente para que una persona actúe de cierta manera, así mismo, no todos los rasgos van a tener la misma relevancia e inclusive la toma de decisiones puede verse influenciada por una superposición entre un rasgo y otro, es por ello que se ha definido la siguiente matriz de priorización (Tabla 5) con la cual se

evaluará a las personas y para determinar cuál es la característica de personalidad dominante en su comportamiento.

Tabla 5

Matriz de priorización de rasgos de personalidad

Rasgo	O	C	E	A	N	H / H
Apertura a la experiencia	0	0,5	0,7	0,4	0,4	0,2
Conciencia	0,8	0	0,6	0,3	0,5	0,8
Extraversión	0,6	0,8	0	0,4	0,4	0,6
Amabilidad	0,5	0,8	0,6	0	0,2	0,8
Neuroticismo	0,5	0,8	0,4	0,6	0	0,2
Honestidad / humildad	0,5	0,8	0,6	0,8	0,5	0

De esta tabla, sus valores de la diagonal principal son cero, ya que la intersección es entre los mismos rasgos de personalidad. Así mismo, en base a los valores definidos se calcula se obtienen los siguientes valores mostrados en **Tabla *6***.

Tabla 6

Valores de coeficientes de priorización por rasgos de personalidad

Rasgo	Sumatoria de priorización	Coeficiente de priorización
Apertura a la experiencia (O)	2.2	**0.13**
Conciencia (C)	3	**0.18**
Extraversión(E)	2.8	**0.17**
Amabilidad (A)	2.9	**0.17**
Neuroticismo (N)	2.5	**0.15**
Honestidad / humildad (H)	3.2	**0.19**
O+C+E+A+N+H	**16.6**	

El valor de sumatoria de cada rasgo de personalidad se obtiene al sumar los números de la fila. Posteriormente se suman estos resultados y se obtiene un nuevo valor. Para calcular el coeficiente de priorización de rasgos, se divide la suma de cada fila para el último valor encontrado. Este coeficiente servirá para calcular un grado de vulnerabilidad en una escala de 0 al 5, esto se debe a que en las preguntas se puede obtener un puntaje de máximo de 5 en cada rasgo de personalidad.

Definición de la muestra poblacional

Según lo definido en el alcance que abordará el presente trabajo, el instrumento de evaluación será aplicado al personal de docentes y estudiantes del DCCO de la Universidad de las Fuerzas Armadas ESPE en su sede matriz.

En este caso, la población de interés responde a las características de docentes y estudiantes de la Matriz de la UFA-ESPE y para obtener la muestra poblacional, se ha delimitado que sean alumnos y profesores del DCCO. Para el periodo académico en el que se desarrolló el presente trabajo, se ha definido un total de 110 personas; entre estudiantes y docentes, que van a ser los sujetos evaluados a los cuales se les remitirá el cuestionario.

Diseño de la herramienta de evaluación

El cuestionario de evaluación propuesto para cumplir con los objetivos de este trabajo ha sido implementado en Google Forms, esto se debe a la factibilidad de uso y difusión que presenta esta aplicación. En primera instancia se definen las instrucciones del cuestionario y se le hace conocer a la persona evaluada que los datos recopilados son de carácter confidencial y el uso de los mismos será exclusivamente en el presente trabajo.

El cuestionario definido incorpora las 42 preguntas definidas en Tabla 4; así mismo, se integran preguntas generales correspondientes a su información institucional, que responden a:

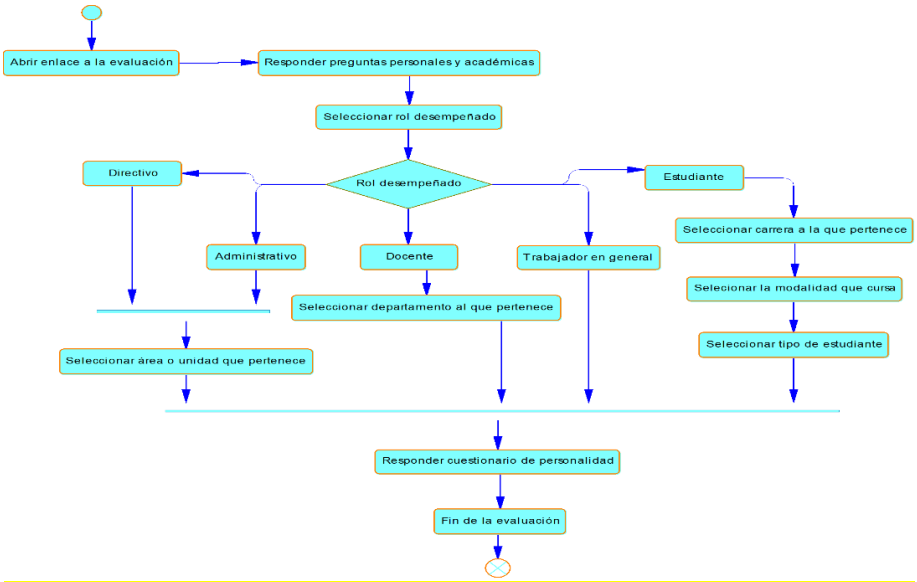
- Rol desempeñado en la universidad.
- Unidad o área a la que pertenece.

- Departamento al que pertenece.
- Carrera a la que pertenece

La presentación de las preguntas a los usuarios va a depender del rol desempeñado en la universidad; es por ello que, si el usuario selecciona el rol de Directivo o Administrativo se le redirigirá a la sección de para seleccionar la unidad o área a la que pertenece; en cambio, al seleccionar el rol de Docente, se le pedirá que elija el departamento al que pertenece, si el usuario escoge el rol de Estudiante, deberá responder la carrera a la que pertenece y si es estudiante Militar o Civil, una vez respondidas estas preguntas el usuario está en la posibilidad de responder las preguntas psicológicas para definir sus rasgos de personalidad. En el caso particular de que el usuario seleccione el rol de Trabajador en general, pasará directamente a las preguntas psicológicas. El flujograma del cuestionario se muestra en Figura 5.

Figura 5

Diagrama de flujo para completar la evaluación de personalidad.



También se incluye un par de preguntas que corresponde a información demográfica en donde se desea conocer el rango de edad en la que se encuentra la persona a ser evaluada, las opciones disponibles van desde los 17 años hasta los 60 años en adelante; así mismo, se requiere conocer el género de los individuos ya sea femenino, masculino o en su defecto, si el usuario no se identifica con ninguno de estos dos géneros.

Una vez respondidas estas preguntas de información institucional, personal y demográfica, la persona podrá responder las preguntas que evalúan sus rasgos de personalidad, las mismas que van a ser mostradas en un orden aleatorio.

Las preguntas psicológicas pueden ser respondidas en una escala de Likert que va del uno al cinco; donde, uno es equivalente a Totalmente en desacuerdo y cinco corresponde a Totalmente de acuerdo.

A continuación, en **Figura 6**, **Figura 7**, **Figura *8*** y **Figura *9*** se presenta la evaluación que va a ser enviada a los usuarios mediante el correo electrónico institucional de la UFA-ESPE para la muestra poblacional definida anteriormente.

Figura 6

Indicaciones generales del cuestionario de personalidad.

Figura 7

Preguntas de tipo institucional y personal.

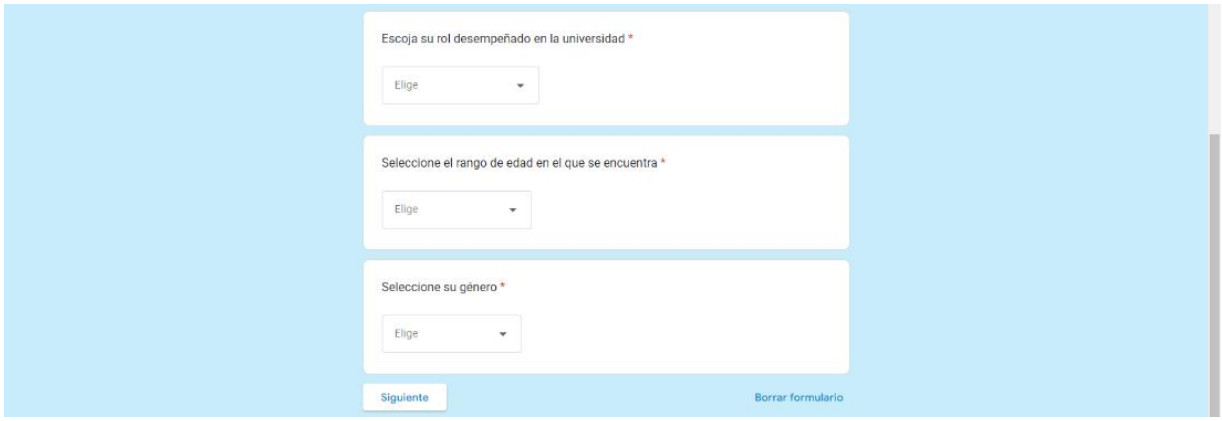


Figura 8

Preguntas definidas para el caso de estudiantes.

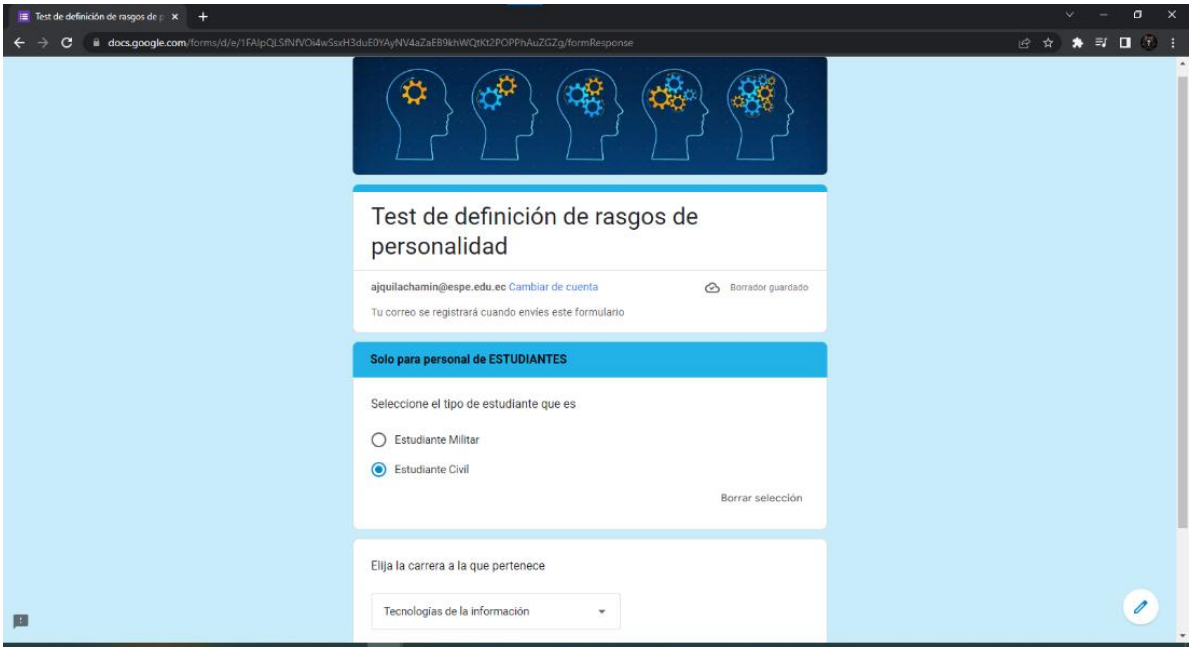
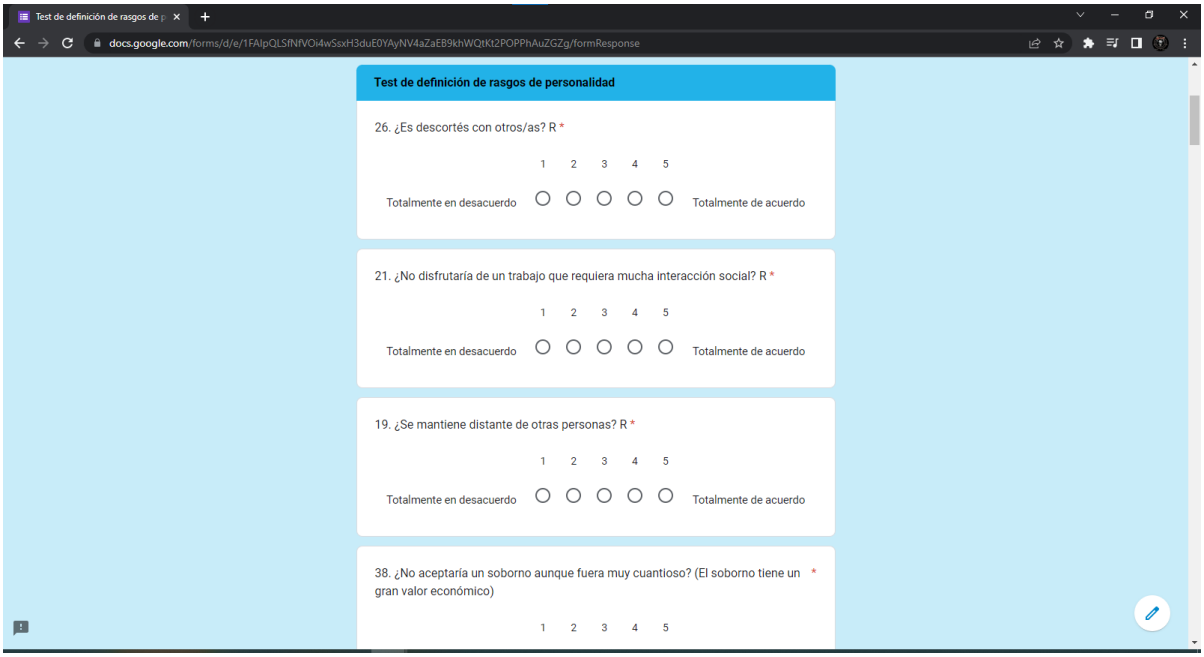


Figura 9

Fragmento de preguntas de personalidad presentadas en orden aleatorio.


Test de definición de rasgos de p
docs.google.com/forms/d/e/1FAIpQLSfNfVOi4wSsxH3duE0YAyNV4aZaEB9khWQtKt2POPPhAuZGZg/formResponse
Test de definición de rasgos de personalidad
26. ¿Es descortés con otros/as? R *
1 2 3 4 5
Totalmente en desacuerdo
Totalmente de acuerdo
21. ¿No disfrutaría de un trabajo que requiera mucha interacción social? R *
1 2 3 4 5
Totalmente en desacuerdo
Totalmente de acuerdo
19. ¿Se mantiene distante de otras personas? R *
1 2 3 4 5
Totalmente en desacuerdo
Totalmente de acuerdo
38. ¿No aceptaría un soborno aunque fuera muy cuantioso? (El soborno tiene un gran valor económico) *
1 2 3 4 5

Capítulo IV

Aplicación y evaluación

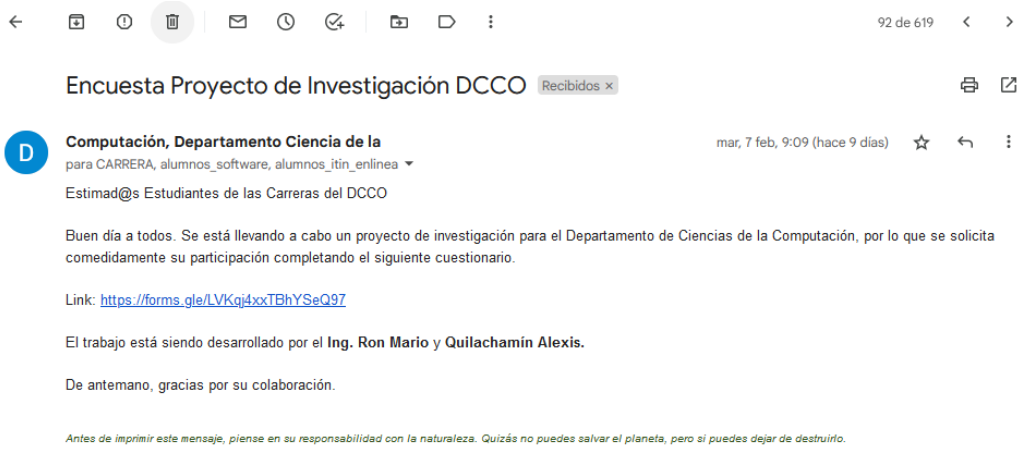
En este capítulo se describe la forma en que se aplicó la evaluación de rasgos de personalidad a los miembros del DCCO. El método de difusión del cuestionario se lo hizo mediante el correo electrónico institucional de la UFA-ESPE. Debido a que un estudiante no puede enviar correos electrónicos a grupos administrados por la organización, se solicitó la ayuda de la secretaria del departamento para que se difunda el formulario a los estudiantes y docentes para que puedan completar la evaluación.

A continuación, se muestra en la Figura 10 una copia del correo electrónico enviado para alumnos y docentes. Los correos electrónicos correspondientes son:

- alumnos_itin@espe.edu.ec
- alumnos_software@espe.edu.ec
- alumnos_itin_enlinea@espe.edu.ec
- docentes_dcco@espe.edu.ec

Figura 10

Correo electrónico enviado con la evaluación de rasgos de personalidad.



El tiempo requerido para la fase de aplicación del cuestionario ha empezado desde el 31 de enero de 2023 hasta el 10 de febrero del mismo año; es decir, para la recopilación de respuestas se ha empleado un total de 11 días, dentro de los mismos, las personas evaluadas respondieron a la evaluación de acuerdo a su disponibilidad de tiempo.

Como se había mencionado, se obtuvo una muestra poblacional de 110 miembros del DCCO, de los cuales 15 encuestados fueron docentes y las otras 95 personas fueron estudiantes de las carreras de Ingeniería en Tecnologías de la Información en su modalidad presencial y en línea e Ingeniería de Software.

Procesamiento de los resultados obtenidos

Una vez que ha terminado la fase de aplicación del cuestionario se realiza el procesamiento respectivo de las 110 evaluaciones obtenidas.

El procesamiento cosiste el normalizar los puntajes de las preguntas que tienen una valoración reversa según lo indica Tabla 4; con esto, las respuestas a las preguntas que tienen una R deben cambiados por su valor opuesto dentro de la escala para obtener el puntaje de cada rasgo. Por esta razón se hizo el cambio respectivo de los valores, como se lo evidencia en Figura 11, en esta figura se muestra una porción de los cambios realizados.

Figura 11

Intercambio de puntajes obtenidos en preguntas con valoración reversa.

H	I	J	K	L	M	N	O
3. ¿Es creati	4. ¿Cree que el arte es a		5. ¿Se siente	6. ¿Le desagrada tener c		7. ¿Prefiere que su traba	
2	2	4	4	3	3	4	2
4	1	5	5	1	5	4	2
4	1	5	5	2	4	1	5
4	1	5	4	1	5	2	4
3	1	5	3	1	5	2	4
3	1	5	4	4	2	3	3
4	3	3	5	3	3	2	4
5	1	5	5	1	5	1	5
5	1	5	5	1	5	2	4
5	1	5	4	3	3	3	3
5	1	5	5	1	5	1	5
5	3	3	5	2	4	2	4
5	1	5	2	2	4	1	5
4	2	4	4	3	3	3	3

Una vez intercambiados los valores, se procede a calcular los puntajes obtenidos por cada evaluado en cada rasgo de personalidad, esto implica realizar la sumatoria de los valores obtenidos por cada pregunta, con lo cual se obtiene el resultado que se muestra a continuación en

Figura **12**.

Figura 12

Puntajes obtenidos por cada rasgo de personalidad.

CA	CB	CC	CD	CE	CF
Apertura	**Conciencia**	**Extraversion**	**Amabilidad**	**Neuroticism**	**Hones/Humil**
3.14	3.71	2.14	3.57	4.00	3.14
3.57	3.14	2.14	3.86	3.43	3.43
3.57	4.00	2.71	3.86	2.43	2.57
2.86	3.00	3.00	2.57	3.14	2.86
4.86	5.00	4.00	4.57	1.57	4.14
3.43	4.29	3.00	4.43	1.57	3.86
4.29	4.14	3.43	4.00	2.57	4.00
4.43	5.00	3.57	4.43	1.00	3.29
4.14	5.00	2.71	5.00	1.57	4.71
4.00	5.00	3.86	5.00	1.14	4.43
4.57	4.43	2.71	3.71	1.14	2.86
4.43	4.86	3.29	3.86	2.43	4.43
3.86	5.00	3.57	4.71	1.29	4.43
4.71	5.00	3.57	3.86	1.86	3.86
3.86	3.86	2.29	4.71	3.14	4.71
4.00	4.43	3.86	3.86	1.71	3.14
3.86	3.86	3.29	3.14	2.57	3.43

A continuación, el cálculo para determinar el puntaje o grado de vulnerabilidad que tienen las personas para ser víctimas de ingeniería social. Este grado se obtiene mediante la multiplicación de cada valor obtenido en

Figura **12** y los coeficientes de priorización de cada rasgo (Tabla 6). Para evidencia de ello, se muestran los valores finales de este procedimiento (Figura 13).

Figura 13

Grado de vulnerabilidad obtenido por cada evaluado.

CA	CB	CC	CD	CE	CF	CG	CH	CI	CJ
Apertura	Conciencia	Extraversion	Amabilidad	Neuroticism	Hones/Humil		Puntaje de	Vulnerabilidad	Grado
3.14	3.71	2.14	3.57	4.00	3.14			3.28	Leve
3.57	3.14	2.14	3.86	3.43	3.43			3.25	Leve
3.57	4.00	2.71	3.86	2.43	2.57			3.19	Leve
2.86	3.00	3.00	2.57	3.14	2.86			2.90	Medio
4.86	5.00	4.00	4.57	1.57	4.14			4.06	Baja
3.43	4.29	3.00	4.43	1.57	3.86			3.49	Leve
4.29	4.14	3.43	4.00	2.57	4.00			3.75	Leve
4.43	5.00	3.57	4.43	1.00	3.29			3.65	Leve
4.14	5.00	2.71	5.00	1.57	4.71			3.93	Leve
4.00	5.00	3.86	5.00	1.14	4.43			3.98	Leve
4.57	4.43	2.71	3.71	1.14	2.86			3.24	Leve
4.43	4.86	3.29	3.86	2.43	4.43			3.91	Leve
3.86	5.00	3.57	4.71	1.29	4.43			3.89	Leve
4.71	5.00	3.57	3.86	1.86	3.86			3.83	Leve
3.86	3.86	2.29	4.71	3.14	4.71			3.80	Leve
4.00	4.43	3.86	3.86	1.71	3.14			3.52	Leve
3.86	3.86	3.29	3.14	2.57	3.43			3.36	Leve

Para tener una clara perspectiva de los resultados obtenidos se ha aplicado una escala de colores con lo cual se identifica adecuadamente la vulnerabilidad que representa cada grado obtenido. La escala en mención se puede observar en Figura 14.

Figura 14

Escala de colores de vulnerabilidad.

Puntaje	Tipo de vulnerabilidad
5	Vulnerabilidad Nula
4	Vulnerabilidad Baja
3	Vulnerabilidad Leve
2	Vulnerabilidad Media
1	Vulnerabilidad Alta
0	Vulnerabilidad Crítica

Interpretación de resultados

Una vez finalizado el procesamiento de los resultados es necesario interpretarlos y presentarlos para tener una visualización general del grado de vulnerabilidad que tienen los docentes y estudiantes del DCCO.

En primera instancia se obtuvo que, del total de participantes en la evaluación, ninguno obtuvo una clasificación Alta o Crítica en vulnerabilidad para ingeniería social, lo cual representa una buena métrica en donde no existen miembros del DCCO que puedan ser un medio que fácilmente pueda ser aprovechado para vulnerar la seguridad de la información dentro del DCCO. Por otra parte, tampoco se encontró algún miembro que sea

invulnerable para ingeniería social, esto tiene coherencia debido a que ninguna persona puede ser lo suficientemente segura como para no caer en algún tipo de ataque ya sea informático o no.

Resultados del grado de vulnerabilidad en términos generales

De los 110 evaluados, tres participantes que representan el 2.73% del total, tienen un comportamiento más seguro, dado que la vulnerabilidad calculada fue baja. Por otra parte, 98 personas que equivale al 89.09% de los encuestados tienen una personalidad que puede ser levemente vulnerable para ser víctimas de ingeniería social. Por último, el porcentaje restante de 8.18%; es decir, nueve personas obtuvieron un grado medio en vulnerabilidad. Estos valores pueden ser contrastados con lo que se muestra en Tabla 7 y cuya representación gráfica se muestra en

Figura ***15***.

Tabla 7

Porcentaje de personas de acuerdo a su grado de vulnerabilidad

Grado de vulnerabilidad	Evaluados	Porcentaje
Nula	0	0%
Baja	3	2.73%
Leve	98	89.09%
Media	9	8.18%
Alta	0	0%
Crítica	0	0%

Figura 15

Porcentaje de participantes según el grado de vulnerabilidad.

Resultados por rasgos de personalidad en docentes

Como se mencionó anteriormente, existe un grupo de 15 evaluados que actualmente son profesores del DCCO, de ellos se han obtenido resultados de que tienen un comportamiento más seguro ante una posible situación de ataque de ingeniería social.

Se ha generado datos de estadística descriptiva que se encuentran presentes en Tabla 8, de donde se puede apreciar que el promedio del grado de vulnerabilidad presente en docentes es de 3.71, con lo que se etiqueta una vulnerabilidad leve, el valor de 0.24 en la desviación estándar la dispersión media en la variación que existe entre los distintos valores que ha obtenido cada docente. En donde el docente que tiene una vulnerabilidad baja ha obtenido un puntaje de 4.06 y el que tiene grado de vulnerabilidad leve más bajo ha obtenido un valor de 3.24 (**Tabla *8***).

Tabla 8

Datos estadísticos de vulnerabilidad para el segmento de docentes participantes.

Estadísticas de docentes	
Media	3.71
Error típico	0.06
Mediana	3.75
Moda	#N/D
Desviación estándar	0.24
Varianza de la muestra	0.06
Curtosis	-0.64
Coeficiente de asimetría	-0.47

Estadísticas de docentes	
Rango	0.82
Mínimo	3.24
Máximo	4.06
Suma	55.61
Cuenta	15.00

La información de los rasgos de personalidad que poseen los docentes, en general tiene una tendencia con poca variabilidad, esto se puede verificar en Figura 16, en donde se observa que los valores difieren hasta en dos puntos.

De esto se puede definir que los docentes tienen el rasgo de apertura a la experiencia de manera uniforme, para el caso de la conciencia o escrupulosidad varía entre 4 y 5 lo cual denota que su comportamiento es apegado a las reglas o normas que definen su accionar.

La extraversión ser ve marcada entre 2.5 y 4 con lo cual se puede notar que conservan un comportamiento reservado en cualquier situación; sin embargo, podrían generar alguna conversación más larga de lo normal si algún tema llama su interés.

Al referirnos a la amabilidad, sus valores oscilan entre 5 y 3, con esto podrían estar aislados a peticiones de sus semejantes que podrían tener un interés por debajo, aunque, podrían llegar a no sospechar de las malas intenciones de los demás, de alguna manera tienen un nivel intermedio de este rasgo.

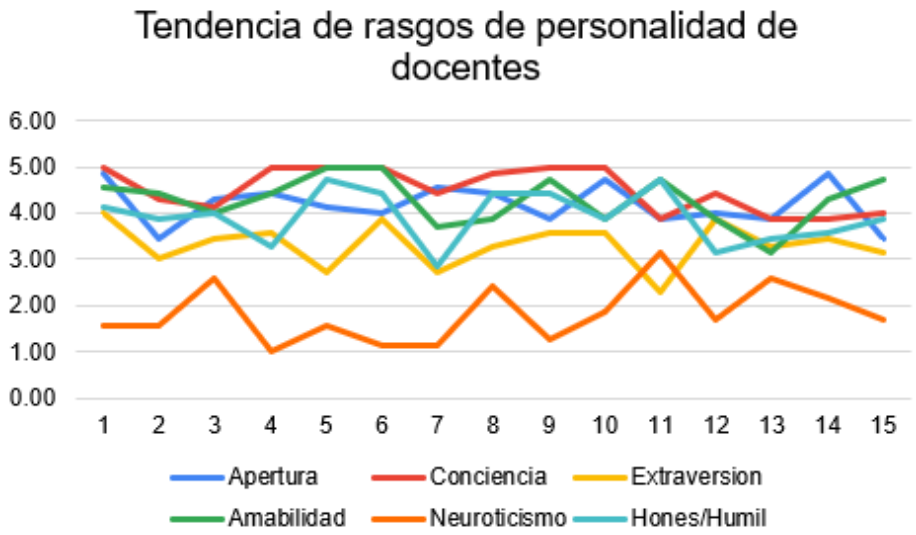
Al hacer referencia al neuroticismo, se evidencian valores bajos que están en el rango de 1 y 3, de acuerdo a lo presentado anteriormente, podrían verse influenciados por una autoridad ya que deben cumplir con las indicaciones que se les dé, en ocasiones pueden pasar por alto algunas políticas de seguridad ya que no visualizan completamente las malas intenciones del resto.

Por último, para el rasgo de honestidad / humildad este puntaje se encuentra entre 3 y 5, con esto se determina que son personas que actúan de forma correcta y justa en

cualquier situación con el fin de no perjudicarse ni perjudicar a la organización que pertenecen. Lo expuesto anteriormente se puede evidenciar en Figura 16.

Figura 16

Tendencia de rasgos de personalidad de docentes.

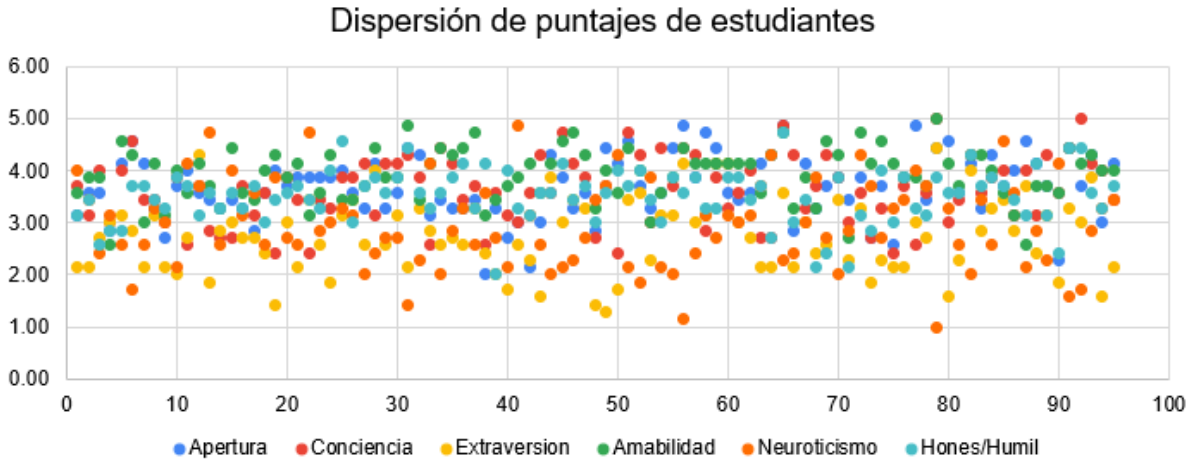


Resultados por rasgos de personalidad en estudiantes

Para el caso de los estudiantes (**Figura *17***), los evaluados tienen una mayor variabilidad entre rasgos de personalidad, como en el caso de la extraversión y neuroticismo, en donde sus valores pueden ir desde 1 a 5, esto puede deberse al entorno social en que se desenvuelven y la herencia genética; es decir, su temperamento.

Figura 17

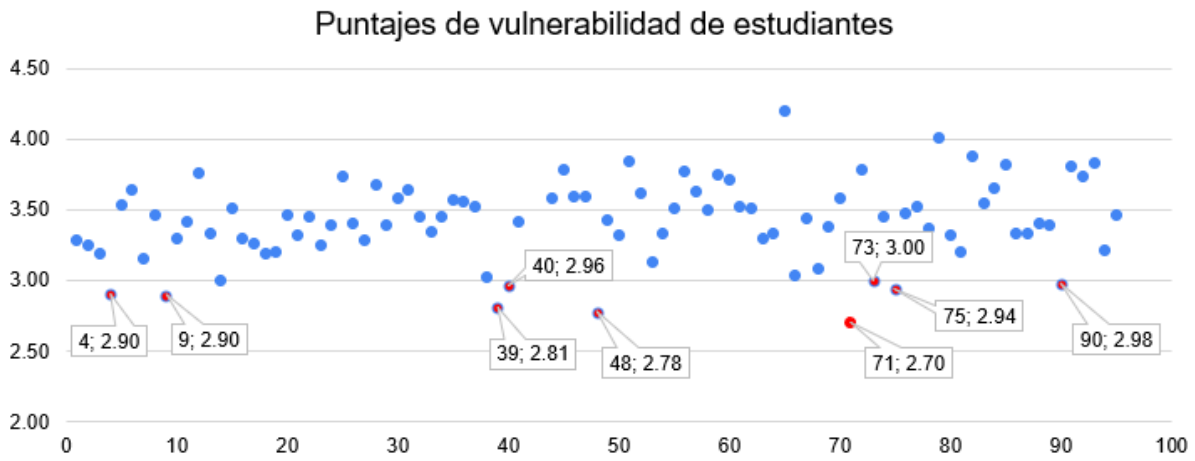
Dispersión de puntajes de estudiantes.



Dentro de la interpretación de los resultados de estudiantes, se puede identificar los nueve participantes que se encuentran marcados de color rojo (**Figura *18***) y que tienen un grado de vulnerabilidad medio, es decir, aquellos que obtuvieron un puntaje de 2 a 3.

Figura 18

Puntajes de vulnerabilidad de estudiantes.



Además, en **Figura *19*** se observan datos estadísticos de los rasgos de personalidad que presenta el grupo de estudiantes, en donde se evidencian los valores mínimos y máximos, la media y el rango en el que varían los puntajes.

Figura 19

Datos estadísticos por rasgos de personalidad en estudiantes.

Apertura a la experiencia	
Media	3.68
Mediana	3.71
Moda	3.29
Desviación es	0.61
Varianza de l	0.37
Rango	2.86
Mínimo	2.00
Máximo	4.86
Cuenta	95.00

Conciencia	
Media	3.60
Mediana	3.57
Moda	3.86
Desviación es	0.64
Varianza de l	0.41
Rango	2.57
Mínimo	2.43
Máximo	5.00
Cuenta	95.00

Extraversion	
Media	2.76
Mediana	2.71
Moda	2.14
Desviación es	0.71
Varianza de l	0.51
Rango	3.14
Mínimo	1.29
Máximo	4.43
Cuenta	95.00

Amabilidad	
Media	3.92
Mediana	4.00
Moda	4.14
Desviación es	0.50
Varianza de l	0.25
Rango	2.43
Mínimo	2.57
Máximo	5.00
Cuenta	95.00

Neuroticismo	
Media	2.96
Mediana	2.86
Moda	2.57
Desviación es	0.82
Varianza de l	0.68
Rango	3.86
Mínimo	1.00
Máximo	4.86
Cuenta	95.00

Hones/Humil	
Media	3.50
Mediana	3.57
Moda	3.57
Desviación es	0.51
Varianza de l	0.26
Rango	2.71
Mínimo	2.00
Máximo	4.71
Cuenta	95.00

Resultados de docentes clasificados por género

Para contrastar los rasgos de personalidad presentes en profesores, se muestra a continuación una gráfica de dispersión en donde se visualiza que para el rasgo Amabilidad y Honestidad / Humildad, las docentes mujeres tienen una media ligeramente mayor con respecto a sus semejantes masculinos, esto se puede verificar en **Tabla *9*** y está representado en **Figura *20***.

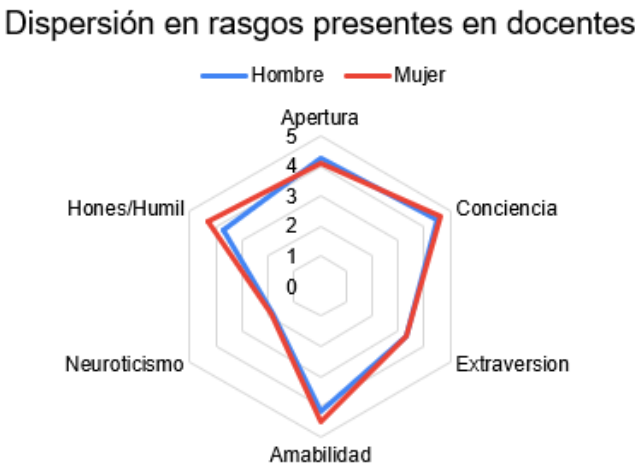
Tabla 9

Media por rasgos de personalidad en docentes clasificados por géneros.

	Media por géneros	
Rasgo	**Hombre**	**Mujer**
Apertura	4.24	4.06
Conciencia	4.47	4.6
Extraversión	3.33	3.29
Amabilidad	4.17	4.51
Neuroticismo	1.8	1.89
Hones/Humil	3.73	4.29

Figura 20

Dispersión en rasgos presentes en docentes.



Resultados de estudiantes clasificados por género

De forma similar se realizó una comparación de las medias calculadas para los rasgos de personalidad de los estudiantes, con esto se puede observar en

Figura ***21*** que para el neuroticismo, los estudiantes hombres tienen un puntaje menor con respecto a las estudiantes mujeres, con valores de 2.82 y 3.38, respectivamente, como se evidencia en **Tabla *10***.

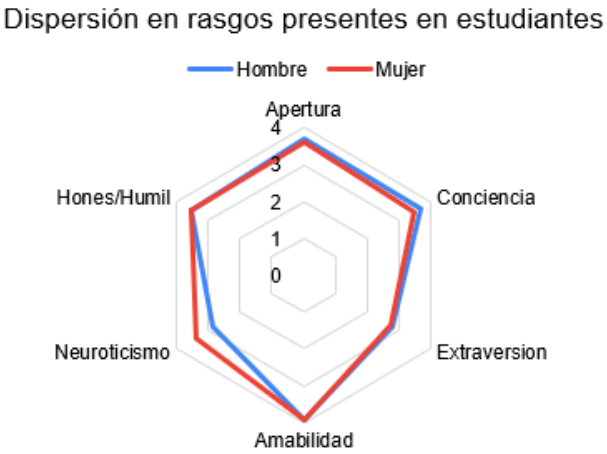
Tabla 10

Media por rasgos de personalidad en estudiantes clasificados por géneros.

	Media por géneros	
Rasgo	**Hombre**	**Mujer**
Apertura	3.7	3.63
Conciencia	3.65	3.46
Extraversión	2.77	2.73
Amabilidad	3.91	3.94
Neuroticismo	2.82	3.38
Hones/Humil	3.51	3.49

Figura 21

Dispersión en rasgos presentes en estudiantes.



Resultados de rasgos de personalidad de Docentes Vs. Estudiantes

Para finalizar, se muestra en **Tabla 11** *que no existe diferencia significativa para el rasgo de extraversión y amabilidad entre ambos grupos de interés, para el caso de apertura a la experiencia, conciencia y honestidad / humildad, los estudiantes tienen una media inferior a los docentes*

Figura *22*.

Los alumnos presentan un mayor nivel de neuroticismo a diferencia de los profesores, esto puede ser a causa de que los docentes al tener una edad mayor, también tienen mayor experiencia ante situaciones que se presentaron a lo largo de sus vidas, mientras que los estudiantes; por su corta edad, podrían tener algún temor o timidez por eventos nuevos en los que no sepan actuar y únicamente tomen decisiones a la ligera y sin medir las buenas o malas consecuencias que podrían acarrear.

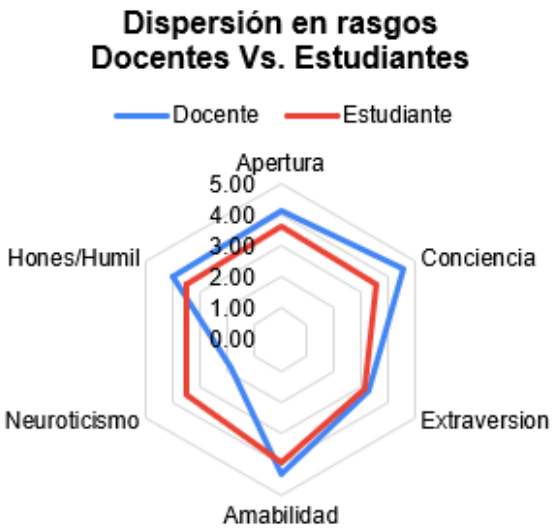
Tabla 11

Media por rasgos de personalidad Docentes Vs. Estudiantes

	Media por rol desempeñado	
Rasgo	**Docente**	**Estudiante**
Apertura	4.15	3.67
Conciencia	4.54	3.56
Extraversión	3.31	3.11
Amabilidad	4.34	3.92
Neuroticismo	1.84	3.51
Hones/Humil	4.01	3.50

Figura 22

Dispersión en rasgos Docentes Vs. Estudiantes.


Dispersión en rasgos
Docentes Vs. Estudiantes
Docente
Estudiante
Apertura
5.00
4.00
3.00
2.00
1.00
0.00
Conciencia
Extraversion
Amabilidad
Neuroticismo
Hones/Humil

Capítulo V

Conclusiones y recomendaciones

Conclusiones

Aunque los métodos y herramientas técnicas disponibles en el mercado sean las más sofisticadas y tengan resultados sobresalientes para proteger a los sistemas de información y mitigar los ataques que pueden afectar a los mismos, no serán suficientes si se deja a un lado el eslabón más débil en seguridad de la información; las personas, que pueden ser un medio por el cual los atacantes puedan aprovecharse de las vulnerabilidades humanas para causar perjuicios a una organización.

Al usuario final se le debe aplicar una evaluación psicológica con la cual se permita tener un perfil general de la personalidad; en base a sus rasgos característicos, para poder determinar qué tan vulnerable puede ser y que se convierta en una amenaza a la seguridad de la información, es por ello que este trabajo presenta el modelo de evaluación de personalidad en base a cuestionarios y la técnica de cálculo de vulnerabilidad.

Este modelo surge por medio del método ecléctico que integra los aspectos fundamentales de los modelos de personalidad FFM, MBTI y HEXACO, tanto para su guía metodológica como para la definición de la herramienta de evaluación de vulnerabilidad a ataques no técnicos como la ingeniería social.

De los resultados obtenidos, es importante mencionar que, de la muestra utilizada para este estudio, ninguno de los evaluados presentó un grado de vulnerabilidad crítico o alto. Del total de encuestados, el 2.73% y 89.09% de personas fueron clasificadas con una vulnerabilidad baja y leve, respectivamente. Por otra parte, se concluye que para el rasgo de neuroticismo existe una diferencia notable en la valoración entre docentes y estudiantes, estos últimos tienen un 33.4% más de neuroticismo que los profesores, lo cual indica que pueden tener cierta ventaja para no ser víctimas de ingeniería social, debido al miedo a realizar acciones por su falta de experiencia a posibles situaciones que los catedráticos pudieron haber enfrentado a lo largo de su vida.

Dentro de las investigaciones utilizadas para el presente trabajo, múltiples autores aclaran que no solamente es necesario evaluar la personalidad de las personas de forma separada, sino que también debe estar acompañada de factores demográficos, académicos e inclusive económicos y de la situación que en su momento se encuentren los individuos, esto para tener una descripción más detallada que permita moldear el comportamiento que puedan tener en determinadas circunstancias y que influencien sus acciones.

Recomendaciones

El modelo presentado en este trabajo podrá ser complementado con más herramientas que evalúen el comportamiento de las personas en entornos en línea, es decir, conectados a Internet debido a las nuevas modalidades de trabajo y estudio que se han generado por causa de la pandemia de COVID-19.

Así mismo se deberá incluir evaluaciones de conducta en redes sociales puesto que se convierten en un medio de contacto directo con las posibles víctimas y los atacantes. También se deben considerar más a profundidad otros aspectos sociales, económicos, demográficos, académicos y laborales como lo recomiendan los autores de la bibliografía utilizada para la elaboración de este trabajo.

A pesar de que la temática de este estudio es sobre medir la vulnerabilidad de las personas para ingeniería social, en futuros trabajos se puede investigar sobre el perfil de los atacantes y los rasgos de personalidad que moldean su conducta para desarrollar y aplicar distintos tipos de delitos informáticos. Esto se podría materializar con un estudio detallado del modelo de la Triada Oscura de Personalidad.

Por otra parte, se recomienda utilizar una muestra poblacional de mayor tamaño con el fin de corroborar los resultados obtenidos por el modelo para que en trabajos futuros se pueda diseñar una aplicación con inteligencia artificial que utilice aprendizaje supervisado para entrenar el modelo de forma controlada y que determine con mayor precisión el grado de vulnerabilidad de las personas en sistemas de información.

No se recomienda dejar a un lado el criterio de un profesional de la psicología que analice los resultados, puesto que la personalidad de las personas puede variar al depender de las circunstancias o necesidades y, además, el comportamiento humano puede modificarse con el paso de los años. Esta tarea no puede ser designada en su totalidad a una aplicación de software, puesto que la personalidad es una característica humana única y diferente entre todas las personas.

Referencias

Anaya, F. (07 de Octubre de 2021). *El "factor humano" en la ciberseguridad*. Obtenido de El Economista: https://www.eleconomista.es/opinion-blogs/noticias/11422755/10/21/El-factor-humano-en-la-ciberseguridad.html

Andrade, R. O., Cazares, M., & Fuertes, W. (2021). Cybersecurity Attacks During COVID-19: An Analysis of the Behavior of the Human Factors and a Proposal of Hardening Strategies. *Advances in Cybersecurity Management*, 37-53.

Arroyo Siruela, C. d. (23 de Septiembre de 2021). *El factor humano: elemento clave de la ciberseguridad*. Obtenido de Teléfonica Tech: https://empresas.blogthinkbig.com/factor-humano-elemento-clave-ciberseguridad/#:~:text=%C2%BFCu%C3%A1l%20es%20la%20importancia%20del,el%20phishing%2C%20de%20interacci%C3%B3n%20humana.

Banco Pichincha. (01 de Diciembre de 2020). *Qué son los ataques de ingeniería social y cómo evitarlos*. Obtenido de Banco Pichincha: https://www.pichincha.com/portal/blog/post/ataques-ingenieria-social

Benavides-Astudillo, E., Tipan-Guerrero, N., Castillo-Zambrano, G., Fuertes Díaz, W., Rodríguez Galán, G. E., Cazáres, M. F., & Nuñez-Agurto, D. (2022). A Framework Based on Personality Traits to Identify Vulnerabilities to Social Engineering Attacks. *Communications in Computer and Information Science*.

Bodnar, D. (04 de Agosto de 2022). *Ingeniería social y cómo protegerse*. Obtenido de Avast Academy: https://www.avast.com/es-es/c-social-engineering

Borkovich, D. J., & Skovira, R. J. (2019). Cybersecurity inertia and social engineering: Who's worse, employees or hackers? *Issues in Information Systems*, 139-150.

Calbet, J. (16 de Mayo de 2017). *Indicador MBTI. Tipos psicológicos Myers-Briggs (herramientas 7)*. Obtenido de NeuroQuotient: https://neuroquotient.com/indicador-mbti-indicador-de-tipos-psicologicos-de-myers-briggs-herramientas-7/

Cieciuch, J., & Strus, W. (2021). Toward a Model of Personality Competencies Underlying Social and Emotional Skills: Insight From the Circumplex of Personality Metatraits. *Frontiers in Psychology*.

Coindreau, R. (07 de Enero de 2022). *Evaluación 360 Grados: Guía Completa para Aplicarlas en 2022*. Obtenido de Integratec: https://www.integratec.com/blog/evaluacion-360-grados-guia-completa.html

Conteh, N. Y., & Royer, M. D. (2016). The Rise in Cybercrime and the Dynamics of Exploiting the Human Vulnerability Factor. *International Journal of Computer*, 1-12.

Cortez Pinto, M. G. (Marzo de 2013). Las Vulnerabilidades Humanas En Relación A La Seguridad Informática Para Evitar La Fuga De Información Confidencial En El Departamento De Recursos Humanos De La Universidad Técnica De Ambato. Ambato, Tungurahua, Ecuador: Universidad Técnica de Ambato.

Cusack, B., & Adedokun, K. (2018). The impact of personality traits on user's susceptibility to social engineering attacks. *Australian Information Security Management Conference* (págs. 83-89). Perth, Australia: Edith Cowan University.

Donnellan, M. B., Oswald, F., Baird, B. M., & Lucas, R. E. (2006). The Mini-IPIP Scales: Tiny-Yet-Effective Measures of the Big Five Factors of Personality. *Psychological assessment*, 192-203.

Equipo de AMBIT. (10 de Noviembre de 2020). *Tipos de Vulnerabilidades y Amenazas informáticas*. Obtenido de AMBIT BST: https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

Equipo de Aprender compartiendo. (30 de Mayo de 2017). *Factor Humano y su relación con la Ciberseguridad*. Obtenido de Aprender compartiendo: https://aprendercompartiendo.com/factor-humano-relacion-ciberseguridad/

Equipo de Black Swan Security. (14 de Abril de 2020). *What are Information Assets?* Obtenido de Black Swan Security: https://blog.blackswansecurity.com/2020/04/what-are-information-assets/

Equipo de GWC. (s.f.). *Seguridad de la información vs. seguridad informática*. Obtenido de GWC: https://gwc.global/seguridad-informatica-seguridad-informacion/

Equipo de ISOTools Excellence. (26 de Enero de 2017). *¿Seguridad informática o seguridad de la información?* Obtenido de ISOTools Excellence: https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

Equipo de LISA Institute. (03 de Marzo de 2021). *Diferencia entre Ciberseguridad, Seguridad Informática y Seguridad de la Información*. Obtenido de LISA Institute: https://www.lisainstitute.com/blogs/blog/diferencia-ciberseguridad-seguridad-informatica-seguridad-informacion

Equipo de Psicología y vida. (22 de Junio de 2013). *La personalidad - Estructura y tipos* . Obtenido de Psicología y vida: https://psicologayvida.blogspot.com/2013/06/la-personalidad-estructura-y-tipos.html

Equipo de REDVOISS. (20 de Octubre de 2021). *¿Qué son los activos de información en una empresa?* Obtenido de REDVOISS: https://blog.redvoiss.net/que-son-los-activos-de-informacion-en-una-empresa#:~:text=Los%20activos%20de%20informaci%C3%B3n%20en%20la%20empresa,o%20transmisi%C3%B3n%20de%20dicha%20informaci%C3%B3n.

Erbasi, A., Caliskan, A., & Akdeniz, G. (2022). The Effect of Personality Traits on Green Organizational Behaviour. *Journal of the Faculty of Economics and Administrative Sciences*, 154-185.

Fuertes, W., Arévalo, D., Castro, J. D., Ron, M., Estrada, C. A., Andrade, R., . . . Benavides, E. (2022). Impact of Social Engineering Attacks: A Literature Review. *Developments and Advances in Defense and Security*, 25-35.

García Muñoz, T. (Marzo de 2003). *Repositorio universitario.* Obtenido de Universidad Santana: http://www.univsantana.com/sociologia/El_Cuestionario.pdf

Halevi, T., Lewis, J., & Memon, N. (2013). A Pilot Study of Cyber Security and Privacy Related Behavior and Personality Traits. *WWW' 13: 22nd International World Wide Web Conference.* Rio de Janeiro: Association for Computing Machinery.

Kelland, M. D. (16 de Agosto de 2020). *Paul Costa and Robert McCrae and the Five-Factor Model of Personality*. Obtenido de LibreTexts Social Sciences: https://socialsci.libretexts.org/Bookshelves/Psychology/Book%3A_Personality_Theory_in_a_Cultural_Context_(Kelland)/10%3A_Trait_Theories_of_Personality/10.07%3A_Paul_Costa_and_Robert_McCrae_and_the_Five-Factor_Model_of_Personality

Kitchenham, B., Brereton, P., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering-A systematic literature review. *Information and Software Technology*, 7-15.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2014). Advanced social engineering attacks. *Journal of Information Security and Applications*. Obtenido de Advanced social engineering attacks

Lee, K., & Ashton, M. C. (s.f.). *Scale Descriptions*. Recuperado el 09 de Diciembre de 2022, de THE HEXACO PERSONALITY INVENTORY: https://hexaco.org/scaledescriptions

Majumdar, N., & Ramteke, V. (2022). Human elements impacting risky habits in cybersecurity. *AIP Conference Proceedings 2519*, (pág. 030006).

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception.* Indianapolis: Wiley.

Montañez, R., Golob, E., & Xu, S. (2020). Human Cognition Through the Lens of Social Engineering Cyberattacks. *Frontiers in Psychology*.

Mouton, F., Malan, M., Leenen, L., & Venter, H. S. (2014). Social Engineering Attack Framework. *Information Security for South Africa*.

Papatsaroucha, D., Nikoloudakis, Y., Kefaloukis, I., Pallis, E., & Markakis, E. K. (2021). A Survey on Human and Personality Vulnerability Assessment in Cybersecurity: Challenges, Approaches, and Open Issues. *arXiv preprint*.

Perallis Security. (s.f.). *14 TIPOS DE ATAQUES QUE APLICAN LA INGENIERÍA SOCIAL*. Recuperado el 14 de Noviembre de 2022, de Perallis Security: https://www.perallis.com/noticias/14-tipos-de-ataques-que-aplican-la-ingenieria-social

Quiel, S. (20 de Agosto de 2013). *Semantic Scholar.* Obtenido de Social Engineering in the Context of Cialdini's Psychology of Persuasion and Personality Traits: https://www.semanticscholar.org/paper/Social-Engineering-in-the-Context-of-Cialdini%27s-of-Quiel/2c8ca5aaf22aa144d06eea1bd5757aa704ec2a9d

Revnivykh, A. V., & Fedotov, A. M. (2015). Root Causes of Information Systems Vulnerabilities. *Indian Journal of Science and Technology*, 1-6.

Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). Planning for cybersecurity in schools: The human factor. *Educational Planning*, 23-39.

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., . . . Castillo Merino, M. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* 3Ciencias.

Ruiz Mitjana, L. (16 de Mayo de 2019). *¿Qué es la Personalidad según la Psicología?* Obtenido de Psicología y Mente: https://psicologiaymente.com/personalidad/que-es-personalidad

Stergiou, D. (2013). Social Engineering and InfluenceA Study that Examines Kevin Mitnick's Attacks through Robert Cialdini's Influence Principles. *(Tesis de Maestría).* Luleå University of Technology, Norrbotten County.

Teruel, S. (01 de Septiembre de 2021). *Conoce los principios de la seguridad informática y protege tu empresa*. Obtenido de Emburse Captio: https://www.captio.net/blog/principios-generales-seguridad-informatica

Uebelacker, S., & Quiel, S. (2014). The Social Engineering Personality Framework.

van Winsen, B. (27 de Abril de 2020). Determining secure digital behavior of individuals using HEXACO personality traits. Rotterdam, Países Bajos: Erasmus University Rotterdam.

Wang, Z., Zhu, H., & Sun, L. (2021). Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. *IEEE Access*, 11895-11910.

Weijer, S., & Leukfeldt, E. (2017). Big Five Personality Traits of Cybercrime Victims. *Cyberpsychology, Behavior, and Social Networking*.