Un Framework para Detectar la Vulnerabilidad de las Personas a Ataques de Ingeniería Social Basado en sus Rasgos de Personalidad

Castillo Zambrano, Gema Gabriela y Tipán Guerrero, Néstor Alejandro

Departamento de Ciencias de la Computación

Carrera de Ingeniería en Tecnologías de la Información

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

Ing. Benavides Astudillo, Diego Eduardo Mgs.

8 de septiembre de 2021

Informe de originalidad

NOMBRE DEL CURSO
NRC 6932 - MIC - PI PROFESIONALIZANTE

NOMBRE DEL ALUMNO
NESTOR ALEJANDRO TIPAN GUERRERO

NOMBRE DEL ARCHIVO
CastilloGema_TipanNestor-Tesis_IngenieriaSocial-Revisión de Originalidad

SE HA CREADO EL INFORME
8 sept 2021

Resumen

Fragmentos marcados	6	0,9 %
Fragmentos citados o entrecomillados	2	0,2 %

Coincidencias de la Web

books.google.com	4	0,5 %
listindiario.com	1	0,2 %
informador.mx	1	0,2 %
researchgate.net	1	0,1 %
ecu.edu.au	1	0,1 %

1 de 8 fragmentos
Fragmento del alumno ENTRECOMILLADO

...de la Universidad Edith Cowan en su trabajo denominado "**The impact of personality traits on user's susceptibility to social engineering attacks**

Mejor coincidencia en la Web

The impact of personality traits on user's susceptibility to social engineering attacks. In proceedings of the 16th Australian Information Security Management Conference (pp.

The impact of personality traits on user's susceptibility to social en https://ro.ecu.edu.au/ism/228/

2 de 8 fragmentos
Fragmento del alumno ENTRECOMILLADO

(Stewart & Dawson, 2018) en su investigación titulada "**How the modification of personality traits leave one vulnerable to manipulation in social engineering**

Mejor coincidencia en la Web

How the Modification of Personality Traits Leave One Vulnerable to Manipulation in Social Engineering. January 2018; International Journal of Information Privacy Security and Integrity 3(3).

How the Modification of Personality Traits Leave One Vulnerable to
... https://www.researchgate.net/publication/324528783_How_the_Modification_of_Personality_Traits_Leave_One_Vulnerable_to_Manipulation_in_Social_Engineeri

3 de 8 fragmentos
Fragmento del alumno MARCADO

...**Conservador: Especialmente favorable a mantener el orden social y los valores tradicionales frente a las innovaciones y los cambios radicales**.

Mejor coincidencia en la Web

La Real Academia de la Lengua: un conservador es especialmente favorable a mantener el orden social y los valores tradicionales frente a las innovaciones y los cambios radicales.

¿Quién es conservador, Presidente? | El Informador https://www.informador.mx/mexico/Quien-es-conservador-Presidente-20210228-0009.html

4 de 8 fragmentos
Fragmento del alumno MARCADO

...**Impulsivo: Que suele hablar o proceder sin reflexión ni cautela, dejándose llevar por la impresión del momento**

Mejor coincidencia en la Web

Impulsividad Definiciones clásicas — La Real Academia Española define impulsividad (s.f., definición 1) como «cualidad de impulsivo», siendo **impulsivo** (s.f., definición 2) «dicho de una persona: **que**...

Análisis funcional de la conducta humana: Concepto, metodología y ... https://books.google.com/books?id=UWL8DwAAQBAJ&pg=PT185&lpg=PT185&dq=impulsivo+suele+hablar+proceder+reflexi%C3%B3n+ni+cautela+dej%C3%A1ndose+llevar+impresi%C3%B3n&so

DIEGO EDUARDO BENAVIDES ASTUDILLO

Nombre de reconocimiento (DN): c=EC, o=SECURITY DATA S.A. 1, ou=ENTIDAD DE CERTIFICACION DE INFORMACION, serialNumber=160520182521, cn=DIEGO EDUARDO BENAVIDES ASTUDILLO
Versión de Adobe Acrobat Reader: 2021.005.20060

Ing. Benavides Astudillo, Diego Eduardo Mgs.

DIRECTOR

DEPARTAMENTO DE DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

CERTIFICADO DEL DIRECTOR

Certifico que el trabajo de titulación, **"UN FRAMEWORK PARA DETECTAR LA VULNERABILIDAD DE LAS PERSONAS A ATAQUES DE INGENIERÍA SOCIAL BASADO EN SUS RASGOS DE PERSONALIDAD"** fue realizado por los señores **Castillo Zambrano, Gema Gabriela y Tipán Guerrero, Néstor Alejandro** el cual ha sido revisado y analizado en su totalidad por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Santo Domingo de los Tsáchilas, 8 de septiembre de 2021

Firma:

DIEGO EDUARDO BENAVIDES ASTUDILLO

Nombre de reconocimiento (DN): c=EC, o=SECURITY DATA S.A. 1, ou=ENTIDAD DE CERTIFICACION DE INFORMACION, serialNumber=160520182521, cn=DIEGO EDUARDO BENAVIDES ASTUDILLO
Versión de Adobe Acrobat Reader: 2021.005.20060

Ing. Benavides Astudillo, Diego Eduardo Mgs.

C. C.: 1712883063

DEPARTAMENTO DE DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

RESPONSABILIDAD DE AUTORÍA

Nosotros, **Castillo Zambrano, Gema Gabriela y Tipán Guerrero, Néstor Alejandro**, con cedulas de ciudadanía **N° 1313602920 y 2350338139**, declaramos que el contenido, ideas y criterios del trabajo de titulación: **"UN FRAMEWORK PARA DETECTAR LA VULNERABILIDAD DE LAS PERSONAS A ATAQUES DE INGENIERÍA SOCIAL BASADO EN SUS RASGOS DE PERSONALIDAD"** es de mi/nuestra 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.

Santo Domingo de los Tsáchilas, 8 de septiembre de 2021

Firmas:

Castillo Zambrano Gema Gabriela

C.C.: 1313602920

Tipán Guerrero Néstor Alejandro

C.C.: 2350338139

DEPARTAMENTO DE DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

AUTORIZACIÓN DE PUBLICACIÓN

***N*osotros Castillo Zambrano, Gema Gabriela y Tipán Guerrero, Néstor Alejandro, con cédulas de ciudadanía** N° 1313602920 y 2350338139 **autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación:** "UN FRAMEWORK PARA DETECTAR LA VULNERABILIDAD DE LAS PERSONAS A ATAQUES DE INGENIERÍA SOCIAL BASADO EN SUS RASGOS DE PERSONALIDAD" **en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.**

Santo Domingo de los Tsáchilas, 8 de septiembre de 2021

Firmas:

Castillo Zambrano Gema Gabriela

C.C.: 1313602920

Tipán Guerrero Néstor Alejandro

C.C.: 2350338139

DEDICATORIA

Le dedico este trabajo a mi mamá Marlene Zambrano por creer en mí, por ser mi sustento de cada día y por el sacrificio que ha hecho siempre para ayudarme a lograr mis metas.

A mi hermano Marcelo Castillo, porque me ha motivado a seguir su ejemplo y demostrarle que con esfuerzo y dedicación todo es posible.

A las personas que han aportado cosas buenas en mi vida, me han brindado su cariño y me han apoyado moralmente.

Gema G. Castillo Z.

DEDICATORIA

Este trabajo va dedicado mis padres Néstor y Sandra, por todo el amor que me han dado, su paciencia, siempre estar a mi lado, contar con ellos en cualquier momento de necesidad y el gran esfuerzo que han realizado para que hoy este a puertas de culminar una carreara universitaria.

A mis Hermanos, por darme ánimos día tras día y haber estado para mí siempre que los necesite.

A las personas que a pesar de no tener un vínculo familiar me han brindado su apoyo, confianza y más sinceros sentimientos.

Néstor A. Tipán G**.**

AGRADECIMIENTOS

Agradezco a mi madre Marlene Zambrano, por brindarme su amor y su apoyo incondicional, por ser mi motivación para seguir adelante, es mi heroína por evitar que me rinda en esta etapa de mi vida hasta que logre cumplir con este objetivo, más que una madre es mi mejor amiga y siempre me ayuda a resolver los problemas.

A Dayana Guevara por ser una persona muy especial en mi vida, que siempre me ha demostrado su cariño, me ha apoyado y me ha inspirado a ser una mejor persona.

A la Universidad de las Fuerzas Armadas ESPE Santo Domingo, a la Carrera de Ingeniería en Tecnologías de la Información y al personal docente que supo brindarnos todo su apoyo y ayudarnos a crecer como profesionales y personas de bien.

A nuestro director de tesis el Ing. Diego Eduardo Benavides por guiarnos con gran profesionalismo, aportar con su conocimiento y experiencia durante todo el proceso de realización de la investigación.

A mi compañero de tesis Néstor Tipán, por ser un gran colega y un buen amigo, por su entusiasmo para desarrollar este proyecto con pensamiento creativo y actitud positiva.

A mis compañeros de estudio, que estuvieron siempre dispuestos a ayudar en las situaciones difíciles de nuestra carrera.

Gema G. Castillo Z.

AGRADECIMIENTOS

A mi familia por siempre brindarme su ayuda, buenos deseos y su apoyo para lograr culminar esta etapa de mi vida. Gracias a mis padres Néstor y Sandra, por haberme educado y aconsejado de la mejor manera posible, además de brindarme todo lo que ha estado a su alcance, todo lo que soy se los debo a ellos.

A la Universidad de las Fuerzas Armadas ESPE Santo Domingo, a la Carrera de Ingeniería en Tecnologías de la Información y al personal docente que supo brindarnos todo su apoyo y ayudarnos a crecer como profesionales y personas de bien.

A nuestro director de tesis el Ing. Diego Eduardo Benavides por guiarnos con gran profesionalismo, aportar con su conocimiento y experiencia durante todo el proceso de realización de la investigación.

A Nicole Zambrano, por ser una persona muy especial en mi vida que me dedicado todo su apoyo, ha estado ahí siempre que he necesitado a alguien, además de ayudarme a corregir mis errores y mejorar como persona.

A mi compañera de tesis Gema Castillo por su amistad, su apoyo, ser una gran persona, además de la dedicación y compromiso que han permitido que se lleve a cabo esta investigación.

Agradezco a todas las personas que de una u otra manera han colaborado y contribuido a mi formación académica.

Néstor A. Tipán G.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El día de hoy, prácticamente todas las personas usamos dispositivos digitales conectados a internet, pero un problema que también se ha incrementado con esta masificación, es el número de ciberdelincuentes que usan técnicas de Ingeniería Social para extraer información sensible de los usuarios, aprovechando los rasgos de personalidad de ellos, tales como la amabilidad, el desconocimiento de medidas básicas de seguridad, o exceso de confianza. Es así como el objetivo principal de este estudio es ofrecer una herramienta que permita determinar, que personas son más vulnerables a ataques de Ingeniería Social. Para combatir este tipo de ataque, se ha desarrollado en este documento, un Framework basado en los rasgos de personalidad, que permite conocer, qué personas son más vulnerables que otras. La metodología para llegar al objetivo se basó en primero, determinar cuáles son los rasgos más comunes que se relacionan con la vulnerabilidad, luego, determinar los rasgos de personalidad de un grupo encuestado, y finalmente, empatar los rasgos más vulnerables con los rasgos de personalidad de los encuestados. Los rasgos de personalidad en los que se enmarcó nuestra investigación son los de Five Factor Model, modelo en el cual se determinó que los rasgos que nos hacen más vulnerables son: Apertura (28.8%), seguido por Agradabilidad (27.9%), Concientización (20.2%), Neuroticismo (11.5%) y Extraversión (11.5%).

Palabras clave:

- **RASGO PERSONAL**
- **CIBERSEGURIDAD**
- **INGENIERÍA SOCIAL**
- **MODELO DE LOS CINCO FACTORES**
- **FRAMEWORK**

ABSTRACT

Nowadays, practically everyone uses digital devices connected to the Internet, but a problem that has also increased with this massification, is the number of cybercriminals who use social engineering techniques to extract sensitive information from users, taking advantage of their personality traits, such as friendliness, ignorance of basic security measures, or overconfidence. Thus, the main objective of this study is to provide a tool to determine which people are more vulnerable to social engineering attacks. To combat this type of attack, a Framework based on personality traits has been developed in this document, which allows to know which people are more vulnerable than others. The methodology to reach the objective was based on first, determining which are the most common traits that are related to vulnerability, then, determining the personality traits of a surveyed group, and finally, matching the most vulnerable traits with the personality traits of the respondents. The personality traits in which our research was framed, are those of Five Factor Model, a model in which it was determined that the traits that make us more vulnerable are: Openness (28.8%), followed by Agreeableness (27.9%), Conscientiousness (20.2%), Neuroticism (11.5%) and Extraversion (11.5%).

Key words:

- **PERSONAL TRAIT**
- **CYBERSECURITY**
- **SOCIAL ENGINEERING**
- **FIVE FACTOR MODEL**
- **FRAMEWORK**

CAPÍTULO I

INTRODUCCIÓN

En la actualidad, la Ingeniería Social es utilizada por los ciberdelincuentes con el fin vulnerar la seguridad de la información (Benavides et al., 2020b) y robar datos para su beneficio, por medio de técnicas que se basan en la manipulación y el engaño, precisamente esas técnicas de fraude van dirigidas a los usuarios de los sistemas, personas que simplemente utilizan las tecnologías para realizar trámites y transacciones en línea, o aquellos que usan las redes sociales y el correo electrónico para comunicarse, pero no están al tanto de los daños que les pueden ocurrir si entregan su información sin tomar precauciones.

Al día de hoy, los atacantes se enfocan en los seres humanos en lugar que los sistemas informáticos o las computadoras, puesto que los ciberdelincuentes tratan de lograr sus malas intenciones mediante las debilidades de los usuarios finales (Papatsaroucha et al., 2021). Los permanentes avances de la tecnología demandan el desarrollo de sistemas que sean seguros y el mejoramiento de los mecanismos de defensa contra los atacantes. Pero esas labores resultan ser muy complicadas a causa de varios factores que se deben tomar en cuenta como, por ejemplo, los atributos tecnológicos, los patrones de ataque, el comportamiento de los ciberdelincuentes y los ingenieros sociales, entre otros.

Objetivos

Objetivo General

Proponer un modelo que permita determinar que personas son más vulnerables a ser víctimas de ataques de Ingeniería Social, en base a sus rasgos de personalidad.

Objetivos Específicos

- Leer artículos y recopilar información sobre las características más comunes que hacen susceptibles a las personas de ataques de Ingeniería Social.

- Extraer los rasgos de personalidad y psicológicos de las personas obtenidos de los principales artículos.

- Clasificar y tabular las características tomando como base el modelo de los cinco factores de personalidad.

- Realizar una encuesta para determinar los rasgos de la personalidad y tabular los datos obtenidos.

- Desarrollar el modelo propuesto para determinar la vulnerabilidad de las personas en base a la encuesta de personalidad y a la clasificación de los rasgos de personalidad.

CAPÍTULO II

MARCO TEÓRICO

Antecedentes

Las vulnerabilidades de las personas representan una amenaza grave para la seguridad de la información, debido a varios factores humanos como la predisposición para ayudar o ser recíprocos con los demás, así como las características personales, sociales y culturales son indicios de susceptibilidad a ataques basados en el fraude y el engaño.

En este aspecto, los investigadores (Cusack & Adedokun, 2018) de la Universidad Edith Cowan en su trabajo denominado "*The impact of personality traits on user's susceptibility to social engineering attacks*" examinan el impacto de la personalidad de los usuarios en base a la probabilidad de susceptibilidad a los ataques de Ingeniería Social. En esta investigación se realizaron cinco entrevistas a expertos para determinar cuáles son los rasgos que hacen que algunas personas sean más o a veces menos vulnerables a los ataques de Ingeniería Social. Los rasgos de personalidad en esta investigación se obtuvieron con el modelo de personalidad de los cinco grandes factores para correlacionarse con los datos de la entrevista. Los resultados de este trabajo sugieren que los usuarios con puntuaciones altas en rasgos de amabilidad y extraversión son propensos a ser más susceptibles a los ataques de Ingeniería Social que otros.

(Stewart & Dawson, 2018) en su investigación titulada *"How the modification of personality traits leave one vulnerable to manipulation in social engineering",* realizan un estudio no experimental, exploratorio y cuantitativo, basándose en los rasgos de personalidad determinó lo que causa que una persona sea susceptible a la manipulación y explotación del engaño en el contexto de Ingeniería Social. En este estudio los autores realizaron encuestas a una organización para presentar de manera numérica los resultados de los rasgos de personalidad. Los autores determinaron qué rasgos de personalidad o

grupos de rasgos tienen el mejor desempeño en la determinación del riesgo de susceptibilidad al engaño. La variable de susceptibilidad dependiente fue una agrupación puntuada del principio de factores de influencia que incluían confianza, vulnerabilidad, amenaza y obediencia.

(Albladi & George, 2017) en su artículo titulado cómo “Personality Traits and Cyber-Attack Victimisation: Multiple Mediation Analysis”, obtienen información sobre los cinco rasgos de personalidad (conciencia, neuroticismo, extraversión, amabilidad y apertura a la experiencia) en la susceptibilidad de los usuarios a la vulnerabilidad de ciberataques. Los autores proponen un modelo de mediación, que incluye los cinco rasgos de personalidad que afectan la probabilidad del usuario para que sea víctima de ciberataques. El estudio llevó a cabo un experimento basado en escenarios con 316 participantes para probar el modelo. Los resultados empíricos indican que los cinco rasgos de personalidad, excepto la apertura, tienen un efecto indirecto significativo en la susceptibilidad de los usuarios a la vulnerabilidad de ciberataques.

Ingeniería Social

Se denomina Ingeniería Social al conjunto de acciones que se realizan con el fin de engañar a los usuarios para conseguir que estos entreguen su información confidencial o infecten sus computadores de algún tipo de virus o malware, para luego hacer uso ilícito de dicha información (Benavides et al., 2020).

Para considerarse como un ataque de Ingeniería Social debe estar involucrada la manipulación de las personas a través de técnicas o estrategias psicológicas, para conseguir que la víctima realice una acción indebida sin percatarse que lo está haciendo, entre las cuales están la obtención de información, dar acceso a terceros, otorgar permisos de alto nivel, instalar software malicioso.

La Ingeniería Social se basa en el usuario quien es el eslabón más débil, debido a que se puede crear miles de seguridades y políticas para tratar de reducir cualquier tipo de ataque, pero siempre debe existir la intervención humana, generando las brechas o debilidades que serán aprovechadas por los

atacantes al mínimo descuido. Es por ello que los expertos en seguridad informática, suelen decir que la única computadora que está segura es la que se encuentra desconectada, a lo que, los expertos en Ingeniería Social responden que en algún momento se logrará convencer a alguien de conectarla (Castellanos, 2018).

La Ingeniería Social podría considerarse como un tipo de arte, ya que pocas personas son capaces de alcanzar tal grado de manipulación hacia los demás, lo se conoce como habilidades sociales. Gracias a este tipo de técnicas, los crackers se evitan el estar horas intentando romper una contraseña y prefieren conseguir las credenciales o que les asignen una nueva contraseña simplemente llamando al servicio técnico (Kaspersky Lab, 2021).

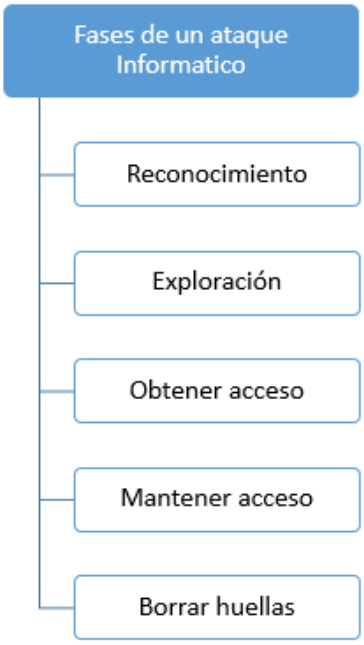
Los ciberdelincuentes suelen aprovecharse de muchos factores que rodean al usuario común, para alcanzar su objetivo. Debido a los constantes avances que tiene la tecnología día tras día, los ataques y métodos que se usan en la Ingeniería Social se vuelven cada vez más complejos (Kaspersky Lab, 2021).

Fases de un ataque informático

Según (Rezabala & Moreira, 2020) al identificar las fases o etapas de un ataque informático, podremos comprender la manera de actuar de los atacantes, ya que esto permite analizar en perspectiva, cómo se lleva a cabo un ataque y qué características toma en cuenta el adversario para identificar a su víctima. En la Figura 1 se presenta de forma resumida las fases de un ataque informático.

Figura 1

Fases de un ataque de informático.



Nota: Adaptada de Análisis de las incidencias e impactos de ataques de Ingeniería Social o ciberdelitos en la Carrera De Ingeniería Civil De La Facultad De Ciencias Matemáticas Y Físicas, (p. 20), R. Rezabala & K. Moreira, 2020.

Reconocimiento

En esta fase el atacante inicia el proceso de recolección de información de la víctima a la cual se afectará ya sea económica o socialmente. Esto le permite establecer una estrategia, la cual se basará en las vulnerabilidades de la víctima.

Exploración

Esta fase consiste en hacer un filtrado de la información vulnerable de la víctima, e identificar más a fondo las vulnerabilidades o fallas de seguridad que tenga en su sistema y que puedan ser usadas en su contra.

Obtener acceso

Es la fase en donde se establece e inicia el ataque teniendo en cuenta las vulnerabilidades o fallas de seguridad identificadas, de manera que estas serán puestas a prueba con el ataque adecuado según las vulnerabilidades identificadas de la víctima.

Mantener acceso

Una vez que el atacante haya accedido al sistema de la víctima su prioridad es mantenerlo habilitado, de manera que creara o usará distintas técnicas para dejar una puerta trasera en el sistema.

Borrar huellas

Al haber accedido y al mantener el acceso, el atacante deberá ocultar o eliminar cualquier tipo de rastro que demuestre que se haya vulnerado el sistema de la víctima, de manera que pueda seguir teniendo acceso y no ser detectado cada vez que lo haga.

Phishing

Se conoce como Phishing a la mezcla entre Ingeniería Social y algún tipo de exploit desarrollado para obtener información de los usuarios. Este tipo de ataques se lo suele realizar con la intención de obtener ganancias económicas, ya sea por robo, estafa o en casos más extremos por chantaje o extorsión (Benavides et al., 2020a).

Por otro lado, el Anti-Phishing Work Group (APWG) define al Phishing como un módulo criminal que se emplea para fines delictivos hacia personas u organizaciones. Comúnmente se suelen implementar varios medios para llegar a la victima de esta manera resulta mucho más creíble y difícil de percibir su falsedad (Abeywardana et al., 2016).

Los ataques de Phishing más comunes son los que se realizan por medio de correos electrónicos maliciosos, en los cuales suele estar adjunto el enlace hacia algún sitio web falso. Este tipo de páginas web suelen tener

diseños muy bien estructurados, siendo casi imposible de diferenciar para un ojo inexperto una página original de una copia maliciosa, es ahí donde suelen los usuarios caer como presas de los ciberdelincuentes, y terminan entregando información muy valiosa o descargando algún tipo de malware (Benavides et al., 2020a).

El Phishing se puede dar mediante correos electrónicos o algún otro sistema en línea. Además de los ataques en línea, tenemos los que se realizan por medio de una llamada telefónica a este tipo de ataques se los conoce como Vishing, en que los atacantes utilizan un sistema de voz interactiva para simular las respuestas que daría un servicio real de un Banco o alguna empresa aleatoria (Alazri, 2016).

La manera en la que se perpetra el ataque suele ser muy similar en todos los casos, realizar una llamada a un número falso, registrarse en algún sitio sospechoso o entregar datos que comúnmente no se suelen pedir, todo esto con el fin de recopilar la información de la víctima y usarla con distintos fines o propósitos (Alazri, 2016).

Varios expertos en el tema concuerdan que una página de Phishing, es aquella que trata de asemejarse a otro sitio web, por ejemplo, a la página oficial de un banco, red social o de algún sitio de ofertas, todo esto con el fin de confundir al usuario a tal punto que realice involuntariamente lo que el atacante desee (Benavides et al., 2020a).

A finales de 2018, dos hombres de Missouri perpetraron un robo de 14 millones de dólares de una empresa, lo más sorprendente de este caso es que no tenían grandes conocimientos sobre piratería informática, más bien implementaron técnicas de Ingeniería Social y Phishing para lograr su cometido (Russo, 2019).

Clasificación de los ataques de Phishing:

Los ataques de Phishing se pueden clasificar de la siguiente manera:

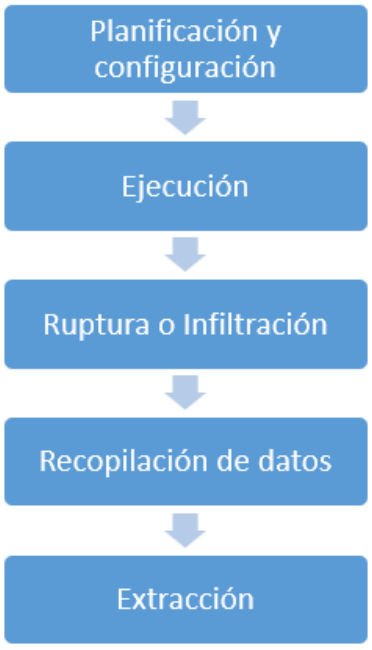
- Por el servicio que se vea afectado: Entidades bancarias, Juegos online, Sistemas de soporte técnico, páginas de actividad económica como compraventa o de subastas, promociones falsas, Redes Sociales, servidores de almacenamiento en la nube, entre otros servicios online (Benavides et al., 2020a).
- Por el modus operandi: Software de tipo Malware o virus, mensajes fraudulentos, correos falsos, DNS o Pharming, Search Engine Phishing, Man in the middle Phishing (Benavides et al., 2020a).

Etapas de un ataque Phishing

Como se puede observar en la Figura 2, un ataque de Phishing consta de 5 etapas que son: planificación y configuración, ejecución, ruptura o Infiltración, recopilación de datos y extracción. A continuación, se proporciona una descripción detallada de cada etapa de este ataque.

Figura 2

Etapas de un ataque de Phishing.



Nota: Adaptada de Caracterización de los ataques de Phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura (p. 97–104), de E. Benavides, 2020, *Ciencia y Tecnología, 13*(1). CC BY NC SA 2.0.

Planificación y configuración:

En la primera fase de un ataque de Phishing se realiza la identificación de los objetivos que pueden ser desde un usuario, una organización o inclusive un país. La principal meta es obtener información relevante de las víctimas, tales como sus cuentas financieras, cuentas de usuario y claves de acceso. Luego se procede a crear y configurar los ataques para difundirlos a través de varios medios como páginas web o emails con información falsa y maliciosa y mensajes directos en redes sociales, entre otros (Benavides et al., 2020a).

Ejecución:

En la segunda fase se realiza la ejecución del ataque, en donde el atacante lleva a cabo el envío de correos falsos a sus víctimas. Dichos correos electrónicos suelen ser muy convincentes, por lo general se encuentran enmascarados como si fuesen correos legítimos de una organización o institución reconocida por su buena reputación y que solicita la información sensible del remitente con un fin aparentemente legal, como por ejemplo la actualización de sus datos. Estos correos tratan de persuadir a la víctima para que responda a la solicitud inmediatamente haciendo clic en un enlace fraudulento (Benavides et al., 2020a).

Ruptura o Infiltración:

En la tercera fase, el objetivo o usuario víctima, opta por dar clic en el enlace malicioso, descarga un malware, o simplemente entrega información directamente por email u otro medio. Una vez realizada esta acción pueden ocurrir vacíos sucesos, dependiendo de cómo se haya diseñado y planificado el ataque. Lo más común es que la víctima sea redirigida a una página web falsa para que proporcione sus datos, o también se puede dar el caso de instalarse automáticamente un malware en su equipo, dando acceso al atacante para que pueda realizar acciones maliciosas sin que el usuario se dé cuenta (Benavides et al., 2020a).

Recopilación de datos:

En la cuarta fase el atacante tiene acceso al sistema o a la información de su objetivo y hace la extracción de los datos que le sean más importantes. Como, por ejemplo, las credenciales de cuentas bancarias que le permitan al atacante acceder a ellas y tomar el dinero ahorrado de la víctima. Por otro lado, los ataques que tienen un malware le permiten el acceso al atacante de manera remota al equipo de su objetivo y extraer la información, o realiza los cambios que más le convengan para seguir recopilando datos de la víctima (Benavides et al., 2020a).

Extracción:

En esta última fase, el atacante se deshace de las evidencias que se hayan podido generar durante el ataque, ya sean las páginas web o cuentas falsas de donde haya enviado los correos. Por último, realiza una evaluación para medir el éxito del ataque y mejorarlo para utilizarlo nuevamente en el futuro con otros ataques (Benavides et al., 2020a).

Spear Phishing

El Spear Phishing se ha convertido en uno de los mayores problemas para la seguridad informática de las empresas, ya que un gran porcentaje de empresas se han visto envueltas en algún caso de ataque este tipo (Thomas, 2018).

Este tipo de ataques son dirigidos, es decir, se utilizan métodos de Ingeniería Social mediante correos electrónicos que por lo general se suelen combinar con llamadas telefónicas en la que seguirán con la misma temática que se encuentra en el correo. Esto lo hará mucho más creíble, incluso para los sistemas de filtrado. El atacante recopilara información de su víctima y lo estudiara por varios días, se acercara paulatinamente para ganarse su confianza y finalmente hará la extracción de información crucial (Abeywardana et al., 2016).

Según el Enterprise Phishing Susceptibility and Resiliency Report, los ataques de Spear Phishing y Phishing son los ciberataques más comunes a

nivel mundial. Aproximadamente el 90% de los ciberataques están basados en algún derivado de Phishing y el restante son ataques a los gobiernos (Abeywardana et al., 2016).

Aproximadamente un tercio de los correos electrónicos de Phishing son abiertos por los usuarios en 1 minuto y 40 segundos, de ellos el 12% en menos de 4 minutos hace clic en enlaces adicionales o ejecuta archivos adjuntos dentro de estos correos electrónicos. La información que se suele implementar de cebo por lo general son ofertas de membrecías gratuitas, mensajes de redes sociales, información pública o cualquier otro tipo de mensaje que llame la atención de la posible víctima (Abeywardana et al., 2016).

SIM Swapping

Se conoce como SIM Swapping al proceso de suplantar la identidad de la víctima, para así conseguir un cambio de número telefónico o inclusive, un duplicado de su actual tarjeta SIM, de este modo puede hacerse con la información de su víctima con mucha más facilidad (Russo, 2019).

Una vez que el atacante tiene acceso al número de su víctima, forzará él envió de mensajes de texto de validación de distintas fuentes, entre las cuales pueden estar entidades bancarias, redes sociales o inclusive solicitar dinero a los conocidos de la víctima. Esto es un grave problema para los sistemas actuales, que trabajan con identificación de dos pasos, basados en la autenticación mediante un código enviado por SMS, ya que al tener acceso al número registrado por la víctima, el atacante puede solicitar un pin de acceso a una cuenta, o un cambio de contraseña, o si ya la conoce, no hay manera en la que se le pueda prohibir el acceso (Russo, 2019).

El tipo de ataque SIM Swapping puede sonar muy complejo y difícil de realizar, pero la realidad es que es todo lo contrario, ya que el atacante puede pretender haber sido víctima de algún robo o pérdida de su tarjeta SIM y solicitar una nueva, con el mismo número directo de la empresa de telefonía. Otro tipo de casos que suele darse es que los mismos operadores de estas empresas telefónicas estén involucrados en el ataque (Russo, 2019).

En la gran mayoría de artículos y blogs de SIM Swapping, no se apunta al ciberdelincuente como el principal problema, sino a los propios proveedores de telefonía, debido a que sus empleados pueden llegar a tener mucha información personal de los usuarios, y los procesos para cambio de numero o asignarle una nueva tarjeta SIM no son muy complejos o estrictos, sin tener en consideración que dichos empleados podrían ser susceptibles a recibir algún tipo de soborno por dicha información (Russo, 2019).

Scareware

Los Scareware son un tipo de software malicioso que se utiliza con el propósito de vulnerar la privacidad de los usuarios de entidades financieras. Este tipo de software suele ser muy difícil de detectar por las medidas de seguridad tradicionales como los antivirus, ya que deberían estar constantemente actualizándose o porque carecen de la capacidad de detectar instancias ocultas (Shahzad & Lavesson, 2011).

Scareware representa un software que se hace pasar por aplicaciones de seguridad de tipo antivirus/anti-malware. Los Scareware en realidad suelen proporcionar un mínimo nivel de seguridad o inclusive ninguna seguridad. Este tipo de software es tan especializado en suplantar programas verdaderos, que genera cuadros de dialogo, escaneos falsos del sistema, alertas, inclusive listas de archivos infectados los cuales ni siquiera existen en nuestro computador o que son incompatibles para nuestro sistema operativo. Estos proceso de escaneo falso se usan para asustar a la víctima, y en su afán de solucionar sus supuestos problemas, compre una membresía falsa para el Scareware, descargue otro tipo de programas, añada archivos adicionales (comúnmente Troyanos), o muchas veces funciona a manera de keyloger para sustraer todas nuestras credenciales de manera oculta (Shahzad & Lavesson, 2011).

Pretexting

El Pretexting es una estrategia usada en la Ingeniería Social para generar confianza entre el atacante y la víctima, ya sea haciéndose pasar por un conocido, un jefe o compañero de trabajo. Comúnmente se suele recabar un poco de información adicional antes del ataque para hacerlo mucho más

verídico. Esto se realiza con la intención de engañar a la víctima y que proporcione información valiosa de su empresa o datos de gran significado (Alazri, 2016).

Para que el Pretexting sea exitoso, no basta con escribirle a alguien diciendo que eres un amigo de antes, estos atacantes deben convertirse en la persona que dicen ser, para ello deben interpretarlo de manera correcta, tener antecedentes de la relación que estos manejen, adquirir su personalidad y actitud, es por ello que se dice que a la Ingeniería Social hasta cierto punto se la puede considerar como un tipo de arte (Alazri, 2016).

Según (Li, 2017), el Pretexting es el acto de crear un escenario ficticio en el cual se trata de persuadir a la víctima para que divulgue información personal, de algún tipo de actividad que lleva a cabo, o que realice alguna acción inconsciente. Es por ello que los atacantes deben realizar el estudio de la víctima y de su ambiente. Uno de los casos más comunes que suele darse, es en el que el atacante se hace pasar por personal técnico de TI, y de este modo conseguir credenciales reales, de este modo perfeccionaran un segundo ataque, o usaran la información proporcionada por la empresa contra ellos mismos (Li, 2017).

El Pretexting es uno de los ataques de Ingeniería Social más difíciles de llevar a cabo, por su complejidad y el tiempo que le toma a los atacantes, pero de igual manera, uno de los que mayores impactos causa a la víctima. Es tan efectivo que no se lo utiliza únicamente en el ámbito informático, sino que también es empleado por supuestos médicos, abogados, adivinos o curanderos que ofrecen curaciones milagrosas (Alazri, 2016).

Tailgating

Los ataques de Tailgating o también llamados a cuestas o de acceso físico, se da cuando el ciberdelincuente ingresa a un lugar físico de trabajo utilizando credenciales falsas, para extraer información confidencial directamente de los computadores. Para realizar dicho ataque suelen vestirse con ropa similar a la del personal o inclusive con los mismos uniformes de la organización, y socializaran con los demás empleados, de este modo no

levantaran sospechas. Por ejemplo, los atacantes le pedirán a un empleado que les ayude manteniendo abierta una puerta porque olvido su tarjeta de acceso o tarjeta RFID (identificación por radiofrecuencia), una vez dentro pueden pedir prestada alguna computadora para dejar instalando software malicioso o inclusive algún tipo de escritorio remoto para poder acceder a voluntad (Salahdine & Kaabouch, 2019).

El Tailgating suele estar acompañado con ataques con tarjeta RFID, ya que al ser uno de los sistemas de identificación más utilizados por las empresas por su bajo costo y amplio uso, los atacantes pueden explotar sus vulnerabilidades para conseguir el acceso de puertas bloqueadas o entradas restringidas. Estos ataques se pueden realizar en la capa física de los sistemas, quebrantando temporal o permanentemente los lectores de las tarjetas RFID, permitiéndoles el acceso con una copia de dichas tarjetas. A nivel de la capa de red se puede manipular la red que maneja estas tarjetas RFID y registrar una nueva tarjeta, o interceptar las señales para intercambiar datos falsos entre estos dispositivos (Salahdine & Kaabouch, 2019).

Quid Pro Quo

El ataque Quid Pro Quo o también llamado algo por algo, es conocido porque busca llegar a un acuerdo mutuo con la victima haciendo uso de técnicas de engaño de Ingeniería Social. El supuesto beneficio que se le ofrece a la víctima, generalmente asume la forma de un servicio, mientras que la recompensa del atacante con frecuencia toma la forma de un bien o información personal (Fan et al., 2017).

A este tipo de ataque se lo asocia comúnmente con hacerse pasar por servicio técnico falso que convenientemente requerirá información confidencial para poder solucionar el problema por el que esté pasando la víctima. El objetivo es lograr infectar con algún malware el dispositivo (Breda et al., 2017)**.**

Técnicas usadas en Tailgating y Quid Pro Quo

Estos ataques se basan principalmente en la recopilación de información, de manera que se obtenga un beneficio de esta. Estos tipos de ataques están

orientados a vulnerar la confianza de la víctima sobre las demás personas, ya sea haciéndose pasar por otra persona o simplemente siendo sociable, explotando las características que comparten las personas en el mundo laboral (Enric Garcia Romero, 2019). Para que estos ataques tengan mayor probabilidad de éxito, se toman en cuenta las siguientes características:

- **Apelar al ego de la persona**: Esta técnica consiste en realizar un halago a la persona de la cual se quiera adquirir algún tipo de beneficio o información, una vez que la víctima haya aceptado el “algo”, se aprovechará la modestia o falsa modestia que está presente, de manera que se pueda establecer una conversación más detallada sobre el tema que se esté tratando.
- **Expresar interés mutuo:** Consiste en que el atacante mostrara interés sobre la víctima ofreciéndole ayuda sobre temas de los que ambos necesiten información, de tal manera, que así el atacante tendrá el control sobre la situación y compartirá información que le interese a la víctima, para que esta brinde información de interés sobre el tema.
- **Hacer una afirmación falsa intencionalmente:** Es una técnica simple con la cual se comparte datos o información falsa durante una charla con trabajadores de alguna empresa sobre algún tema del cual tengan mucho conocimiento, logrando provocar así, que estos trabajadores lo corrijan dando datos reales al atacante.
- **El consentimiento asumido:** Esta técnica se enfoca en mostrar un cierto conocimiento del tema entre varios expertos, de manera que el atacante podrá demostrar, aunque sea de manera muy simple o dando su opinión, que tiene conocimiento del tema, logrando mantenerse dentro de la conversación y haciendo que los expertos sigan compartiendo información, asumiendo que el atacante ya la conoce.
- **Utilizar los efectos del alcohol:** Se trata de hacer bajar la guardia de la víctima ofreciendo bebidas alcohólicas, de manera que esta revele información que en estado de sobriedad no lo haría.
- **El arte de hacer preguntas:** Hacer preguntas oportunas y en el momento adecuado para obtener distinto tipo de información que el atacante requería.

Vishing

El Vishing consiste en aprovechar la tecnología de voz IP (Voice over Internet Protocol, o VoIP), para convencer a la víctima previamente seleccionada para que proporcione información de carácter confidencial, personal o financiera, es por esta razón que el termino Vishing proviene de la mezcla de Voz y Phishing (Yeboah-Boateng & Amanor, 2014).

Vishing se centra en la confianza que puede tener la víctima en los servicios telefónicos, ya que generalmente las personas no son conscientes de la capacidad que puede tener el atacante para estafar, haciendo uso de técnicas de ingeniera social como la suplantación de identidad o utilizar sistemas automatizados de respuesta, para que se vuelva mucho más complicado diferenciar entre una llamada real de una falsa. Debido a que se han ido incrementando las técnicas para detectar ataques de Phishing, los atacantes han optado por técnicas más difíciles de identificar como el Vishing (Yeboah-Boateng & Amanor, 2014).

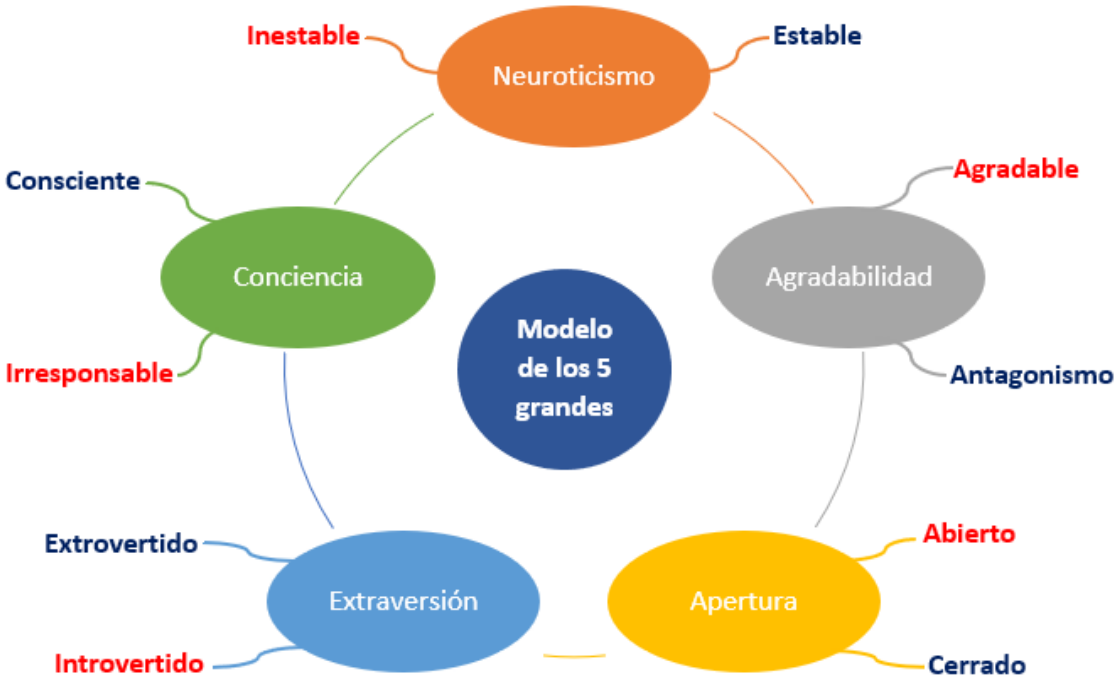
Hace varios años atrás era relativamente sencillo identificar quien era la persona que realizaba una llamada, debido a que con la tecnología de conmutación de circuitos, digitales y electrónicas, las llamadas se podían rastrear hasta la persona que debía pagar la factura por esa llamada, sin embargo, con los actuales sistemas de telefonía IP se puede realizar una llamada desde cualquier computador del mundo, inclusive en la mayoría de los casos estas direcciones IP son enmascaradas para que sean mucho más difícil de localizar (Yeboah-Boateng & Amanor, 2014). Se demostró que los delitos de Phishing de voz se pueden dividir en las etapas de preparación, reclutamiento de vendedores por teléfono, composición del guion, realización de llamadas telefónicas, conversaciones, depósito y retiro y transferencia de dinero (Maseno, 2017).

Modelo de cinco factores (FFM)

El modelo de los cinco factores de la personalidad (Five Factors Model), es una categorización jerárquica de los rasgos de personalidad, en términos de cinco grandes dimensiones básicas que son: Extraversión, Amabilidad, Conciencia, Neuroticismo y Apertura a la Experiencia. Los rasgos de personalidad de este modelo se entienden como patrones psicológicos, comportamientos, sentimientos y pensamientos que son respectivamente perdurables a lo largo de la vida de una persona (McCrae & Jhon, 2013). En la Figura 3 se presenta el modelo de los cinco factores de personalidad.

Figura 3

Modelo de los cinco grandes factores de personalidad.



Nota: Adaptada de A Survey on Human and Personality Vulnerability Assessment in Cybersecurity: Challenges, Approaches, and Open Issues (p. 9), de D. Papatsaroucha, 2021, Department of Electrical and Computer Engineering, Hellenic Mediterranean University.

Entre los varios modelos que existen para poder determinar la personalidad de una persona el más ampliamente aceptado y utilizado es el

Modelo de los cinco factores o FFM por sus siglas en inglés. Este modelo incluye rasgos de la personalidad que se mantienen inalterables a pesar de la edad, cultura, género y transcurso del tiempo (Lawrence & John, 1995). Este modelo comprende los rasgos que se aprecian en la Tabla 1.

Tabla 1

Rasgos de personalidad del modelo de cinco factores.

Rasgo de personalidad	Nivel Alto	Nivel Bajo
Apertura	Curioso, imaginativo	Superficial, conservador
Conciencia	Organizado, confiable, minucioso	Poco fiable, negligente, descuidado
Extraversión	Activo, asertivo, hablador	Pasivo, reservado, pasivo
Agradabilidad	Confiando, cálido bueno	Egoísta, hostil, desconfiado
Neuroticismo	Malhumorado, nervioso, manipulador	Constante, tranquilo

Según (Papatsaroucha et al., 2021) y (Lawrence & John, 1995), los principales rasgos de la personalidad se definen de la siguiente manera, y las características de cada una se describen a continuación a partir de los conceptos de la Real Academia Española (RAE, 2021).

Apertura

Se refiere a la tendencia de los individuos a tener una mentalidad abierta hacia nuevas ideas y experiencias, y a aceptar creencias diferentes. Las personas que obtienen una puntuación alta en el rasgo de apertura exhiben una alta apreciación del arte, una mayor imaginación y un afán de aventura. Por otro lado, las personas que obtienen una puntuación baja se sienten más cómodas en su rutina y no buscan nuevas experiencias.

Nivel Alto.

Valores en asuntos intelectuales, rebelde, inconformista y tiene un proceso de pensamiento inusual.

- **Curioso:** Inclinado a aprender lo que no conoce o Inclinado a enterarse de cosas ajenas.
- **Imaginativo/Fantasioso:** Que continuamente imagina o piensa.
- **Independiente:** Que no tiene dependencia, que no depende de otro.

Nivel Bajo

Favorece los valores conservadores, son jueces en términos convencionales y se siente incómodo con las complejidades.

- **Superficial:** Frívolo, sin fundamento o que está o se queda en la superficie.
- **Conservador:** Especialmente favorable a mantener el orden social y los valores tradicionales frente a las innovaciones y los cambios radicales.
- **Concreto:** Preciso, determinado, sin vaguedad.
- **Convencional:** Un acto, de una costumbre, de una indumentaria, etc. Que se atienen a las normas mayoritariamente observadas.

Conciencia

Incluye características como la honestidad, la confianza, la fuerte auto-orientación y la auto-responsabilidad. Las personas que obtienen una puntuación alta en este rasgo son más propensas a apegarse a los planes y seguir las reglas.

Nivel Alto

Se comporta éticamente, confiable, responsable, productivo y tiene un alto nivel de aspiración.

- **Ordenado:** Que guarda orden y método en sus acciones.
- **Confiable:** Persona en la que se puede confiar.
- **Meticuloso:** Persona muy escrupulosa y concienzuda en sus acciones.
- **Diligente:** Cuidadoso, exacto y activo.

Nivel Bajo

Incapaz de negar la gratificación, auto indulgente y se involucra en soñar despierto.

- **Poco confiable:** Persona en la que no se puede confiar.
- **Negligencia:** Falta de aplicación o descuido.
- **Descuidado:** Que falta al cuidado que debe poner en las cosas, que cuida poco de la compostura en el traje.
- **Impulsivo:** Que suele hablar o proceder sin reflexión ni cautela, dejándose llevar por la impresión del momento

Extraversión

Que se relaciona con las habilidades sociales. Las personas que tienen una puntuación alta en este rasgo se sienten cómodas en grandes grupos de personas y tienden a ser entusiastas, enérgicas y locuaces. Por el contrario, las personas que tienen una puntuación baja en este rasgo pueden ser descritas como introvertidas, por lo tanto, pueden sentirse más cómodos en grupos más pequeños de personas.

Nivel Alto

Locuaz, socialmente preparado y se comporta asertivamente

- **Dinámico:** Persona notable por su energía y actividad.
- **Asertivo:** Que expresa su opinión de manera firme.
- **Conversador:** Que sabe hacer amena e interesante la conversación.

Nivel Bajo

Emocionalmente suave y sumiso, evita las relaciones cercanas y tiene sobre control de los impulsos.

- **Pasividad:** Que deja obrar a los demás o permanece al margen de una acción.
- **Reservado:** Cauteloso, reacio a manifestar su interior. Comedido, discreto, circunspecto. Que se reserva o debe reservarse.

- **Tranquilo:** Que se toma las cosas con tiempo, sin nerviosismos ni agobios, y que no se preocupa por quedar bien o mal ante la opinión de los demás.
- **Retraído:** Que gusta de la soledad.

Agradabilidad

Describe a las personas que son más propensas a ayudar y confiar en los demás porque siempre asumen lo mejor de otras personas. Dependiendo de cuán alto o bajo sea el puntaje de un individuo en este rasgo, la amabilidad puede ser una medida de bondad y compasión.

Nivel Alto

Tiende a ser simpático, considerado, cálido, compasivo y se comporta de forma cedida.

- **Confiado:** Crédulo, imprevisor o presumido, satisfecho de sí mismo.
- **Amable:** Afable, complaciente, afectuoso.
- **Afectuoso:** Amoroso, cariñoso, expresivo, vivo.
- **Servicial**: Dispuesto a complacer y servir a otros.
- **Empático**: Propio o característico de una persona que tiene empatía.

Nivel Bajo

El comportamiento crítico y escéptico es condescendiente, intenta empujar los límites y expresa hostilidad directamente.

- **Egoísta:** Inmoderado y excesivo amor a sí mismo, que hace atender desmedidamente al propio interés, sin cuidarse del de los demás.
- **Hostil:** Contrario o enemigo.
- **Desconfiado:** No confiar, tener poca seguridad o esperanza.
- **Crítico**: Persona que habla con afectación o pedantería.
- **Sospechoso**: Que inspira sospecha

Neuroticismo

Se refiere al aumento de los niveles de ansiedad. Cuanta más alta es la puntuación de alguien en este rasgo, más uno tiende a preocuparse, mientras que las puntuaciones más bajas indican estabilidad emocional.

Nivel Alto

Irritable, ansioso de piel delgada, propenso a la culpa.

- **Malhumorado:** Que está de mal humor, desabrido o displicente.
- **Nervioso:** Inquieto e incapaz de permanecer en reposo, de nervios fácilmente excitables.
- **Temperamental:** De genio vivo, y que cambia con mucha frecuencia de humor o de estado de ánimo.
- **Ansioso**: Que tiene ansia o deseo vehemente de algo.
- **Infeliz**: De suerte adversa, no feliz.
- **Negativo**: Pesimista, inclinada a ver el aspecto desfavorable de las cosas.

Nivel Bajo

Tranquilo, relajado, satisfecho con uno mismo tiene personalidad clara y se enorgullece de su objetividad.

- **Estable/Constante**: Que no se deja dominar ni abatir.
- **Calmado:** Estar en calma o tender a ella
- **Plácido**: Quieto, sosegado y sin perturbación
- **Fiable**: Que es digna de confianza. Que ofrece seguridad o buenos resultados.

CAPÍTULO III

METODOLOGÍA

Modelo para definir la vulnerabilidad del usuario por rasgo de personalidad

Para la realización de nuestro estudio, se siguieron los siguientes pasos:

1. Una revisión sistemática de la literatura basada en soluciones actuales, orientadas a combatir los ataques de Ingeniería Social, según los rasgos de personalidad.

2. Determinación de cuáles son los más importantes rasgos de personalidad para ser vulnerables.

3. Realización de una encuesta a personas de una entidad universitaria, acerca de sus rasgos de personalidad.

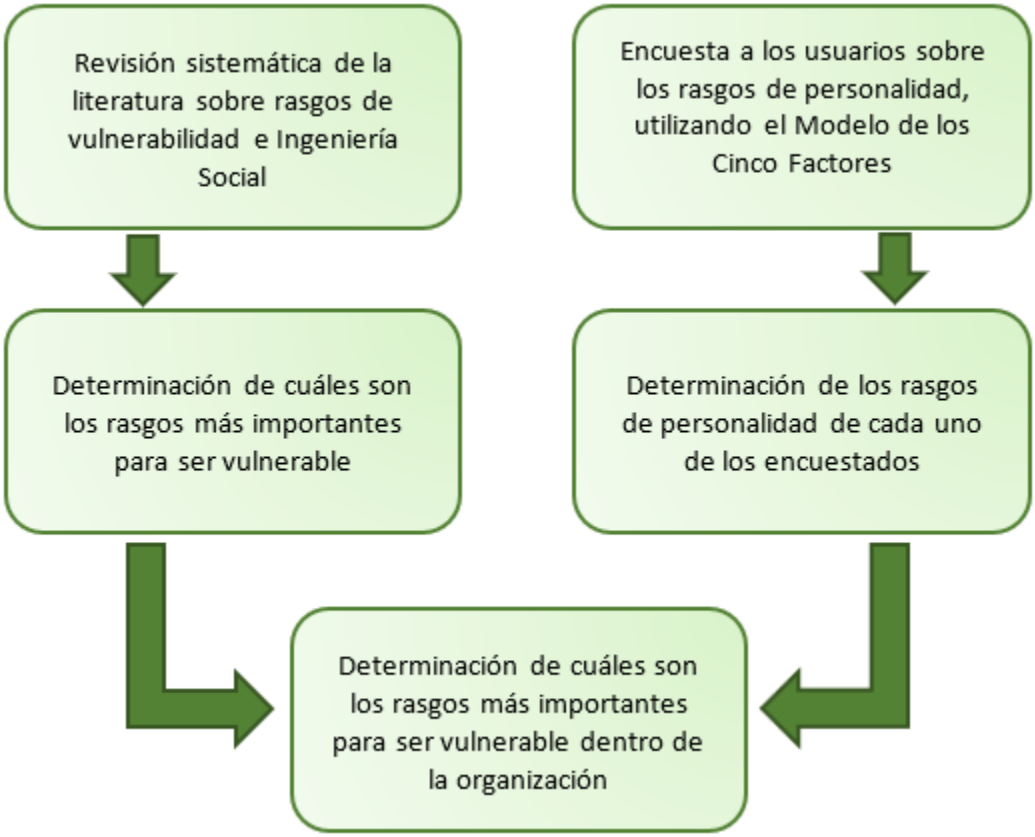
4. Determinación de los rasgos de personalidad de los encuestados.

5. Identificación de que personas o grupo de personas son más vulnerables a ser víctimas de los ataques de Ingeniería Social.

Esta metodología se puede apreciar en la Figura 4:

Figura 4

Modelo para definir la vulnerabilidad del usuario por rasgo de personalidad.

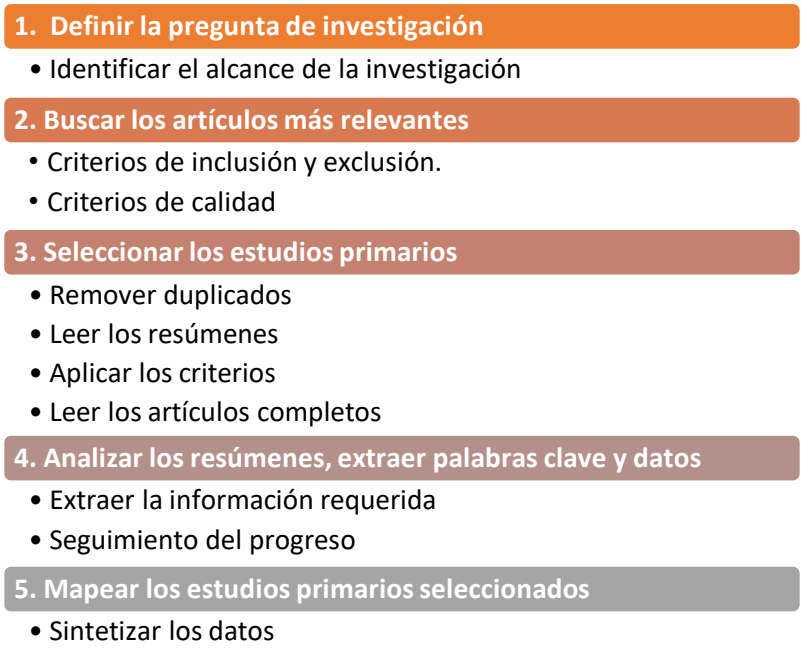


Revisión sistemática de la literatura (SLR) basada en soluciones actuales, orientadas a combatir los ataques de Ingeniería Social, según los rasgos de personalidad

Para realizar la recopilación de las características de las personas que son susceptibles a los ataques de Ingeniería Social, utilizamos la metodología SLR (Systematic Literature Review) propuesta por (Kitchenham et al., 2009), en base a la cual se realizaron los cinco pasos consecutivos que se presentan en la Figura 5.

Figura 5

Pasos de la metodología SLR (Revisión Sistemática de Literatura).



Nota: Adaptada de Systematic literature reviews in software engineering - A systematic literature review (p. 7 - 15), de B. Kitchenham, 2009, Information and Software Technology, 51(1).

Definir la pregunta de investigación

La pregunta de investigación que se planteó se basa en encontrar todas aquellas características o rasgos de personalidad más comunes entre las personas que son víctimas de ataques basados en la Ingeniería Social. Esos rasgos en algunos casos son estudiados y analizados por distintos autores, y en otras son utilizados como referencia para hacer énfasis a las vulnerabilidades humanas, las cuales implican algún riesgo o amenaza para la seguridad de la información.

Por lo tanto, la pregunta de investigación que se definió fue la siguiente:

¿Cuáles son rasgos de personalidad de los usuarios que los hacen más vulnerables a los ataques de Ingeniería Social?

Buscar los artículos más relevantes

Para realizar la búsqueda de artículos que tuvieran más relevancia con respecto a la pregunta de investigación planteada, se define una cadena de palabras que se compone de dos partes “rasgos de personalidad” e “Ingeniería Social”. Después esta cadena de palabras se la utilizó para hacer la búsqueda de la siguiente manera:

Rasgos de personalidad e (“Ingeniería Social” o “Phishing” o “Engaño y fraude” o” Ciberataques” o “Vishing” o “Pretexting”)

Por supuesto, la cadena de búsqueda solo fue ingresada en inglés.

Criterios de Inclusión y Exclusión

Los criterios de inclusión y exclusión se basan en la pregunta de investigación. En este caso, solo se realizó la inclusión de aquellos documentos que cumplen con los siguientes parámetros:

- El tema principal serían Ingeniería Social y los rasgos de personalidad o características personales; y excluir los artículos sólo sobre rasgos de personalidad o solo sobre Ingeniería Social pero no sobre ambos;
- Textos escritos en inglés;
- Describir la influencia de los rasgos de personalidad con la vulnerabilidad a ataques de Ingeniería Social;
- Artículos que tuvieran como máximo 5 años de publicación.

Criterio de Calidad

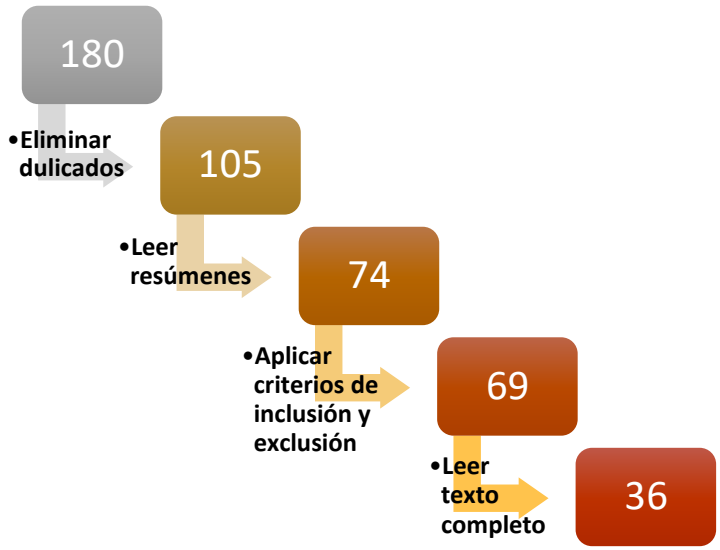
Para cumplir con los criterios de calidad en la búsqueda, se decidió realizar la selección únicamente artículos de journals o revistas, reconocidas a nivel científico en el área de tecnologías de la información. Las bases de datos indexadas que se eligieron fueron las siguientes: Web of Science, Scopus, IEEExplore, Springer, ACM Library y Sciencedirect. De igual manera se hizo la búsqueda de artículos científicos que estuvieran relacionados con el tema como en Google Scholar, Taylor y Francis, pero finalmente esos artículos ya se habían encontrado en las otras bases de datos científicas.

Selección de estudios primarios

Al momento de utilizar la cadena de búsqueda en las bases de datos científicas, en principio se encontraron 180 artículos, después de filtrar los artículos duplicados, realizar la lectura de los resúmenes, leer completamente el contenido de los documentos y aplicar los criterios de inclusión y exclusión se recopilaron en total 36 artículos como estudios primarios. En la en la Figura 6 se describe el proceso de selección.

Figura 6

Selección y filtración de estudios primarios para su lectura completa.



Analizar los resúmenes, extraer palabras clave y datos

Para hacer el análisis de los resúmenes y palabras clave se utilizó la herramienta web Rayyan QCRI (Ayan et al., n.d.) (Robert Ayan et al., n.d.)(Robert Ayan et al., n.d.)la cual pertenece a un proveedor líder de herramientas de colaboración e investigación que impulsan a la comunidad de investigación global en busca de un descubrimiento científico acelerado. Rayyan permite trabajar de forma remota y colaborar con un equipo distribuido, emplea el procesamiento del lenguaje natural, la inteligencia artificial y las tecnologías de aprendizaje automático para acelerar las revisiones sistemáticas (Ayan et al., n.d.).

Esta herramienta da la posibilidad de subir data sets de artículos científicos obtenidos desde las bases de datos indexadas para luego aplicar filtros de selección basados en los criterios de inclusión y exclusión, como se puede ver en la Figura 7, donde se muestra la interfaz de la herramienta que contiene todos los artículos con sus respectivas etiquetas y palabras clave para una mejor clasificación.

Figura 7

Análisis de resumes de los artículos con la herramienta Rayyan QCRI.

Categorización de los rasgos más importantes según el Five Factor Model (FFM)

Una vez realizada la selección de todos los artículos que mejor se adaptan a la investigación, se realizó la lectura completa de ellos, además del análisis y recolección de todos los rasgos que los autores de dichos artículos consideran más importantes, para que una persona pueda ser una posible víctima o no de ataques de Ingeniería Social.

Los rasgos importantes que fueron mencionados en cada artículo se recopilaron y se organizaron mediante una Hoja de Cálculo en Google Sheets, por medio de lo cual se pudo conseguir un panorama mucho más amplio de todas las variaciones o términos distintos, que cada autor utiliza para referirse a las características, que son similares a las que abarca el Modelo de los Cinco

Factores (FFM). Esto se puede ver mejor reflejado en la Figura 8, en donde se aprecian todos los principales rasgos psicológicos de las personas.

Figura 8

Características agrupadas por cada artículo.

Art. 1 (Khidzir et al., 2019)	Art. 2 (Feng et al., 2019)	Art. 3 (Aldawood & Skinner, 2019)	Art. 4 (Corradini & Nardelli, 2019)	Art. 5 (Shaabany & Anderl, 2019)
Mantienen buenas practicas de seguridad	Nivel de actividad (comportamiento activo en redes sociales, Si un usuario publica, reenvía, comenta o le gusta una publicación)	Culpa moral obligatoria	Actitud (positivo, proactivo, responsable, colaborador)	Falta de conocimiento o ignorancia
Regirse a las normas o protocolos establecidos reduce el riesgo de ser victima	Comportamientos interactivos (Si el usuario interactúa con otros usuarios)	Emociones intimidantes (ansiedad, ira, vulnerabilidad o depresión)	Relación (comunicación, cooperación, compartir. Tener buenas relaciones tiene un papel importante para la prevención y gestión de riesgos cibernéticos.)	La curiosidad
	Relaciones sociales de confianza	Naturaleza de confianza	Comportamiento (equidad, responsabilidad)	El miedo a meterse en problemas
	Circulos sociales	Falta de interés	Percepción del riesgo	La disposición a ayudar
	Preferencias obvias del usuario	Falta de conciencia	Confianza (reciprocidad , confiabilidad)	La tendencia a confiar en los demás

El procedimiento descrito en el párrafo anterior, se llevó a cabo con los 36 Papers que se obtuvieron luego del proceso de SLR. Así, para una mejor clasificación y muestreo de todas las distintas características otorgadas por los autores se utilizó el Modelo de los Cinco Factores (FFM) según (Lawrence & John, 1995), donde cada uno de estos factores abarcan todos los rasgos de la personalidad que se puedan definir de un individuo.

De esta manera, basándose en los términos anteriormente expuestos dentro del Marco Teórico, se agruparon todas las características de acuerdo al Factor con el que tengan más relación tengan según el FFM de (Lawrence & John, 1995) y (Papatsaroucha et al., 2021).

Por motivos prácticos, luego se asignó una abreviatura de personalidad y se estableció un color para cada factor, con la finalidad de distinguir si el factor es alto o bajo. Ver Tabla 2.

Tabla 2

Nomenclatura asignada a cada factor alto y bajo.

Apertura (Alto)	**Ap_A**
Apertura (Bajo)	Ap_B
Conciencia (Alto)	Co_A
Conciencia (Bajo)	Co_B
Extraversión (Alto)	Ex_A
Extraversión (Bajo)	Ex_B
Agradabilidad (Alto)	Ag_A
Agradabilidad (Bajo)	Ag_B
Neuroticismo (Alto)	Ne_A
Neuroticismo (Bajo	Ne_B

A continuación, se realizó una exaltación de los rasgos en cada uno de los artículos seleccionados, acorde al color que se asignó según la Tabla 2. Se puede observar el resultado en la Tabla 3. Esto se hizo para poder reconocer de manera más sencilla y rápida, cuáles son los Factores de FFM, que se encontraron en cada artículo.

Tabla 3

Clasificación de las características para cada factor de personalidad.

FFM	Art. 1 (Khidzir et al., 2019)	Art. 2 (Feng et al., 2019)	Art. 3 (Aldawood & Skinner, 2019)	Art. 4 (Corradini & Nardelli, 2019)
Ap_A	Mantienen buenas prácticas de seguridad	Nivel de actividad (comportamiento activo en redes sociales, Si un usuario publica, reenvía, comenta o le gusta una publicación)	Culpa moral obligatoria	Actitud (positivo, proactivo, responsable, colaborador)
Ap_B	Regirse a las normas o protocolos establecidos reduce el riesgo de ser víctima	Comportamientos interactivos (Si el usuario interactúa con otros usuarios)	Emociones intimidantes (ansiedad, ira, vulnerabilidad o depresión)	Relación (comunicación, cooperación, compartir. Tener buenas relaciones.)
Co_A		Relaciones sociales de confianza	Naturaleza de confianza	Comportamiento (equidad, responsabilidad)
Co_B		Círculos sociales	Falta de interés	Percepción del riesgo
Ex_A		Preferencias obvias del usuario	Falta de conciencia	Confianza (reciprocidad, confiabilidad)
Ex_B				
Ag_A				
Ag_B				
Ne_A				
Ne_B				

Una vez que se clasificaron todos los rasgos recolectados, se procedió a realizar el conteo de las veces que cada uno de los Factores fue mencionado según cada artículo. Esto porque existen varias maneras de denominar un mismo término. Como se puede ver en la Tabla 4 se hizo la suma de las características agrupadas en los rasgos de personalidad del FFM.

Tabla 4

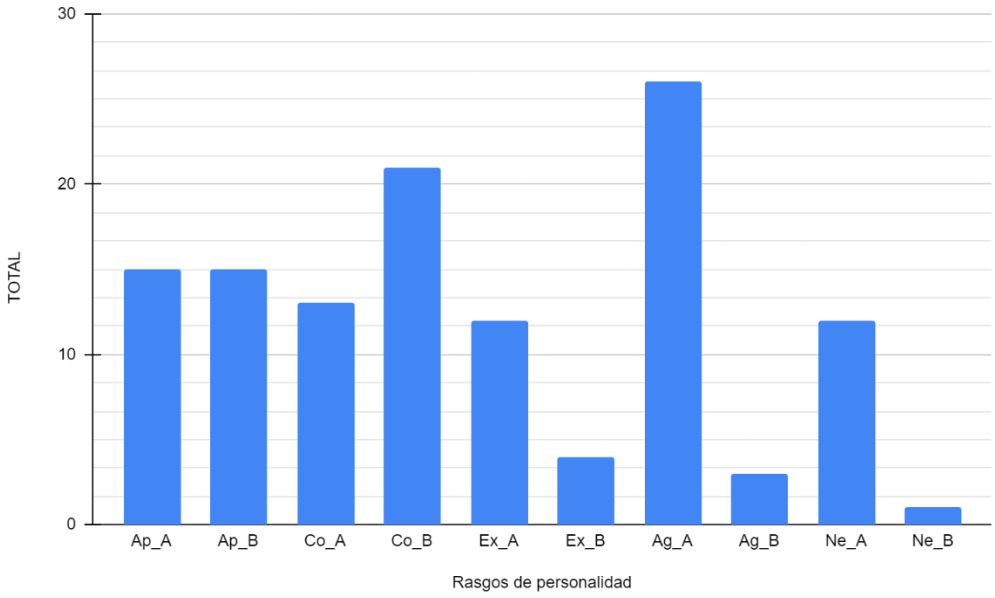
Suma total de todas las menciones de los FFM en los artículos leídos.

Five-Factor Model	Abreviatura	TOTAL
Apertura (Alto)	Ap_A	15
Apertura (Bajo)	**Ap_B**	15
Conciencia (Alto)	**Co_A**	13
Conciencia (Bajo)	**Co_B**	21
Extraversión (Alto)	**Ex_A**	12
Extraversión (Bajo)	**Ex_B**	4
Agradabilidad (Alto)	**Ag_A**	26
Agradabilidad (Bajo)	**Ag_B**	3
Neuroticismo (Alto)	**Ne_A**	12
Neuroticismo (Bajo	**Ne_B**	1

En la Figura 9 se puede observar cuales son las características más importantes a la hora de evaluar si una persona es una potencial víctima o no de un ataque de Ingeniería Social.

Figura 9

Características agrupadas de acuerdo con el Five Factor Modelo.



En la Figura 9 se puede observar que los factores con puntuaciones más altas son: Agradabilidad alta (Ag_A) con una puntuación de 26, Conciencia baja (Co_B) con una puntuación de 21, Apertura baja (Ap_B) y Apertura alta (Ap_A) con una puntuación de 15, Conciencia alta (Co_A) con una puntuación de 13, Extroversión alto (Ex_A) y Neuroticismo alto con una puntuación (Ne_A) de 12, Mientras que los factores con menor puntuación son: Extroversión bajo (Ex_B) con una puntuación de 4, Agradabilidad baja (Ag_B) con una puntuación de 3 y por último Neuroticismo bajo (Ne_B) con una puntuación de 1.

Según (Papatsaroucha et al., 2021) y (Lawrence & John, 1995), existen rasgos en los FFM en que no por ser Altos o Bajos significan que sean de alto o bajo riesgo de vulnerabilidad en ante un ataque de Ingeniería Social. Esto, porque en realidad depende de exclusivamente en que rasgo de personalidad se aplica este rango Alto o Bajo

Por este motivo se ha asignado colores a manera de semáforo para el rango de cada Factor, basándonos en los resultados obtenidos del análisis de los distintos papers recolectados en la revisión de la literatura.

Tabla 5

Estandarización de las categorías de los FFM por semáforo

FFM	Bajo	Medio	Alto
Extraversión	Las personas con puntuación baja pueden ser descritas como introvertidas, por ende, es más difícil sacarles información	Las personas con puntuación media pueden ser algo reservadas, pero si se capta su atención tienen a generar conversación	Las personas que tienen una puntuación alta se sienten cómodas en grandes grupos de personas y tienden a ser entusiastas, enérgicas y muy conversadoras
Agradabilidad	Este tipo de personas suele ser crítico, no es condescendiente y expresa hostilidad ante los demás.	Suelen ser personas a las que no tratan de agradar a nadie, pero de ser necesario estarían dispuestos a ayudar a los demás, estando siempre alerta.	Estas personas que son más propensas a ayudar y confiar en los demás porque siempre asumen lo mejor de otras personas
Conciencia	En este rasgo están quienes son más propensos a no apegarse a los planes y seguir sus propias reglas, sin medir consecuencias.	Personas que tienen sus valores establecidos y en quienes se puede confiar, pero no están exentos a tener pequeños fallos por descuido.	La honestidad, la confianza, la fuerte auto-orientación y la auto-responsabilidad son las principales características de estas personas.
Neuroticismo	Estas personas suelen ser más estables emocionalmente y meditan mejor todas sus acciones.	Suelen mantener la calma, pero mientras más se los fuerce suelen llegan a su punto de quiebre con mayor facilidad.	Cuanta más alta es la puntuación de alguien en este rasgo, más tiende a preocuparse y tomar decisiones apresuradas.
Apertura	Son conservadores, jueces en términos convencionales y se siente incómodo con las complejidades, podría ser malo al no estar al tanto de los nuevos métodos de ataque.	Personas que están dispuestas a aceptar nuevas experiencias, sin perder los valores conservadores.	Son individuos a tener una mentalidad abierta hacia nuevas ideas y experiencias, y a aceptar creencias diferentes

Como podemos apreciar en la Tabla 6 se le ha asignado un valor porcentual a cada uno de los factores según el número de veces que fueron mencionados, únicamente tomando en cuenta los Factores que influyen de manera negativa en el grado de vulnerabilidad de las personas.

Tabla 6

Pesos que poseen los FFM para determinar el grado de vulnerabilidad ante un ataque de Ing. Social.

FFM	Nro de veces mencionado en los papers analizados	Peso porcentual dentro de los papers analizados
Apertura	30	28,8%
Conciencia	21	20,2%
Extraversión	12	11,5%
Agradabilidad	29	27,9%
Neuroticismo	12	11,5%

Al poseer la medida de Bajo, Medio y Alto para denotar el rango de cada uno de los Factores se han dividido los pesos porcentuales entre tres; de este modo se consigue el valor de estas medidas a manera de porcentaje y respetando el peso que tiene cada factor a la hora de determinar el nivel de vulnerabilidad ante un ataque de Ingeniería Social. Ver Tabla 7.

Tabla 7

Distribución de pesos porcentuales entre los tres rangos establecidos.

FFM	Bajo	Medio	Alto
Apertura	19,20	9,60	28,80
Conciencia	20,20	13,46	6,73
Extraversión	3,83	7,66	11,50
Agradabilidad	18,60	9,30	27,90
Neuroticismo	3,83	7,66	11,50

Recolección de datos

Para la recolección de datos de datos se utilizó una metodología de investigación descriptiva, según (Anguita et al., 2003) el tipo de investigación descriptiva permite determinar las cualidades, características o propiedades de los distintos perfiles que podrían presentar las personas o cualquier otro elemento que se pueda someter a algún tipo de análisis, recolección o evaluación de datos. Este tipo de investigación permite establecer algún tipo de relación o predicción entre variables, a pesar de ser poco elaborado.

Esta investigación cuenta tanto con un enfoque cualitativo, como cuantitativo. Para el análisis de características de la personalidad de las personas se utiliza un enfoque cualitativo, ya que gracias a esto se puede analizar los distintos factores que influyen en los rasgos de cada persona, y el enfoque cuantitativo se lo realiza a la hora de tabular y procesar los datos que se han obtenido de las encuestas realizadas, esto con el fin de conseguir información que permita determinar si una persona puede llegar o no a ser una víctima de un ataque de Ingeniería Social.

Instrumento de evaluación

La encuesta que se desarrolló está basada en el Big Five Inventory o BFI según (John et al., 1991). Este es un método de evaluación que consta de 44 items, en el cual se evalúa la Extraversión (8 items), Conciencia (9 items), Agradabilidad (9 items), Neuroticismo (8 ítems) y Apertura (10 items). Para mayor efectividad se utilizó la versión española de (Benet-Martinez & John, 1998), la cual está basada y traducida del BFI-44 de (John et al., 1991). Se tiene evidencia según en los trabajos de (Benet-Martinez & John, 1998) que dicha versión tiene una estructura más favorable para trabajar con personas de habla hispana y mantienen indicadores de confiabilidad en promedio de 0,78 de 1.

Encuesta de personalidad

Con la finalidad de implementar nuestro modelo, se realizó una encuesta para definir los rasgos de personalidad de los participantes. La idea es confrontar los resultados de la encuesta, con los rasgos obtenidos como más importantes para determinar las vulnerabilidades de las personas.

En la encuesta se obtuvo la participación de 146 personas de la Universidad de las Fuerzas Armadas ESPE Santo Domingo, entre docentes, estudiantes y administrativos, de los 800 integrantes de la comunidad universitaria. Se recolectaron los datos con la finalidad de medir en cada uno de los individuos, a que rasgos de personalidad corresponden, según el Modelo de los Cinco Grandes Factores. Cabe aclarar que la información recolectada fue de carácter estrictamente confidencial.

La encuesta estuvo compuesta por 44 enunciados que definen la personalidad de un individuo, en la cual el encuestado debía seleccionar una valoración para indicar cuanto estaba de acuerdo o no, según su propia apreciación y según la forma en que el encuestado se comporta con las demás personas. A continuación, se presentan las preguntas realizadas para la encuesta de definición de personalidad:

1. Le gusta hablar mucho
2. Tiende a encontrar defectos en los demás
3. Hace un trabajo minucioso
4. Está deprimido o triste
5. Es original, se le ocurren nuevas ideas
6. Es reservado
7. Es servicial y desinteresado con los demás
8. Puede ser algo descuidado
9. Es relajado o maneja bien el estrés
10. Tiene curiosidad por muchas cosas diferentes
11. Está lleno de energía
12. Se pelea o discute con los demás
13. Es un trabajador fiable
14. Suele estar tenso
15. Es ingenioso, un pensador profundo
16. Tiene mucho entusiasmo
17. Tiene una naturaleza misericordiosa con los demás
18. Tiende a ser desorganizado
19. Se preocupa mucho
20. Tiene una imaginación activa
21. Tiende a ser tranquilo
22. Es generalmente confiado
23. Tiende a ser perezoso
24. Es emocionalmente estable, no se altera fácilmente
25. Es creativo, inventa cosas nuevas
26. Es asertivo, seguro de sí mismo
27. Puede ser frío y distante
28. Persevera hasta terminar una tarea
29. Puede ser malhumorado
30. Valora las experiencias artísticas y estéticas
31. A veces es tímido, inhibido
32. Es considerado y amable con casi todo el mundo
33. Hace las cosas de manera eficiente
34. Mantiene la calma en situaciones de tensión
35. Prefiere el trabajo rutinario
36. Es extrovertido o sociable
37. A veces es grosero con los demás
38. Hace planes y los cumple
39. Se pone nervioso con facilidad
40. Le gusta reflexionar, jugar con las ideas
41. Tiene pocos intereses artísticos
42. Le gusta cooperar con los demás
43. Se distrae fácilmente
44. Es sofisticado en arte, música o literatura

Clasificación de los resultados

Una vez que se consiguieron los resultados de la encuesta, se procesaron los puntajes conseguidos en cada una de las preguntas, esto para determinar los rangos en los que se encuentra cada persona dentro del Modelo de los Cinco Factores según(Lawrence & John, 1995).

Para la clasificación, se utilizó el estándar de respuestas simple según (Dominguez Lara et al., 2018), en donde cada ítem del cuestionario se evaluó en

un intervalo que va desde 1 (En Total Desacuerdo), hasta 5 (Totalmente de Acuerdo), y posteriormente se realizó la suma de todos los puntajes obtenidos, según las preguntas que pertenezcan a cada uno de los factores a evaluar.

Puntuación de la escala del BFI (Inventario de los Cinco Grandes), en la cual "R" denota elementos con puntuación inversa:

- **Extraversión**: 1, 6R, 11, 16, 21R, 26, 31R, 36;
- **Agradabilidad:** 2R, 7, 12R, 17, 22, 27R, 32, 37R, 42;
- **Conciencia:** 3,8R, 13, 18R, 23R, 28, 33, 38, 43R;
- **Neuroticismo:** 4, 9R, 14, 19, 24R, 29, 34R, 39;
- **Apertura:** 5, 10, 15, 20, 25, 30, 35R, 40, 41R, 44;

Las preguntas que cuentan con una denotación de puntuación inversa se realizaron para evitar un sesgo de información, es decir, que las personas no se retraigan y proporcionen información falsa o errónea. Esto sucede cuando las preguntas son un poco impactantes en las personas, es por ello que se opta por preguntarlo de manera inversa o contraria.

Resultados de la encuesta para determinar los rasgos de personalidad de los usuarios

Paralelamente a la definición de los rasgos de personalidad más importantes, se realizó una encuesta al personal de la universidad, con la finalidad de determinar los rasgos de personalidad de los encuestados. La muestra que se tomó es de 146 personas, de los 800 integrantes de la comunidad universitaria.

De esta manera, se determinó un puntaje para cada encuestado en cada uno de los factores FFM, como se muestra en la Tabla 8 (Como ejemplo se muestran los nueve primeros resultados obtenidos de los 146):

Tabla 8

Resultado numérico de la encuesta realizada enmarcada en FFM

Encuestados	Extraversión	Agradabilidad	Conciencia	Neuroticismo	Apertura
1	17	18	23	31	34
2	21	33	35	22	47
3	22	37	33	23	47
4	26	31	31	25	33
5	24	30	36	22	32
6	32	39	28	29	31
7	36	37	37	11	45
8	18	26	23	21	30
9	23	31	28	19	25

Figura 10

Recuento de puntajes correspondientes a Extraversión, obtenido de los encuestados.

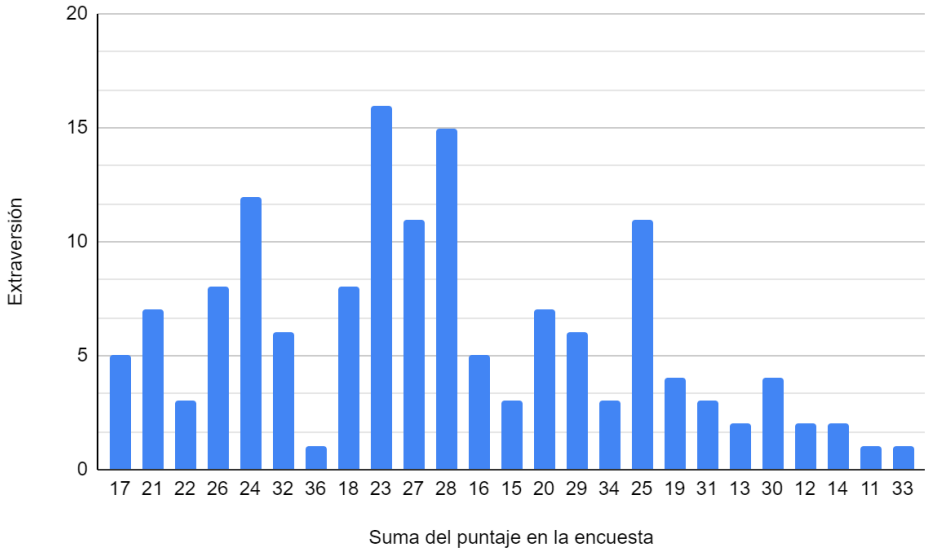


Figura 11

Recuento de puntajes correspondientes a Agradabilidad, obtenido de los encuestados.

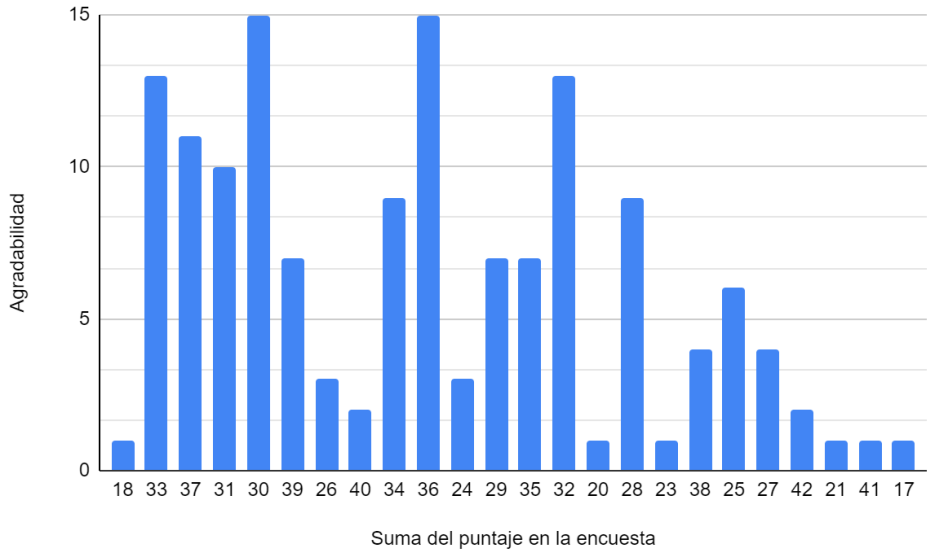


Figura 12

Recuento de puntajes correspondientes a Conciencia, obtenido de los encuestados.

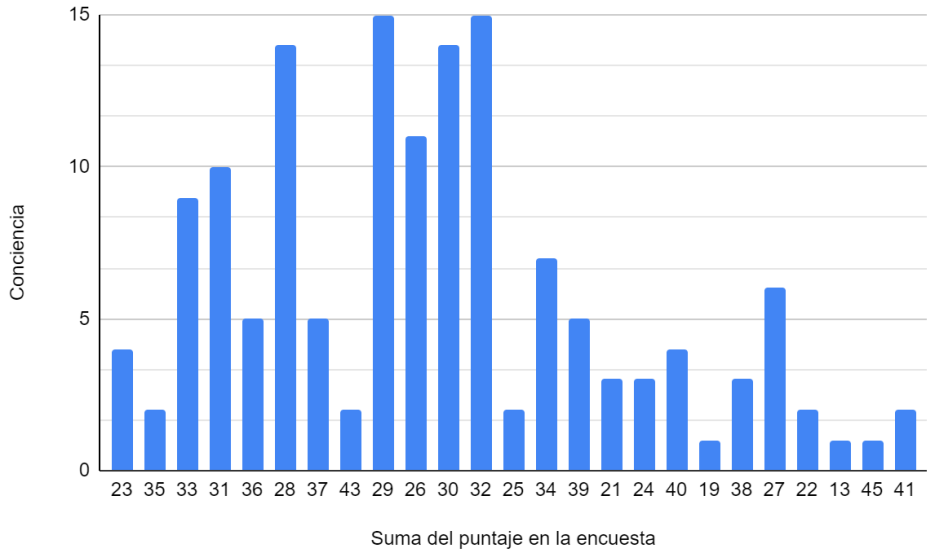
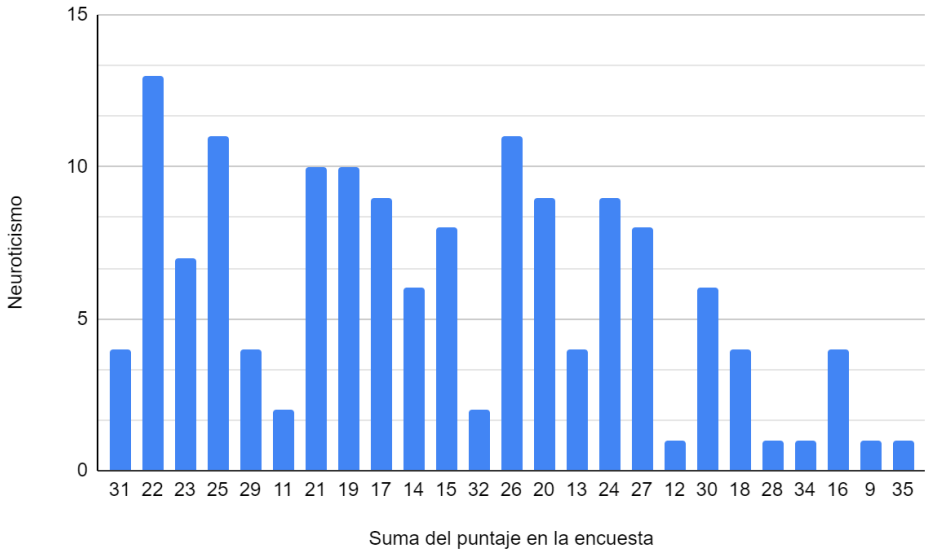


Figura 13

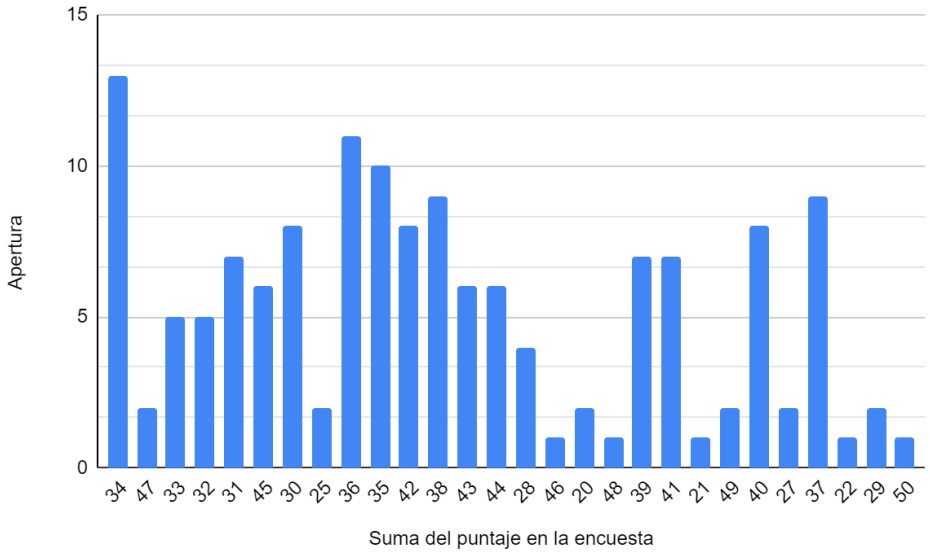
Recuento de puntajes correspondientes a Neuroticismo, obtenido de los encuestados.



.

Figura 14

Recuento de puntajes correspondientes a Apertura, obtenido de los encuestados.



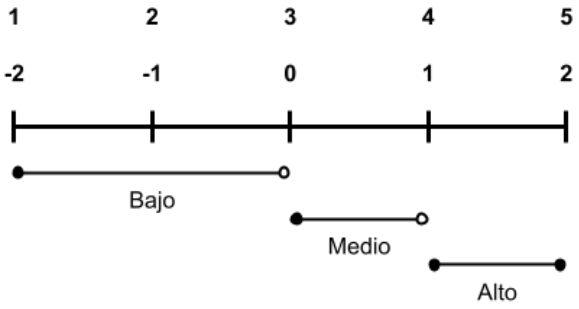
Como se puede apreciar desde la Figura 10 hasta la 14, estos resultados solo exponen las sumatorias correspondientes a cada uno de los FFM de la encuesta. En el eje vertical se encuentra el número de personas que obtuvieron la misma sumatoria, la cual se encuentra marcada en el eje horizontal. Sin embargo, estos datos aun no proporcionan ningún tipo de información considerable, es por ello que se aplica lo planteado por (Dominguez Lara et al., 2018), donde menciona que para obtener los resultados de manera más simple sólo se deberá asignar un rango a cada uno de los FFM, según la sumatoria de los puntajes alcanzado en los ítems correspondientes a cada factor.

Categorización de las respuestas a Bajo, Medio Alto

Para categorizar entre Bajo, Medio y Alto, se ha optado por asignar distintos rangos a los tipos de respuestas que se podían dar, las cuales iban desde En total desacuerdo hasta Totalmente de acuerdo. Debido a esto se ha optado por desplazar dichas respuestas disponibles a una recta numérica, tal como se observa en la Figura 15.

Figura 15

Categorización de valores de las respuestas.



La razón por la que se decidió trabajar de esta manera es que al plasmar los valores de las respuestas en una recta numérica se vuelve mucho más sencillo de comprender. Al ser 3 el valor intermedio que representa a la respuesta “Ni de acuerdo ni en desacuerdo.” se lo puede colocar como el valor de 0 sobre la recta numérica, siendo este el punto de división para los distintos rangos que se desea asignar. El valor de $[-1, 3)$ al ser menores que 3 el cual representa al 0, se los podría considerar como respuestas negativas, en otras palabras, conformarían el rango de bajo. De $(3, 4)$ se les asignaría el rango de

medio, debido a que no alcanzarían el valor de 1 dentro de la recta numérica y finalmente $(4, 5]$ representaría el rango de Alto.

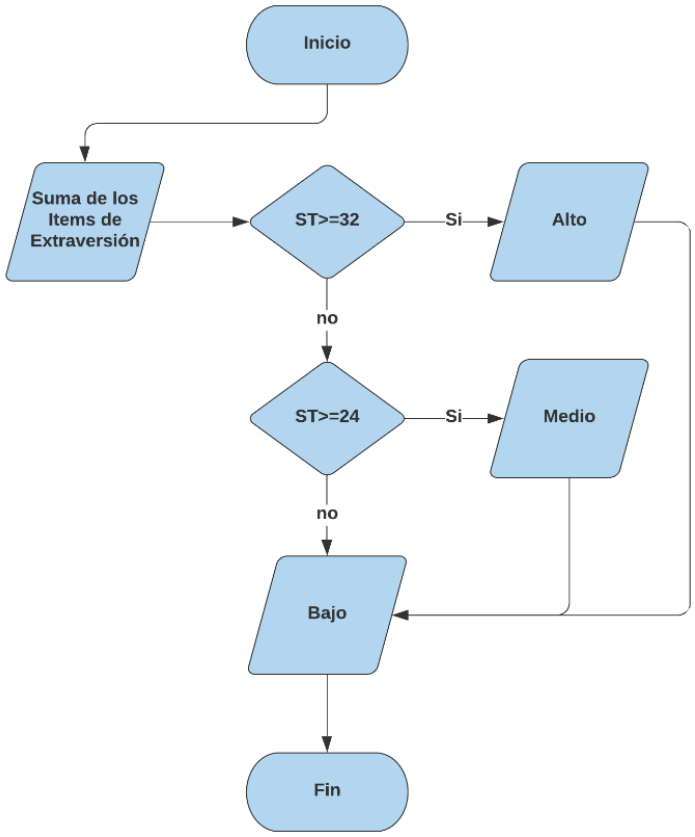
Para ello calcularemos el valor de la sumatoria en los hipotéticos casos en el que todas las respuestas hayan sido 3, esto permitirá tomar este valor como límite para definir los rangos, por ejemplo, para Extraversión:

$ST >= (NItem * 3)$, para ST tomaremos un valor aleatorio de los que se obtuvieron de las respuestas de cada sección del test, y el valor de $NItem$ en el caso de Extraversión es de 8. Tendremos que $17 >= (8 * 3)$ es falso, es decir que su rango estaría en Alto o Bajo. Para determinar en cuál de estos rangos estaría, usaremos el caso en el que todas las respuestas fueron 4, $ST >= (NItem * 4)$, $17 >= (8 * 4)$ su respuesta es falsa, entonces al no estar entre Medio y Alto, estaría en Bajo.

Todo el proceso descrito en el párrafo anterior se ve reflejado en el diagrama de flujo de la Figura 16, que se tomó como ejemplo explicando únicamente al Factor Extraversión. Así, se usaron los tres casos que permitirían tomar un valor base para cada rango. En este caso particular, se ha usado la Extraversión, cuyos límites eran: más de 32, Alto; más de 24, Medio; y menor que 24, Bajo. Este proceso se aplicó con todos los otros Factores.

Figura 16

Diagrama de flujo para determinar los rangos de los FFM acorde a su puntaje.



CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

Ya con los porcentajes conseguidos y el modelo de clasificación, se procede a realizar un match de estos dos resultados para determinar que encuestados son más vulnerables a ataques de Ingeniería Social. Esto se puede observar usando una descripción de semáforo en la Tabla 9.

Tabla 9

Semaforización de los resultados obtenidos de la encuesta

Encuestados	Extraversión	Agradabilidad	Conciencia	Neuroticismo	Apertura
1	Low	Low	Low	Medium	Medium
2	Low	Medium	Medium	Low	High
3	Low	High	Medium	Low	High
4	Medium	Medium	Medium	Medium	Medium
5	Medium	Medium	High	Low	Medium
6	High	High	Medium	Medium	Medium
7	High	High	High	Low	High
8	Low	Low	Low	Low	Medium
9	Low	Medium	Medium	Low	Low

Se muestran únicamente los nueve primeros resultados que se obtuvieron de los 146 encuestados, a partir de aquí se puede determinar las falencias que tiene cada uno de los encuestados de manera individual. Esto abre paso a una posible intervención por parte del personal a cargo y tratar de trabajar con las personas que tengan más falencias en cuanto a sus rasgos de personalidad.

Se pueden interpretar los resultados de la siguiente manera: los encuestados 1 y 8 tienen un solo rasgo de personalidad que los hacen vulnerables (está marcado en rojo), y este es Conciencia baja; los encuestados 2 y 9 también tienen un rasgo que los hacen vulnerables pero en este caso es el 2 tiene Apertura alta y el nueve Apertura baja; en los encuestados 4 y 5, no tienen rasgos peligrosos, pero sus niveles en la mayoría de rasgos llegan hasta un nivel medio; los encuestados 3 y 6 tienen dos rasgos que los hacen aún más vulnerables coincidiendo con una Agradabilidad alta, mientras que el 3 tiene una Apertura alta, el 6 tiene una Extraversión Alta y por último el encuestado 7 tiene alta vulnerabilidad, puesto que tiene tres rasgos negativos, que son Extraversión, Agradabilidad y Apertura en nivel alto.

Cabe mencionar que para este modelo, se define una puntuación por cada factor de personalidad, por lo que en función de la puntuación obtenida, se divide para cada rasgo en niveles bajo, medio y alto descritos en el apartado anterior y como variable objetivo introducida en el modelo.(Souri et al., 2018) en su estudio señalan que cada resultado para cada rasgo no puede tener una influencia o relación en otros resultados también. Por ejemplo, una persona con baja extraversión no puede decidir que está en un grupo bajo o alto de conciencia y agradabilidad. Los demás rasgos también son así, por lo que cada rasgo actúa de forma independiente.

Categorización completa de los resultados

Tabla 10

Resultados de la encuesta filtrados por su rango.

FFM	Bajo	Medio	Alto
Extraversión	65	70	11
Agradabilidad	17	87	42
Conciencia	16	103	27
Neuroticismo	88	54	4
Apertura	14	84	48

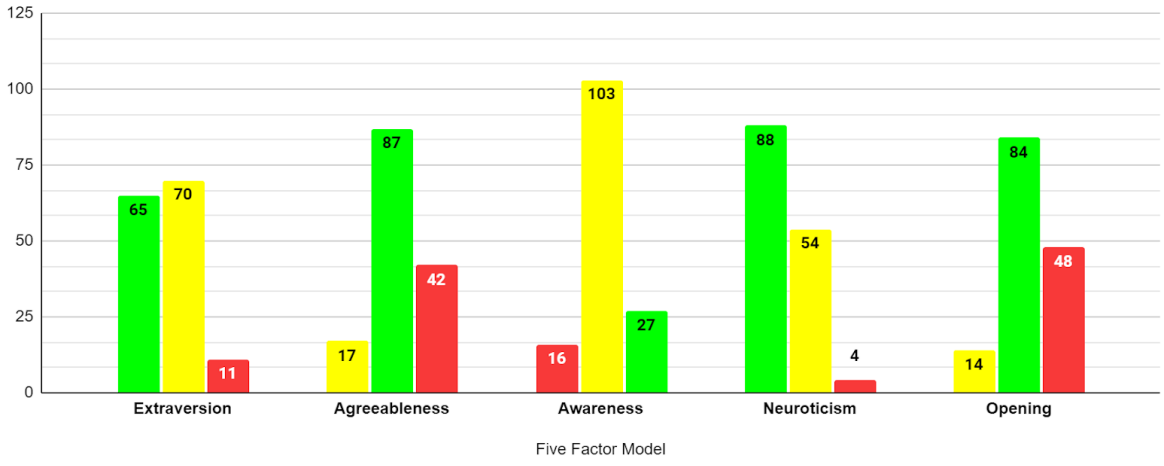
En la Figura 17 se aprecia que los rasgos con mayor regularidad son de Bajo y Medio. Estos datos ya pueden arrojar un significado, simplemente

analizando hacia dónde se inclinan la mayoría de las personas que realizaron la encuesta y cual son las características que presentan cada uno de estos factores según el FFM de (John et al., 1991).

Según (Wehrli, 2008) la extraversión es el rasgo responsable de aproximadamente el 10% de la varianza en el número de amigos, las personas con altos puntajes en extraversión toman posiciones más centrales en su círculo de amistad, es muy probable que las personas que tienen muchos amigos sean más vulnerables. En este caso la extraversión se muestra como un rasgo positivo en los 146 encuestados de la organización, porque en base a los resultados obtenidos tiene un puntaje de 65 en el nivel bajo, 70 en el nivel medio y apenas 11 en el nivel bajo, por lo tanto, se puede decir que la mayoría de los encuestados son menos susceptibles a los ataques de Ingeniería Social por su rasgo de extraversión.

Figura 17

Resultados generales de la encuesta luego de la categorización por rangos.



En base a la Figura 17, se observa que para la institución en la que se realizó el estudio, el factor en que más afecta a la vulnerabilidad de las personas, es el de Apertura, seguido por los de Agradabilidad y Concientización. Por otra parte, el Neuroticismo no es un factor importante en la organización estudiada.

Por otra parte, para obtener una respuesta mucho más objetiva, se optó por procesar las respuestas de cada persona encuestada de manera individual, ya que según el análisis realizado en base a los papers seleccionados, existen factores con mucho más peso que otros. Por ello se unificaron los valores del Modelo de los Cinco Factores.

Tabla 11

Categorización mediante el rango y porcentaje de vulnerabilidad.

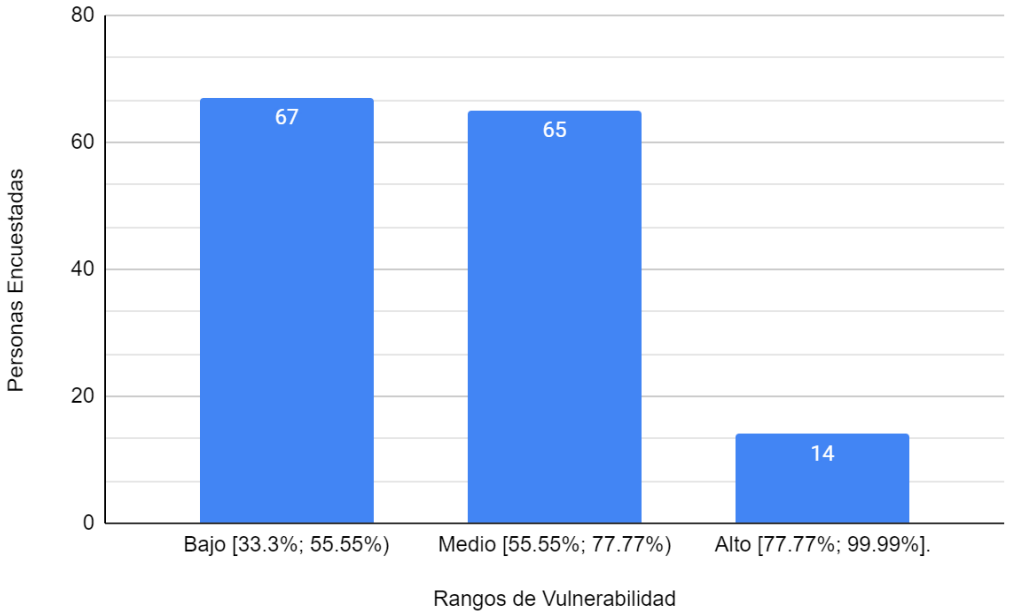
Encuestados	Rango de vulnerabilidad	Porcentaje de vulnerabilidad
1	Medio	59,90
2	Medio	59,23
3	Alto	77,83
4	Bajo	47,70
5	Bajo	37,13
6	Medio	70,13
7	Alto	78,77
8	Medio	56,07
9	Bajo	49,63

Una vez se establecieron los valores que tendría cada rango de los FFM se realizó una nueva tabulación con los datos obtenidos, dando como resultado que el caso óptimo es en el que la puntuación de una persona es de 33.3%, debido a que no existen valores de 0 dentro de la encuesta. Es por ello que para lograr determinar con más precisión en que rango de vulnerabilidad se encuentra cada puntuación se ha establecido los siguientes rangos; Bajo $[33.3; 55.55)$, Medio $[55.55; 77.77)$ y Alto $[77.77; 99.99]$.

Esto dio como resultado lo expuesto en la Figura 18, donde se aprecia que la gran mayoría de la población encuestada se encuentra en los rangos de Bajo y Medio, tendiendo una ligera porción en Alto lo cual podría ser muy peligroso si se tiene en cuenta que un error humano dentro de una institución podría comprometer la seguridad de todos.

Figura 18

Recuento de los rangos de vulnerabilidad de todos los encuestados.



CAPITULO V

CONCLUSIONES

Terminada la investigación se concluye que:

Se realizó con éxito el modelo que nos permite determinar las características o factores de personalidad que hacen más vulnerables a las personas para que sean víctimas de los ataques basados en la Ingeniería Social.

De acuerdo con la Revisión Sistemática de la Literatura, se logró obtener un conjunto de características y rasgos de personalidad más comunes en las personas que son víctimas de ataques de Ingeniería Social. Estas características pasaron por un proceso de extracción y categorización basándose en el FFM, en el cual se determinó que la Agradabilidad alta y la conciencia baja son los factores más comunes que influyen las personas más vulnerables.

Según el estudio realizado y los resultados obtenidos, se pueden clasificar los rasgos de personalidad que hacen más vulnerables a las personas ante los ataques de Ingeniería Social, conforme al FFM como: la Apertura a la experiencia (28.8%), seguido por Agradabilidad (27.9%), Conciencia (20.2%), Neuroticismo (11.5%) y Extraversión (11.5%).

Los resultados de la encuesta fueron favorables para la investigación realizada, ya que gracias a estos resultados se pudo desarrollar una tabulación que permita determinar los rangos de cada Factor dentro del FFM, los cuales son Bajo, Medio y Alto.

En base a la tabulación de los datos obtenidos de la encuesta de personalidad realizada se pudo establecer un modelo que permite determinar el nivel de vulnerabilidad de las personas, esto con el fin de poder determinar si

dentro de una institución u organización el personal que la conforma requiere algún tipo de capacitación en lo que a seguridad informática e Ingeniería Social se refiere.

Como resultado del estudio que se realizó a las 146 individuos de la Universidad de las Fuerzas Armadas ESPE se obtuvo que ;67 personas están en el rango Bajo, es decir que obtuvieron una puntuación entre 33.33% y 55.549%, estas personas podrían reconocer o evitar un ataque de Ingeniería Social al ser más precavidos y cuidados con sus acciones; 65 personas alcanzaron el rango Medio, debido a que su puntuación final se encuentra entre 55.55% y 77.769%, estas personas suelen tener comportamientos discretos o premeditados, pero su curiosidad o necesidad de nuevas experiencias les podría hacer considerar de manera inocente las peticiones del atacante; finalmente tenemos que solo 14 de 146 participantes llegaron al rango Alto los cuales obtuvieron un puntaje entre 77.77% y 99.99%, las personas que se encuentran en este rango son quienes evitan las responsabilidades, tratan de hacer todo de manera apresurada sin tomar las medidas de prevención necesarias y confían en cualquier tipo de propuesta o simplemente actúan por reacción e instinto.

A pesar que solo 14 personas están en el rango Alto, es algo muy negativo para la organización, debido a que luego de la investigación que se realizó se puede determinar que, aunque una sola persona fuese víctima de un ataque de Ingeniería Social ya estaría comprometiendo la seguridad de toda la empresa u organización a la que pertenezca. Es por este motivo que se concluye que la realización de un estudio de los FFM dentro cualquier institución podría ser conveniente a la hora de disminuir las posibles vulnerabilidades que presente el personal, debido a se conocería quienes están teniendo algún tipo de problema y de esta manera ayudarlos a tratar de resolverlos mediante capacitaciones, charlas o cualquier tipo de actividad que la empresa u organización vea conveniente para su personal.

Recomendaciones

Debido al avance y el uso intensivo de las tecnologías de la información, junto con la naturaleza confiada e ingenua de las personas, han surgido nuevas técnicas de fraude y engaño que los atacantes tienen como objetivo ejecutar a través de la Ingeniería Social, así, es recomendable que los usuarios tomen las medidas necesarias o sean capacitados para evitar que sean víctimas a dichos ataques.

Para comprender la clasificación y la puntuación de los rasgos de personalidad del modelo de los cinco factores que influyen en el comportamiento de las personas ante los ataques de Ingeniería Social, se recomienda hacer una revisión sistemática de la literatura sobre el Inventario de los Cinco Grandes (BFI).

Trabajo a futuro

Mientras se desarrolló este proyecto se utilizó el Modelo de los Cinco Factores para enmarcar los rasgos de personalidad de las personas, pero este estudio puede ser extendido al usar otro modelo de rasgos de personalidad, como el Indicador Myers-Briggs (Myers–Briggs Type Indicator) o la Triada Oscura (Dark Triad), y hacer una comparación entre estos modelos versus los ataques de Ingeniería Social.

Extender la encuesta de este estudio a un número mayor de personas, con el propósito de recopilar más información, la cual puede ser utilizada en un algoritmo de Aprendizaje Automático, que permita determinar de manera más precisa los rasgos de personalidad que influyen en las vulnerabilidades de las personas encuestadas.

Este modelo puede ser implementado en una plataforma web abierta al público, para que pueda ser utilizada por distintas organizaciones o instituciones que opten por realizar una evaluación de rasgos de personalidad a sus trabajadores. Dicha evaluación le puede proporcionar un resultado automático e

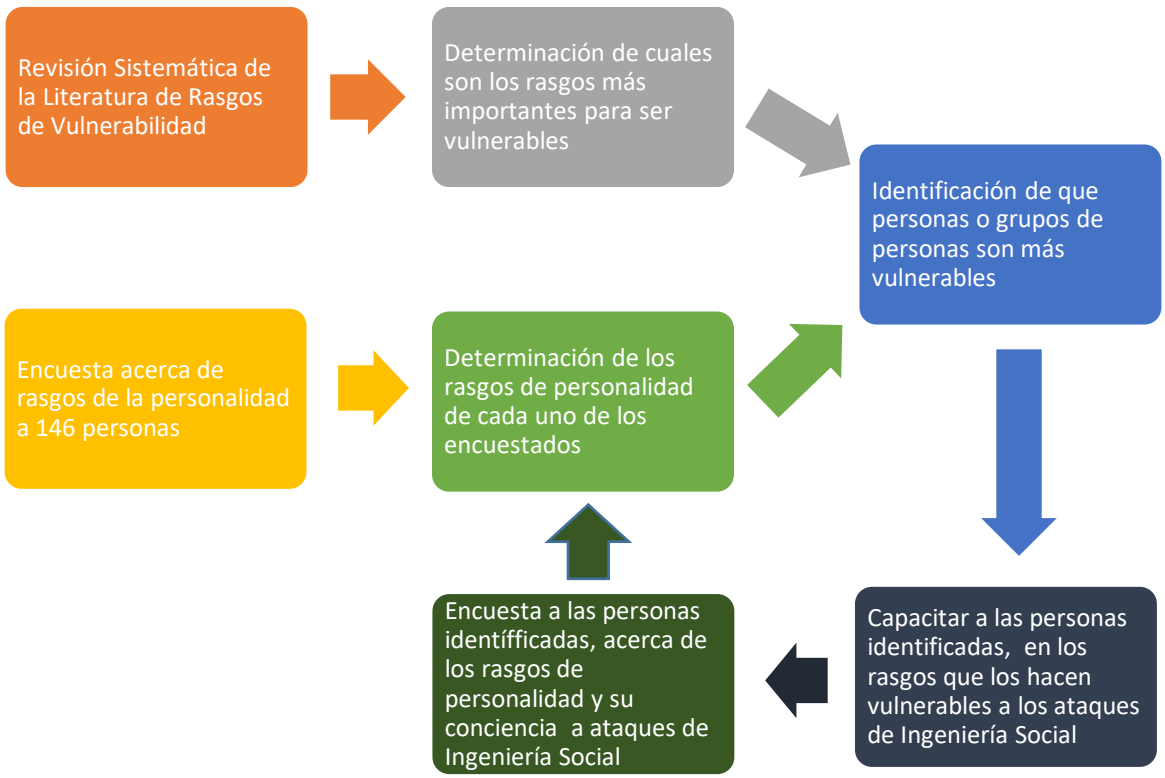
inmediato sobre aquellas personas que pueden ser más vulnerables a los ataques de Ingeniería Social y que necesitan de una capacitación.

Desarrollar y ejecutar un ataque controlado a baja escala que se base en los rasgos de personalidad del modelo de los cinco factores para medir su porcentaje de efectividad y luego realizar una capacitación a las personas que hayan sido víctimas del ataque para que mejoren sus rasgos personales que las hacen más vulnerables.

En la Figura 19, se propone un algoritmo que puede ser implementado en la metodología un proyecto a futuro. Como se puede observar, a diferencia de la metodología utilizada en este estudio, se puede continuar con la capacitación a las personas vulnerables identificadas y realizar una nueva encuesta para determinar si esas personas se capacitaron adecuadamente para cada factor de personalidad.

Figura 19.

Algoritmo de la metodología del modelo a utilizar en un proyecto futuro



CAPÍTULO VI

BIBLIOGRAFÍA

Abeywardana, K. Y., Pfluegel, E., & Tunnicliffe, M. J. (2016). A layered defense mechanism for a social engineering aware perimeter. *Proceedings of 2016 SAI Computing Conference, SAI 2016*, 1054–1062. https://doi.org/10.1109/SAI.2016.7556108

Alazri, A. S. (2016). The awareness of social engineering in information revolution: Techniques and challenges. *2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015*, 198–201. https://doi.org/10.1109/ICITST.2015.7412088

Albladi, S. M., & George, R. S. (2017). Personality traits and cyber-attack victimisation: Multiple mediation analysis. *Joint 13th CTTE and 10th CMI Conference on Internet of Things - Business Models, Users, and Networks*, *2018-Janua*, 1–6. https://doi.org/10.1109/CTTE.2017.8260932

Anguita, J. C., Labrador, J. R. R., & Campos, J. D. (2003). La encuesta como técnica de investigación . Elaboración de cuestionarios y tratamiento estadístico de los datos (I). *Atención Primaria*, *31*(8), 527–538. https://doi.org/10.1016/S0212-6567(03)70728-8

Ayan, R., Nesnow, G., Hammady, H., Mora, R., & Moeller, G. (n.d.). *About Rayyan*. https://www.rayyan.ai

Benavides, E., Fuertes, W., & Sanchez, S. (2020a). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura. *Ciencia y Tecnología*, *13*(1), 97–104. https://doi.org/10.18779/cyt.v13i1.357

Benavides, E., Fuertes, W., & Sanchez, S. (2020b). Un experimento para crear conciencia en las personas acerca de los ataques de Ingeniería Social. *Ciencia Unemi*, *13*(32), 27–40. https://doi.org/10.29076/issn.2528-7737vol13iss32.2020pp27-40p

Benet-Martinez, V., & John, O. P. (1998). Los Cinco Grandes Across Cultures and Ethnic Groups. *Journal of Personality and Social Psychology Copyright*, *75*(3), 729–750.

Breda, F., Barbosa, H., & Morais, T. (2017). Social Engineering and Cyber Security. *INTED2017 Proceedings*, *1*, 4204–4211. https://doi.org/10.21125/inted.2017.1008

Castellanos, E. J. S. (2018). *INGENIERÍA SOCIAL: CORROMPIENDO LA MENTE HUMANA*. ..SEGURIDAD. https://revista.seguridad.unam.mx/numero-10/ingenierí-social-corrompiendo-la-mente-humana

Cusack, B., & Adedokun, K. (2018). The impact of personality traits on user's susceptibility to social engineering attacks. *Proceedings of the 16th Australian Information Security Management Conference*, 83–89. https://doi.org/10.25958/5c528ffa66693

Dominguez Lara, S., Merino Soto, C., Zamudio, B., & Guevara Cordero, C. (2018). Big Five Inventory in peruvian college students: Preliminary results of its validation. *Psykhe*, *27*(2), 1–12. https://doi.org/10.7764/psykhe.27.2.1052

Fan, W., Lwakatare, K., & Rong, R. (2017). Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations. *International Journal of Computer Network and Information Security*, *9*(1), 1–11. https://doi.org/10.5815/ijcnis.2017.01.01

John, O. P., Hampson, S. E., & Goldberg, L. R. (1991). The basic level in personality-trait hierarchies: Studies of trait use and accessibility in different contexts. *Journal of Personality and Social Psychology*, *60*(3), 348–361. https://doi.org/10.1037//0022-3514.60.3.348

Kaspersky Lab. (2021). *Ingeniería social*. Latam Kaspersky. https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering - A systematic literature review. *Information and Software Technology*, *51*(1), 7–15. https://doi.org/10.1016/j.infsof.2008.09.009

Lawrence, P., & John, O. (1995). *Handbook of personality*. http://jenni.uchicago.edu/econ-

psych-traits/John_Srivastava_1995_big5.pdf

Li, X. (2017). A Review of Motivations of Illegal Cyber Activities. *Kriminologija & Socijalna Integracija*, *25*(1), 110–126. https://doi.org/10.31299/ksi.25.1.4

Maseno, E. M. (2017). *Vishing attack detection model for mobile users*. 1–69.

McCrae, R. R., & Jhon, P. O. (2013). *An Introduction to the Five-Factor Model and Its Applications*. 1–3.

Papatsaroucha, D., Nikoloudakis, Y., Kefaloukos, I., & Pallis, E. (2021). *A Survey on Human and Personality Vulnerability Assessment in Cyber- security : Challenges , Approaches , and Open Issues*.

RAE. (2021). *Diccionario de la lengua española*. Real Academia Española. https://dle.rae.es

Rezabala, E. R., & Moreira, K. A. (2020). *"Análisis De Las Incidencias E Impactos De Ataques De Ingeniería Social O Ciberdelitos En La Carrera De Ingeniería Civil De La Facultad De Ciencias*.

Robert Ayan, Geoff Nesnow, Hossam Hammady, Ramy Mora, & Greg Moeller. (n.d.). *Rayyan - About Us*. Retrieved September 5, 2021, from https://www.rayyan.ai/about-us

Russo, T. (2019). *SIMulated Trust: How Malicious Actors Take Advantage of Cellular Carriers to Perform SIM Swapping Attacks*.

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4). https://doi.org/10.3390/FI11040089

Shahzad, R. K., & Lavesson, N. (2011). Detecting scareware by mining variable length instruction sequences. *2011 Information Security for South Africa - Proceedings of the ISSA 2011 Conference*. https://doi.org/10.1109/ISSA.2011.6027523

Souri, A., Hosseinpour, S., & Rahmani, A. M. (2018). Personality classification based on profiles of social networks' users and the five-factor model of personality. *Human-Centric Computing and Information Sciences*, *8*(1). https://doi.org/10.1186/s13673-

018-0147-4

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

Thomas, J. E. (2018). Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks. *International Journal of Business and Management*, *13*(6), 1. https://doi.org/10.5539/ijbm.v13n6p1

Wehrli, S. (2008). Personality on social network sites: An application of the five factor model. *ETH Zurich Sociology Working Paper*, *7*, 1–17.

Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing , SMiShing & Vishing : An Assessment of Threats against Mobile Devices. *Journal of Emerging Trends in Computing and Information Sciences*, *5*(4), 297–307.