Detección de Vulnerabilidades en el

Comportamiento de las Personas para Evitar que sean Víctimas de Ataques de Ingeniería Social

Rocohano Ramos, Ronny Gonzalo y Silva Ordoñez, Luis Daniel

Departamento de Ciencias de la Computación

Carrera de Ingeniería en Tecnologías de la Información

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

Ing. Benavides Astudillo, Diego Eduardo, Mgs.

8 de septiembre 2021

Informe de originalidad

NOMBRE DEL CURSO
NRC 6932 - MIC - PI PROFESIONALIZANTE

NOMBRE DEL ALUMNO
RONNY GONZALO ROCOHANO RAMOS

NOMBRE DEL ARCHIVO
RonnRocohano_LuisSilva - Revisión de Originalidad

SE HA CREADO EL INFORME
8 sept 2021

Resumen

Fragmentos marcados	0	0 %
Fragmentos citados o entrecomillados	1	0,1 %

Coincidencias de la Web

csu.edu.au	1	0,1 %

1 fragmento

Fragmento del alumno ENTRECOMILLADO

El artículo presentado por (Wilcox & Bhattacharya, 2016) titulado, "A Framework to Mitigate Social Engineering through Social Media within the Enterprise

Mejor coincidencia en la Web

Wilcox, H., & Bhattacharya, M. ... (2016). **A Framework to Mitigate Social Engineering through Social Media within the Enterprise**. In Proceedings of the 2016 IEEE ...

A Framework to Mitigate Social Engineering through Social Media ... https://researchoutput.csu.edu.au/en/publications/a-framework-to-mitigate-social-engineering-through-social-media-w

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 CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

CERTIFICACIÓN

Certifico que el trabajo de titulación, **"Detección de Vulnerabilidades en el Comportamiento de las Personas para Evitar que sean Víctimas de Ataques de Ingeniería Social"**, fue realizado por los señores **Rocohano Ramos, Ronny Gonzalo y Silva Ordoñez, Luis Daniel**, 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 sustenten públicamente.

Santo Domingo, 8 de septiembre 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 CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

RESPONSABILIDAD DE AUTORÍA

Nosotros, **Rocohano Ramos, Ronny Gonzalo** y **Silva Ordoñez, Luis Daniel**, con cedulas de ciudadanía n° 2300369010 y 1724856859, declaramos que el contenido, ideas y criterios del trabajo de titulación: **"Detección de Vulnerabilidades en el Comportamiento de las Personas para Evitar que sean Víctimas de Ataques de Ingeniería Social"** es de 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, 8 de septiembre 2021.

Rocohano Ramos, Ronny Gonzalo
C.C.: 2300369010

Silva Ordoñez, Luis Daniel
CC.: 1724856859

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

AUTORIZACIÓN DE PUBLICACIÓN

Nosotros, **Rocohano Ramos, Ronny Gonzalo** y **Silva Ordoñez, Luis Daniel**, con cedulas de ciudadanía n° **230036901-0 y 172485685-9,** autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **"Detección de Vulnerabilidades en el Comportamiento de las Personas para Evitar que sean Víctimas de Ataques de Ingeniería Social"** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi/nuestra responsabilidad.

Santo Domingo, 8 de septiembre 2021.

Rocohano Ramos, Ronny Gonzalo
C.C.: 2300369010

Silva Ordoñez, Luis Daniel
CC.: 1724856859

Dedicatoria

Esta tesis está dedicada principalmente a Dios,

por darme la fuerza y perseverancia para cumplir con el objetivo de acabar mis estudios.

A mis padres y a mi hermano, por su sacrificio, trabajo y amor, en este proceso de estudio.

Gracias a ustedes he logrado culminar esta importante etapa de mi vida.

A todas las personas que me han apoyado y me dieron la oportunidad de cumplir mis metas, en especial, a aquellos docentes que compartieron sus conocimientos.

Ronny Rocohano

Esta tesis está dedicada principalmente a Dios,

por darme la fuerza y perseverancia para cumplir con el objetivo de acabar mis estudios.

A mis padres y a mis hermanos, por su sacrificio, trabajo y apoyo, en este proceso de estudio.

A aquellos docentes que me apoyaron y compartieron sus conocimientos.

Luis Silva

Agradecimiento

Agradezco principalmente a Dios por guiarme a lo largo de mi vida, bendecirme y permitirme haber llegado hasta este momento.

Mi profundo agradecimiento a mis padres Gonzalo y Nelly, y a mi hermano Sebastián, por ser ellos mi principal fuente de inspiración y los promotores de cumplir este sueño.

Agradezco a las autoridades, al Departamento de Ciencias de la Computación, y a la carrera de Ingeniería en Tecnologías de la Información de la Universidad de las Fuerzas Armadas ESPE, Sede Santo Domingo, por confiar en mí y darme la oportunidad de culminar esta etapa educativa dentro de su establecimiento.

De igual manera mis agradecimientos a mi director de Tesis, el Ing. Benavides, Eduardo, Mgs, quien, con la enseñanza, sus consejos y correcciones hoy he podido culminar este trabajo.

Ronny Rocohano

Agradezco a mis padres William y Alicia, y a mis hermanos Erick y Melany, por ser ellos mi principal fuente de inspiración y los promotores de cumplir este objetivo en mi vida.

Agradezco a la carrera de Ingeniería en Tecnologías de la Información de la Universidad de las Fuerzas Armadas ESPE, Sede Santo Domingo, por confiar en mí y darme la oportunidad de culminar esta etapa educativa dentro de su establecimiento.

De igual manera mis agradecimientos a mi Tutor de Tesis, el Ing. Benavides, Eduardo, Mgs, gracias a quien he podido culminar este trabajo.

Luis Silva

Índice de contenidos

Carátula 1
Análisis Google Assignments 2
Certificado del director 3
Responsabilidad de autoría 4
Autorización de publicación 5
Dedicatoria 6
Agradecimiento 7
Índice de contenidos 8
Índice de tablas 11
Índice de figuras 12
Resumen 13
Abstract 14
Capítulo I 15
Introducción 15
Antecedentes 15
Definición de la problemática 16
Justificación 18
Objetivos 19
Objetivo General 19
Objetivos Específicos 19
Alcance 19
Capítulo II 20
Marco Teórico 20
Estado del arte 20
Fases de un ataque informático 24
Reconocimiento 25
Exploración 25
Obtener acceso 25
Mantener acceso 25
Borrar huellas 25
Tecnologías de la Información 25
Virus Informático 26

Seguridad Informática 26
Seguridad de la información 26
Riesgo 27
Amenaza 27
Vulnerabilidad 28
Triada de la seguridad 28
Confidencialidad 28
Integridad 28
Disponibilidad 29
Impacto 29
Ciberdelincuente 29
Ciberataque 30
Ingeniería Social 30
Phishing 30
Pretexting 31
Ransomware 31
Spyware 31
Componentes de la encuesta de comportamiento 32
Escala de comportamiento de riesgo - Risky Behavior Scale (RBS) 32
Escala de comportamiento conservador - Conservative Behavior Scale (CBS) 32
Escala de exposición a ofensas - Exposure to Offence Scale (EOS) 32
Escala de percepción del riesgo - Risk Preception Scale (RPS) 32
Capítulo III 33
Metodología 33
Tipo de investigación 34
Fuente de datos 34
Planteamiento de la hipótesis 35
Planteamiento del diseño de la investigación 35
Selección de la muestra 36
Tamaño de la muestra 37
Muestra seleccionada para la investigación 38
Recolección de datos 38
Perfiles de Usuario 39

Sección para Docentes 40
Sección para Estudiantes 41
Sección para personal Administrativo 42
Escala de Comportamiento de Riesgo (RBS) 43
Escala de Comportamiento Conservador (CBS) 44
Escala de Exposición a ofensas (EOS) 46
Escala de Percepción de Riesgos (RPS) 47
Periodo de recolección de datos 48
Análisis de datos 48
Capítulo IV 50
Resultados y Discusión 50
Resultados de los datos demográficos 50
Resultados de los grupos Docentes, Administrativo y Estudiantes 51
Resultados de las escalas (RBS, CBS, EOS, RPS) 54
Prueba de Hipótesis 65
Prueba de H1: No hay diferencia significativa entre las escalas {RBS, CBS, EOS, RPS} con respecto a su promedio. 65
Prueba de H2: No hay diferencia significativa entre los grupos encuestados (docentes, administrativos o militares, estudiantes) con respecto a su promedio 67
Prueba de H3: La exposición de horas/día que tienen los usuarios al usar el Internet afecta el promedio de las escalas {RBS, CBS, EOS, RPS}. 70
Prueba de H4: Existe una correlación significativa entre los promedios de las escalas {RBS, CBS, EOS, RPS}. 72
Capítulo V 76
Conclusiones, Trabajo Futuro y Recomendaciones 76
Conclusiones 76
Trabajo Futuro 76
Recomendaciones 77
Bibliografía 77

Índice de tablas

Tabla 1 Investigaciones publicadas en relación a los ataques de Ingeniería Social 21
Tabla 2 Preguntas para recolectar información de los usuarios encuestados 39
Tabla 3 Preguntas para recolectar información de los Docentes encuestados 40
Tabla 4 Preguntas para recolectar información de los Estudiantes encuestados 41
Tabla 5 Preguntas para recolectar información del personal Administrativo y militar 42
Tabla 6 Escala de Comportamiento de Riesgo (RBS) 44
Tabla 7 Escala de Comportamiento Conservador (CBS) 45
Tabla 8 Escala de Exposición a Ofensas (EOS) 46
Tabla 9 Escala de Percepción de Riesgos (RPS) 47
Tabla 10 Resultados de las preguntas de la sección Perfil de Usuario 51
Tabla 11 Resultados de las preguntas de la sección Docentes 52
Tabla 12 Resultados de las preguntas de la sección Estudiantes 52
Tabla 13 Resultados de las preguntas de la sección Administrativos y militares 53
Tabla 14 Resultados de las preguntas de la Escala de Comportamiento de Riesgo (RBS) 54
Tabla 15 Resultados de las preguntas de la Escala de Comportamiento Conservador (CBS) 58
Tabla 16 Resultados de las preguntas de la Escala de Exposición a Ofensas (EOS) 60
Tabla 17 *Resultados de las preguntas de la Escala de Percepción del Riesgo (RPS)* 62
Tabla 18 Promedio de las respuestas de las escalas (RBS, CBS, EOS, RPS) 65
Tabla 19 Cálculo ANOVA entre las escalas {RBS, CBS, EOS, RPS} 66
Tabla 20 Descripción general de las escalas (RBS, CBS, EOS, RPS) 66
Tabla 21 Resultados de la prueba de Tukey entre las escalas (RBS, CBS, EOS, RPS) 67
Tabla 22 ANOVA entre los grupos Docente, Estudiante, Administrativo y Militar 68
Tabla 23 Resultados de la prueba de Tukey entre los grupos (Docentes, Administrativo y Estudiantes) y la escala (CBS) 69
Tabla 24 Resultados de la prueba de Tukey entre los grupos (Docentes, Administrativo y Estudiantes) y la escala (RPS) 69
Tabla 25 ANOVA del Tiempo medio de uso de Internet entre los grupos Docente, Estudiante, Administrativo y Militar 70
Tabla 26 Resultados de la prueba de Tukey entre el tiempo medio de uso de Internet y la escala (RBS) 71
Tabla 27 Resultados de la Correlación de Pearson 72

Índice de figuras

Figura 1 Etapas de un ataque informático 24
Figura 2 Dispersión entre las escalas CBS y RPS 73
Figura 3 Dispersión entre las escalas CBS y EOS 74
Figura 4 Dispersión entre las escalas EOS y RPS 75

Resumen

Uno de los ataques más efectivos en la ciberseguridad, es el de Ingeniería Social, en que el atacante engaña a un usuario final, con la finalidad de perjudicarlo. Existen medidas de hardware y software para hacer frente a este tipo de ataques, sin embargo, las personas en sí son el eslabón más vulnerable en esta cadena de la seguridad, además, se hace la suposición de que características propias del comportamiento de las personas, las hacen más vulnerables, es así que el objetivo de este estudio es determinar cuáles son las características más comunes que hacen vulnerables a estas personas, y qué grupos de personas son más vulnerables. Para esto, se realizó una encuesta a 153 personas, entre docentes, administrativos y estudiantes de una entidad educativa superior, sobre cuatro escalas que toman en cuenta los siguientes comportamientos: comportamiento de riesgo, comportamiento conservador, exposición a la ofensa y percepción al riesgo. Luego, los resultados obtenidos son analizados, obteniéndose que los usuarios que tienen mayor percepción de riesgo, son los que están menos expuestos a un ataque de Ingeniería Social. También se concluye que, los grupos analizados de docentes y administrativos, son menos propensos a ser víctimas de estos ataques, en comparación con los estudiantes, y que las personas que pasan más tiempo frente a un computador, y las que son más permisivas a comportamientos de riesgos, son más vulnerables a estos ataques.

- Palabras claves:
    - **INGENIERÍA SOCIAL**
    - **CIBERSEGURIDAD**
    - **RIESGO**
    - **VULNERABILIDADES**
    - **COMPORTAMIENTO**

Abstract

One of the most effective attacks on cybersecurity is Social Engineering, in which the attacker deceives an end-user to harm him. There are hardware and software countermeasures to deal with these types of attacks. However, people themselves are the most vulnerable link in this security chain. In addition, there are influencing factors in people's behavior, which make them more vulnerable. This study aims to determine the most common characteristics that make users vulnerable, either individually or in groups. For this, we conduct an exploratory and descriptive study on 153 persons among administrative, academics, and students of a superior educational entity on four scales that consider the following behaviors: risk behavior, conservative behavior, exposure to offense, and perception of risk. The results obtained show that the users with the highest risk are the least exposed to a Social Engineering attack. It is also concluded that the analyzed groups of academics and administrators are less likely to be victims of these attacks than students. Finally, it is inferred that people who spend more time in front of a computer and are more permissive of risky behaviors are more vulnerable to these attacks.

- Keywords:
    - **SOCIAL ENGINEERING**
    - **CYBERSECURITY**
    - **RISK**
    - **VULNERABILITIES**
    - **USER BEHAVIOR**

Capítulo I

Introducción

Este capítulo tiene como propósito realizar la investigación y revisión del estado del proyecto. En esta sección se detallan los antecedentes del proyecto, los cuales se centran en la revisión de literatura de los ataques informáticos, el alcance del proyecto mediante una muestra a una población determinada y los objetivos. La iniciación de este capítulo nos servirá como punto de partida para conocer los aspectos actuales de la Seguridad de la Información y los ataques de Ingeniería Social. Una vez revisados los antecedes, se pudo determinar la problemática existente y la dirección del proyecto de titulación.

Antecedentes

El gran avance de las tecnologías en los últimos años ha generado un salto considerable a nuevas formas de comunicación y divulgación de la información. Con el paso el tiempo, la información se ha convertido en el punto central a proteger a nivel personal u organizacional, pero a pesar de los avances en la seguridad de los Sistemas de Información, el usuario final sigue siendo el factor más vulnerable y el causante de las brechas de seguridad (Lee et al., 2018).

Según (Orgill et al., 2004), en su estudio de “La ciberseguridad mediante la piratería de empleados”, describe que las personas, los procesos y la tecnología son los pilares fundamentales de los cuales depende la Seguridad de la Información. En gran parte, estos pilares son afectados por los ataques de Ingeniería Social, los cuales se producen cuando se logra obtener información o activos mediante técnicas de manipulación de usuarios (Lee et al., 2018). Muchos investigadores se han dado a la tarea de buscar los puntos débiles en seguridad dentro las organizaciones, para evitar los ataques de Ingeniera Social, debido a que los ataques son enfocados a personas que utilizan infraestructuras de Tecnologías de la Información (TI). Los atacantes utilizan un conjunto de procesos o técnicas que conllevan a crear brechas o generar

comportamientos convincentes dentro de los pilares de la Seguridad de la Información, haciendo que el objetivo divulgue información o que actué a favor del adversario para que este realice trabajos maliciosos (Edwards et al., 2017).

Para contrarrestar los ataques de Ingeniería Social, se ha logrado comprender que el usuario final es el eslabón más débil dentro de los Sistemas de Información y que es donde la mayoría de la protección se debería enfocar, es por ello que en el estudio de (Öɬütçü et al., 2016a), se detalla que es importante evaluar el comportamiento humano y los riesgos que se encuentran relacionados a los usuarios. Esta investigación explora estos comportamientos mediante la realización de una encuesta hecha por expertos empleados de la Asociación Turca de Seguridad de la Información y de la rama de Delitos Cibernéticos de la Dirección General de Seguridad. La investigación encontró una relación entre cuatros escalas de comportamiento del usuario, que hacen vulnerable al usuario final por características como: promedio de edad, desconocimiento al utilizar los Sistemas de Información, exposición a riesgos, entre otros.

Definición de la problemática

Las TI han sido desarrolladas a partir de la búsqueda del acceso y producción de la información, teniendo una gran acogida actualmente en aspectos personales y organizaciones. Debido al gran desarrollo y uso de las TI, estas se encuentran en todas las áreas de trabajo ofreciendo resolución de problemas y sencillez en la realización de tareas cotidianas. Esto ha encaminado a que los usuarios utilicen con exceso de confianza las TI y se olviden que estas no cuentan con una protección completa, generando que personas externas o atacantes, por medio del uso de un conjunto de técnicas conocidas como Ingeniera Social, obtengan acceso a datos, procesos, credenciales, entre otros, de una persona u organización.

La utilización de las TI trae consigo amenazas y riesgos, que son generados por vulnerabilidades o brechas que son explotadas por atacantes, cuyo objetivo es conseguir de manera ilegal accesos a todo tipo información y causar daños dentro de una organización o directamente a una persona. Desde que empezaron los ataques a sistemas, pérdida o robos de información y accesos no autorizados, varios investigadores se han dado a la tarea de combatir los ataques de Ingeniera Social, tratando de cerrar las brechas de seguridad que se encontraban en las redes de acceso a Internet, ordenadores, móviles, tabletas, servidores, entre otros. Al investigar las causas de los ataques de Ingeniería Social, los investigadores llegaron a la conclusión de que el usuario final era el factor más débil de la Seguridad Informática y que debido a su forma de actuar, daba paso a ser atacado.

Se ha logrado demostrar que mientras el usuario sea concientizado en la Seguridad de la Información, este tomará las debidas precauciones para salvaguardar la información a la que tiene acceso. En el caso en que el usuario no tenga conocimiento de Seguridad de la Información, y al no saber las formas de proteger esta información, va a ser más propenso a sufrir ataques de Ingeniería Social. Tener en cuenta esta situación tendrá beneficios para todas las personas que utilicen las TI y contribuirá a mejorar la protección de la información por medio de procesos que eviten a los atacantes encontrar vulnerabilidades.

Este proyecto tiene como objetivo medir el conocimiento que tienen las personas acerca de la Seguridad de la información y comprender como estas pueden actuar frente a posibles ataques de Ingeniería Social. Se utilizarán métodos cuantitativos para obtener una visión profunda entre los diferentes tipos de personas y sus comportamientos, lo que derivará en ayudar a las personas u organizaciones a evitar los ataques de Ingeniería Social.

Justificación

La Ingeniería Social es un conjunto de técnicas que son usadas por los atacantes, quienes buscan sustraer información de una víctima. Los atacantes usan esta técnica debido al alto nivel de eficacia que tiene para lograr engañar a una víctima. Para identificar a una víctima, los atacantes se enfocarán en diversas características que pueden hacer más o menos vulnerable a una persona. Las personas no le dan la suficiente importancia a lo vulnerable que puede ser su información, ya sea su información personal o información que comprometa a la institución donde son empleados. En el contexto actual, la pandemia Covid-19 ha cambiado el estilo de vida de muchas personas, de manera que ahora estas están más expuestas al uso de Internet, ya sea por el trabajo en línea, educación o simplemente hacer uso de servicios en línea como pueden ser: servicios de streaming, de compras y pagos en línea. Así, hay una gran cantidad de usuarios que están expuestos a ser víctimas de estos ataques, debido a que al estar más tiempo haciendo uso de Internet o de dispositivos de TI, se encuentran mucho más vulnerables, y los atacantes se han dado cuenta de esto, de manera que en el reporte del año 2021 de ESET se ve reflejado que en el año 2020 los ataques de Ingeniería Social se duplicaron con respecto al 2019 (Lubeck, 2021), con lo que se tiene una base para demostrar la importancia que una persona debe dar a su seguridad al navegar por Internet.

Este proyecto de titulación está enfocado hacia las personas que son vulnerables a ataques de Ingeniería Social, para que con el conocimiento sobre los diversos tipos de ataques a los que pueden estar expuestos al hacer uso de Internet o de dispositivos de TI, pueda identificar estos ataques y saber cómo reaccionar al encontrarse expuesto ante esa situación.

Objetivos

Objetivo General

Determinar la relación que existe entre determinados comportamientos de las personas, y los ataques de IS de los que son víctimas

Objetivos Específicos

- Realizar una encuesta para poder caracterizar a las personas que son más propensas a recibir un ataque de Ingeniería Social.
- Realizar un análisis correlacional entre las características de las personas que son víctimas de ataques de Ingeniería Social.
- Analizar la relación existente entre las escalas de comportamiento de los usuarios.

Alcance

Este proyecto se plantea con el objetivo de ofrecer una propuesta para detectar que personas debido a su comportamiento, son más vulnerables a ser atacadas por técnicas de Ingeniería Social. El resultado puede ser utilizado posteriormente para que personas u organizaciones, puedan identificar a estas personas vulnerables y realizar una estrategia de concientización al peligro de estos ataques. Estas vulnerabilidades se pudieron identificar con una encuesta desarrollada en la Universidad de las Fuerzas Armadas Sede Santo Domingo, tomando en cuenta a los tres grupos principales de la Universidad, los cuales son: docentes, estudiantes y personal administrativo y militar los cuales de ahora en adelante serán mencionados como personal administrativo; logrando así, obtener información de los grupos, con la que se pudo recopilar los rasgos personales y sus comportamientos, e identificar las ocasiones y las técnicas, a las cuales pueden ser más vulnerables.

Capítulo II

Marco Teórico

En este capítulo se detallan los términos y conceptos necesarios para la comprensión de la propuesta del proyecto de titulación, tomando como punto principal la Seguridad de la Información tanto para usuarios como para organizaciones, el riesgo, vulnerabilidad, la probabilidad de ser víctima, el impacto que esto puede representar, las técnicas de Ingeniería Social, incluyendo sus fases, entre otros.

Para el desarrollo de este proyecto, se tomaron en cuenta investigaciones relacionadas con la Ingeniería Social. Al inicio de este proyecto se realizó una encuesta, similar a la realizada por (Öɬütçü et al., 2016a), la cual fue actualizada y aplicada en la Universidad de las Fuerzas Armadas ESPE Sede Santo Domingo, con el fin de identificar las características de los usuarios finales y aportar a las investigaciones pasadas con datos y procedimientos actuales.

Estado del arte

El estado del arte hace referencia a los estudios relacionados con la problemática descrita en el Capítulo I.

A continuación; se presentan los estudios o investigaciones, que ayudaron a resolver la problemática anteriormente mencionada, los que permitieron obtener, conceptos, análisis o palabras claves que ayudaron al desarrollo del presente trabajo de titulación.

Tabla 1

Investigaciones publicadas en relación a los ataques de Ingeniería Social

Titulo	Cita	Palabras claves
Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review	(Lee et al., 2018) Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. Journal 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)	social engineering, Phishing , anti-social engineering, cyber security awareness, information security awareness
Analysis of personal information security behavior and awareness	(Ö‡ütçü et al., 2016a) : Analysis of personal information security behavior and awareness. Manuscript Computers & Security	Information Security Behavior, Personal Information Security, Information Security Awareness, Scale Development, social engineering
A Risk Analysis Framework for Social Engineering Attack Based on User Profiling	(Ye et al., 2020) A Risk Analysis Framework for Social Engineering Attack Based on User Profiling. Journal of Organizational and End User Computing	Authority, Cloud Security, Network Security Assessment, Operating Frequency, Risk Analysis, Social Engineering, User Profiling, Vulnerability
A Framework to Mitigate Social Engineering through Social Media within the Enterprise	(Wilcox & Bhattacharya, 2016) A Framework to Mitigate Social Engineering through Social Media within the Enterprise. Journal	Social Media; Online Social Networking; Social Engineering; Securing Social Media; loT Security Governance; Social Media

Titulo	Cita	Palabras claves
	Proceedings of the 2016 IEEE 11th Conference on Industrial Electronics and Applications, ICIEA 2016	Policy; Information Security Threats.

(Rodriguez Rincón & García Valdés, 2018), presentan en su proyecto de titulación "Estudio de Metodologías de Ingeniería Social", una serie de procesos que son utilizados por los atacantes, para realizar fraudes con la información obtenida de diferentes víctimas, además de la caracterización de los ataques al momento de encontrar brechas de seguridad. Para fines de aprendizaje sobre los ataques de Ingeniería Social, el autor brinda el significado y los conceptos de todos los términos que tiene relación con los ataques informáticos, además de dar a conocer procesos, técnicas, métodos de prevención y ejemplos, para lograr un mejor entendimiento de las metodologías de la Ingeniera Social. Este estudio describe las técnicas que son utilizadas en la actualidad para realizar ataques de Ingeniería Social, mediante recursos audiovisuales, web o libros. El objetivo de la investigación es lograr que la Ingeniería Social esté presente en los usuarios finales, para que sepan cómo protegerse, cómo mitigar el riesgo dentro de una institución, cuáles son los roles que intervienen y sus características, la información que los atacantes buscan frecuentemente y cómo evitar ser un blanco fácil o ser engañado.

(Öɬütçü et al., 2016a), en su manuscrito "Analysis of personal information security behavior and awareness", plantea un estudio, para investigar los comportamientos de los usuarios finales al enfrentarse a riesgos en los Sistemas de Información, que pueden ser perjudiciales y generar daños a la Seguridad de la Información. Los autores presentaron acciones para prevenir que los usuarios finales no caigan como víctimas de ataques informáticos al no contar con experiencia adversa o medición de los riesgos. Como punto central los autores se

enfocaron en estudiar el comportamiento de los usuarios finales por medio de 4 escalas presentadas en una encuesta realizada a estudiantes, docentes y personal administrativo de una universidad en Turquía, las cuales medirían el comportamiento de riesgos, conservador, exposición a ofensas y percepción a riesgos.

Al finalizar el estudio llegaron a la conclusión que la mayor amenaza dentro de los Sistemas de Información son los usuarios, por lo que es importante evaluar el comportamiento de los mismos ante los riesgos presentes dentro de un lugar establecido. Las víctimas no solo son individuos, sino también grandes empresas o instituciones. Los autores tienen en cuenta que mientras los usuarios tengan más conocimiento en seguridad, puede que su comportamiento frente a los riesgos sea el más efectivo para proteger la información.

El articulo presentado por (Ye et al., 2020) titulado, “A Risk Analysis Framework for Social Engineering Attack Based on User Profiling”, describe la gravedad y el aumento de los ataques de Ingeniería Social al hacer uso de servicios en la nube, cómo los atacantes usan las diferentes técnicas y metodologías para obtener información privada enfocándose principalmente en el perfil del usuario. La investigación menciona la posibilidad de ser una víctima al usar servicios en la nube. Los autores hacen uso de instrumentos de evaluación cuantitativa, con los que relacionaron los perfiles y agruparon a los usuarios que tendrían un riesgo mayor y la clasificación de las características de los mismos. Con esta investigación, los autores aportan un marco de análisis enfocado en los ataques de Ingeniería Social, basándose en la cuantificación del riesgo y vulnerabilidad de los perfiles de usuarios analizados, que hicieron uso de los servicios de computación en la nube.

El artículo presentado por (Wilcox & Bhattacharya, 2016) titulado, “A Framework to Mitigate Social Engineering through Social Media within the Enterprise”, menciona el peligro y

las vulnerabilidades que tienen las empresas debido a los empleados que hacen uso de las redes sociales dentro de su área de trabajo. Los ataques de Ingeniería Social descritos en esta investigación, tienen el objetivo de obtener información confidencial de la empresa, a través de los empleados que hacen uso de redes sociales. La investigación se centra, en el estudio de los ataques de Ingeniería Social a través de los medios de comunicación para la creación de políticas de seguridad enfocadas a la seguridad de los dispositivos de TI de los empleados, con lo que esperan generar conocimiento sobre los posibles ataques de Ingeniería Social, al usar las redes sociales dentro de la organización y de esta manera reducir, prevenir o mitigar posibles vulnerabilidades de seguridad.

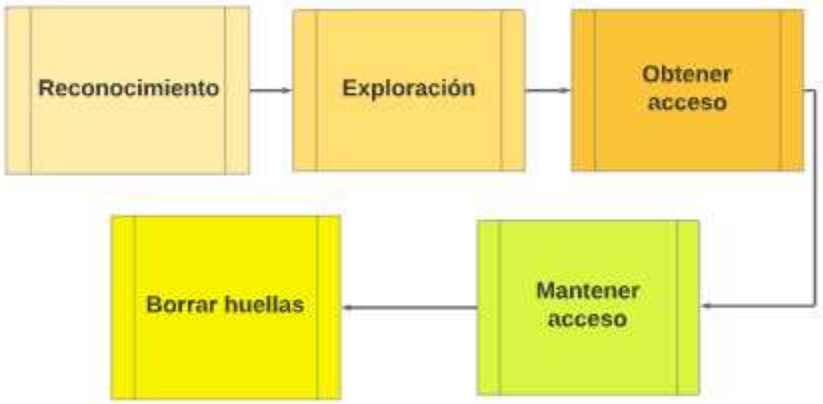
Fases de un ataque informático

Al identificar las fases o etapas de un ataque informático se reconoce la manera de actuar de los atacantes, esto permite analizar la perspectiva de cómo se lleva a cabo un ataque y qué características toma en cuenta el adversario para identificar a su víctima.

A continuación, en la Figura 1 se describen las fases de los ataques informáticos:

Figura 1

Etapas de un ataque informático



Reconocimiento

En esta fase, el adversario inicia el proceso de recolección de información de la víctima, la cual será afectada ya sea económicamente o socialmente; esto le permite al atacante establecer su estrategia basándose en las vulnerabilidades de la víctima.

Exploración

Esta fase consiste en hacer un filtrado de la información 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 adversario haya accedido al sistema de la víctima, su prioridad es mantener el sistema habilitado, de manera que creara o usará distintas técnicas para dejar una puerta trasera en el sistema.

Borrar huellas

Al haber accedido y mantener el acceso del sistema, el adversario 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 ingrese.

Tecnologías de la Información

Las TI se consideran herramientas, las cuales ayudan a la sociedad a mejorar su comunicación, divulgación y manejo de la información, haciendo uso de herramientas

tecnológicas (Causado Rodríguez et al., 2015). Esto permite que la sociedad pueda comunicarse haciendo uso de distintos tipos de dispositivos, sin importar la distancia y el acceso a la información.

Virus Informático

Los virus informáticos son una de las amenazas más antiguas en el mundo de la computación, ya que estos han existido desde la aparición de los ordenadores, con el objetivo de invadir los equipos de cómputo y crear problemas a los usuarios (Torres, 2021). Con el paso del tiempo, los virus informáticos han cambiado, siendo más independientes y asemejándose a los virus biológicos, de tal manera que estos se propagan infectando a todo el equipo, haciendo que peligre la información del dispositivo infectado. Hoy en día existen diversos tipos de virus informáticos, los cuales pueden afectar de diferentes maneras a los dispositivos que estén infectados. Con la creación de estos virus informáticos también se presentó la necesidad de crear antivirus para los dispositivos de TI, siendo los encargados de la detección y eliminación de los virus informáticos.

Seguridad Informática

Según (Suárez & Ávila, 2015), la seguridad informática es necesaria en todos los campos en los que estén involucrados los equipos tecnológicos, además se caracteriza por la confidencialidad que brinda a la información que contenga, por lo que se aplican diversos métodos para dar robustez a los sistemas de información de manera que estos sean más seguros y confiables.

Seguridad de la información

La seguridad de la información consiste en la protección de la información, haciendo uso de un conjunto de herramientas con el fin de proteger la información de accesos, divulgación,

modificación, lectura o eliminación de datos sin previa autorización, con el objetivo de mantener alejados a los atacantes, logrando que la información sea confidencial, mantenga su integridad y que está siempre se encuentre disponible (Soriano, n.d.).

Riesgo

La definición que ofrece la (ISO/IEC 27000, 2018) sobre el riesgo en el contexto de los sistemas de seguridad, este que este es un efecto previsto o negativo que recae sobre los sistemas de información. Esto está relacionado con la posibilidad de recibir un ataque, de manera que en caso de recibirlo se explotaran las vulnerabilidades que tengan los sistemas o las instalaciones de la organización, pero en el caso de que el riesgo sea asumido puede pasar de improvisto y no afectar a los sistemas, la información o las instalaciones de la organización. Existen diversos métodos de tratar los riesgos, estos se deben evaluar para saber el efecto negativo o esperado que tendrán dentro de la organización o del sistema de información y una vez analizados se deberán tomar decisiones para mitigarlos, mejorar la seguridad o definir si los riesgos serán asumidos (Park & Huh, 2020).

Amenaza

La definición que ofrece la (ISO/IEC 27000, 2018) sobre la amenaza en el contexto de la seguridad de la información, es que es algo que puede suceder o no, siendo cualquier cosa que pueda causar un daño grave sobre los sistemas o sobre la información que estos contengan. Las amenazas que se pueden presentar se enfocan en explotar las vulnerabilidades que presente el sistema. Estas se deber corregir o disminuir en lo posible, para que el sistema de información sea lo más seguro posible y pueda salvaguardar la información de los atacantes o de daños a las a los equipos de TI.

Vulnerabilidad

La definición que ofrece la (ISO/IEC 27000, 2018) sobre la vulnerabilidad en el contexto de la seguridad de los sistemas de información, es que esta es una debilidad que puede ser explotada por los atacantes, para vulnerar el sistema más fácilmente, enfocándose en que el sistema o procedimiento exponga la información ante las diversas amenazas. Estas deben ser identificadas y mitigadas en su mayoría, para que no representan una amenaza para la organización o la información que se esté almacenando en el sistema.

Triada de la seguridad

Esta triada corresponde a un modelo de Seguridad de la Información que permite enfocar las políticas de un individuo o una organización con el fin de mantener su información segura. Los tres principios de la triada de la seguridad son:

Confidencialidad

La definición que brinda la (ISO/IEC 27000, 2018) sobre la confidencialidad, es que es la propiedad con la cual la información no estará puesta a disposición libre, ni se puede divulgar a usuarios u organizaciones no autorizadas. Con esto se refiere al uso de mecanismos específicos como puede ser la aplicación de procesos de autenticación, control de acceso, entre otros, con los cuales se garantizará la confidencialidad e impedirá que la información o los datos puedan ser tomados por agentes externos.

Integridad

La definición que brinda la (ISO/IEC 27000, 2018) sobre la integridad, es que es la propiedad de la información con la que mantendrá su consistencia y exactitud de los datos almacenados, de manera que estos no sean alterados o estén incompletos. Se aplican modelos

o tipos de datos para validar que la información se mantenga exactamente como cuando fue ingresada, almacenada, recuperada o transferida.

Disponibilidad

La definición que brinda la (ISO/IEC 27000, 2018) sobre la disponibilidad, es que es la propiedad de la información que la hace accesible y utilizable, al momento en que el usuario la solicite. Para que los datos o la información siempre esté disponible y el acceso a la misma sea seguro, dependerá del Sistema de Información donde se encuentre almacenada, para que se pueda acceder de manera más fácil o difícil a los datos. En estos casos el sistema de información no deberá comprometer la información ni la accesibilidad a la misma.

Impacto

El impacto son los efectos que tienen las amenazas informáticas sobre la información, ya sea que se enfoquen contra una persona u organización (Quiroz & Macias, 2017). Dependiendo de la gravedad del impacto, esto generara incidentes a la confidencialidad, disponibilidad e integridad de la información, haciendo que el sistema de información ya no sea fiable y por ende los datos tampoco, generando problemas a la organización o a los usuarios que necesiten de dichos datos almacenados.

Ciberdelincuente

Un ciberdelincuente tiene un perfil parecido al de un delincuente tradicional, pero este aplica técnicas tecnológicas hacia sus víctimas, buscando obtener información personal de la víctima, para obtener una remuneración a cambio de devolver la información sustraída o simplemente para dañar la imagen de la víctima o de una organización (Warikoo, 2014). Los ciberdelincuentes, emplean diferentes tipos de herramientas para elaborar el ataque, y una vez con las herramientas, elaboran el método de ataque que explote de mejor manera las

vulnerabilidades que estos pudieran identificar como pueden ser: ataque de denegación de servicio (DDoS), spam, Phishing, entre otros. El éxito de su ataque dependerá de sus habilidades, de los riesgos que estén dispuesto a correr para lograr su objetivo, y del impacto que el ataque pueda conllevar.

Ciberataque

Las bases de un ciberataque se enfocan en intentar alterar los puntos operativos de un sistema, con el objetivo de eludir los protocolos o controles de acceso, para obtener información, datos relevantes, dar de baja al sistema o el servicio que este bajo ataque (Zhou et al., 2020). Los atacantes hacen uso de herramientas y métodos para detectar las vulnerabilidades y explotarlas al desarrollar el ataque, para que este sea lo más exitoso posible logrando los objetivos que los atacantes esperan.

Ingeniería Social

Según (López & Salvador, 2015), detalla que el término Ingeniera Social, es usado en primera instancia por Kevin Mitnick, mejor reconocido como el mejor hacker del mundo, donde sostiene que la Ingeniera Social es el uso de técnicas que son utilizadas, para poder ganarse la confianza de un usuario autorizado y engañarlo para que proporcione acceso a los sistemas informáticos de una entidad y realizar acciones de forma anónima con el fin de vulnerar brechas de seguridad.

Phishing

El Phishing es la técnica de Ingeniera Social más efectiva actualmente, en la cual los atacantes utilizan métodos como él envió de correos electrónicos para hacerse pasar por una entidad o personas reconocidas con el fin de sustraer información confidencial. En algunos casos el Phishing hace que las victimas tomen decisiones basándose en las emociones, y seguido a

esto manipulan a los usuarios, para proporcionar algún tipo de acceso o datos de gran importancia (López & Salvador, 2015).

Pretexting

El proceso del ataque Pretexting está basado en investigar de manera detallada a una víctima con el fin de utilizar un pretexto convincente y obtener información confidencial o valiosa que permita tener acceso a un sistema o servicio. Las etapas del Pretexting están divididas en crear un pretexto o historia convincente, contactar a la víctima y recopilar información.

Ransomware

Este ataque tiene como objetivo secuestrar información de uno o varios dispositivos a la vez. Una vez que el adversario tiene acceso a la información, la encripta para que la víctima no tenga acceso a esta. Lo que hace el adversario es pedir un rescate por la información, generando una clave privada y una publica, estas claves tienen la capacidad de encriptar y desencriptar la información. El adversario almacena esta clave en un servidor externo, donde la víctima no tendrá acceso (López & Salvador, 2015).

Spyware

Los Spyware, también conocidos como softwares espía, son programas que utilizan un código malicioso que es instalado en las computadoras o dispositivos de una víctima. El objetivo de este programa es espiar las acciones que realiza un usuario sin que este se dé cuenta. Lo que registran los Spyware son: comportamientos de la víctima, uso de Internet, contraseñas y nombres de usuario. Una vez obtenida la información de la víctima, esta se envía al propietario del software espía, el cual puede utilizar esta información para actos delictivos (Egele et al., 2007).

Componentes de la encuesta de comportamiento

Para la realización de este estudio, después de haber realizado una exhaustiva revisión de la literatura, se decidió utilizar la encuesta propuesta en (Öǂütçü et al., 2016b), la cual consta de la siguientes cuatro escalas:

Escala de comportamiento de riesgo - Risky Behavior Scale (RBS)

La escala RBS hace referencia al comportamiento de los usuarios, frente a un riesgo en los Sistemas de Información. Este comportamiento se puede dar cuando un usuario utiliza un ordenador sin las respectivas medidas de seguridad, y pone en riesgo a las demás personas que conviven o trabajan en el mismo espacio.

Escala de comportamiento conservador - Conservative Behavior Scale (CBS)

La escala CBS tiene como objetivo medir el actuar del usuario cuando está utilizando un Sistema de Información, es decir, define las acciones específicas que toman los usuarios para proteger su información.

Escala de exposición a ofensas - Exposure to Offence Scale (EOS)

Esta escala (EOS) tiene como objetivo medir la exposición que tienen los usuarios frente a cualquier amenaza de seguridad cibernética. Esta escala resalta la exposición a riesgos, amenazas e impactos, que son generados por comportamientos y ocurrencias de los usuarios.

Escala de percepción del riesgo - Risk Preception Scale (RPS)

La escala RPS mide el grado de riesgo o peligro, el cual es captado por un usuario que está utilizando las TI. Esta percepción está relacionada con el ámbito de la confianza que tiene un usuario frente a posibles ataques cibernéticos.

Capítulo III

Metodología

En este capítulo se explica la metodología utilizada para el desarrollo de nuestro estudio, la cual consta del diseño de la encuesta y estudio de la relación existente. Así, la encuesta se desarrolló, basándose en las escalas de comportamiento, exposición y percepción del riesgo (RBS, CBS, EOS y RPS), la cual será aplicada al personal de la Universidad de las Fuerzas Armadas ESPE Sede Santo Domingo. Además, esta sección se realiza el estudio de la relación existente entre la conciencia de los usuarios hacia la Seguridad de la Información, y a su vez, el comportamiento humano al usar las TI, adicionalmente se toma en cuenta a las variables principales, que serán las que definan la relación entre conciencia y comportamiento. En esta sección se plantean dos objetivos los cuales son:

1. Definir y evaluar los comportamientos, exposición y percepción de riesgo de los usuarios para determinar su nivel de conciencia en Seguridad de la información.
2. Analizar si existe una relación entre las percepciones, los comportamientos y exposiciones de los usuarios al usar las TI o Internet.

Para generalizar la conciencia de la Seguridad de la Información, el primer paso es medir la conciencia de los usuarios, aunque los usuarios siempre son conscientes de cualquier evento adverso, esto no define que cumplan correctamente con las medidas de seguridad, es por ello que también se debe examinar el comportamiento de los usuarios mientras utilizan las TI, ya que este comportamiento tiene una relación directa con la Seguridad de la Información. Otro punto a tomar en cuenta es el nivel de exposición al delito de los usuarios, debido a que esto puede influir en la relación entre la perspectiva del usuario y el comportamiento del riesgo. Para que las normas de Seguridad de la Información se establezcan de manera efectiva, es necesario

e importante detectar y medir los comportamientos, percepciones, valores y exposiciones de los usuarios ante factores que generen un impacto en los activos de TI.

Tipo de investigación

El tipo de investigación del presente trabajo de tesis es de tipo descriptivo y cuantitativo. Es descriptivo debido a que se pretende definir la actitud y el comportamiento de usuarios que utilizan o tiene relación con las TI, mediante la recolección de información con respecto a los conceptos de la Seguridad de la Información. Además de buscar y medir relaciones entre comportamientos, se pretende encontrar actitudes entre los grupos de docentes, administradores o militares y estudiantes.

Debido a los objetivos que se planteó previamente se miden las variables de forma independiente, luego se realizó un análisis de manera general agrupando cada variable en diferentes grupos, en este caso los grupos correspondientes a los docentes, administradores o militares, estudiantes y las escalas de comportamiento. Todo esto con el fin de poder encontrar una similitud entre usuarios, debido a su área de estudio, trabajo, o características que hacen que un usuario actúe diferente a otros.

El enfoque de la investigación es cuantitativo, ya que el análisis de los datos arrojados se encuentra presentados mediante mediciones numéricas y los resultados esperados se analizan de forma estadística. Este enfoque secuencial nos permite encontrar de manera particular un conocimiento del objeto de estudio.

Fuente de datos

Para definir y encontrar una relación entre la conciencia, el comportamiento y el conocimiento de los usuarios sobre la Seguridad de la Información, se realizó y compartió una encuesta, la cual hizo uso de cuatro escalas propuestas y definidas por (Öɬütçü et al., 2016a), las

cuales son: Escala de Comportamiento de Riesgo (RBS), Escala de Comportamiento Conservador (CBS), Escala de Exposición a Ofensas (EOS) y Escala de Percepción de Riesgo (EPS). Estas escalas con la ayuda de una evaluación estadística, permiten medir los diversos comportamientos, niveles de conciencia, valores y percepciones que los usuarios puedan tener sobre las TI o la Seguridad de la Información.

Planteamiento de la hipótesis

Una vez realizada la encuesta se espera obtener los datos necesarios para comprobar o negar las siguientes hipótesis:

- H1: No hay diferencia significativa entre las escalas {RBS, CBS, EOS, RPS}, con respecto a su promedio.
- H2: No hay diferencia significativa entre los grupos encuestados (docentes, administrativos, estudiantes) con respecto a su promedio.
- H3: La exposición a más horas/día que tienen los usuarios al usar el Internet, afecta el promedio de las escalas {RBS, CBS, EOS, RPS}.
- H4: Existe una correlación significativa entre los promedios de las escalas {RBS, CBS, EOS, RPS}.

Planteamiento del diseño de la investigación

Para el desarrollo de la encuesta se tuvieron en cuenta las preguntas planteadas por (Ö1ütçü et al., 2016a), donde se menciona que un grupo de expertos de la Asociación Turca de Seguridad especializados en Delitos Cibernéticos fueron quienes desarrollaron las preguntas para cada una de las escalas, además de verificar su validez y así presentar la encuesta a los docentes, administrativos y estudiantes de la Universidad de Turquía. Al ser una investigación desarrollada en el año 2015 está contenía preguntas que actualmente no tendrían relevancia,

así que para la actualización de la encuesta se tuvieron en cuenta conocimientos y conceptos sobre Seguridad Informática, Seguridad de la Información y de TI, además de contar con la ayuda de un grupo de investigación de Seguridad Cognitiva de la Universidad de las Fuerzas Armadas, quienes aportaron con sus comentarios y recomendaciones para que la encuesta no pierda su capacidad de obtener información relevante. Con la actualización de las preguntas de la encuesta se redujo la cantidad de preguntas por escala, con el objetivo de tener una encuesta más breve, comprensible y fácil de desarrollar para los grupos de usuarios encuestados. Además, se agregaron preguntas de manera que la encuesta este más relacionada a la actualidad y así poder obtener información relevante sobre los posibles comportamientos, exposición o percepción de riesgo que los usuarios puedan tener ante diversas situaciones de riesgo.

Selección de la muestra

Los encuestados del estudio han sido seleccionados como una muestra, la cual incluye a estudiantes, docentes, y personal administrativo y militares de la Universidad de las Fuerzas Armadas ESPE Sede Santo Domingo, la cual integran las carreras de Tecnologías de la Información, Biotecnología y Agropecuaria. La razón por la que selecciono esta muestra, es que debido a que la Universidad de ESPE desde el año 2017 inicio con sus carreras que emplean en de su malla el uso de TI, y gran parte del personal actual son “Nativos Digitales” entre las edades de 17 a 45 años. Los Nativos Digitales según (García et al., 2007), nacieron en la era digital, y utilizan permanentemente las tecnologías, tienen como característica principal la tecnófila, es decir, sienten atracción por todo lo que esté relacionado a nuevas tecnologías. Además, se tiene en cuenta que las Universidades han sido uno de los objetivos más frecuentes de ciberataque, debido a la gran cantidad de información pública y privada que manejan, estas han sufrido ataques informáticos con grandes impactos.

Tamaño de la muestra

Este estudio toma en cuenta los factores considerados en el manuscrito de (Ö1ütçü et al., 2016a), donde de manera similar se tomó el odd ratio de respuesta a algunas preguntas de la encuesta como 0,5 y suponiendo que se tiene una distribución heterogénea, el margen de error es de 0,08 y un intervalo de confianza del 95%, el tamaño mínimo de la muestra que se espera calcular es de 131 encuestados, el cual incluye los grupos de docentes, administrativos o militares y estudiantes. Los estratos para los docentes fueron los departamentos o áreas de estudio en los que trabajan, para los estudiantes fue la carrera que estudian y el nivel que están cursando actualmente y para los administrativos o militares su nivel de educación y el cargo o lugar de trabajo.

Las escalas propuestas para el diseño de la encuesta que será presentada a cada uno de los grupos e individuos ya sea docente, administrativo y estudiantes que conforman la Universidad de las Fuerzas Armadas ESPE Sede Santo Domingo. Para la evaluación y cálculo de resultados, las respuestas de las preguntas están desarrolladas en base a una escala de Likert, ya que (Boone et al., 2012) desarrolló un análisis y menciona que esta escala permite medir las actitudes, carácter y rasgos de personalidad, para convertir los datos cualitativos a datos cuantitativos con el fin de poder tabular y analizar los datos obtenidos. Para analizar correctamente los datos de la escala de Likert, en este caso para la medición de los datos se hará uso de los valores “Siempre” con 5 puntos, “Casi siempre” con 4 puntos, “A veces” con 3 puntos, “Casi nunca” con 2 puntos y “Nunca” con 1 punto; en los casos de las escalas RBS y CBS, para así poder medir el riesgo de los usuarios encuestados. La escala EOS permite medir que tan expuestos están los usuarios a ser víctimas de un ciberataque. La escala RPS cuenta con los intervalos “Demasiado Peligros” con 5 puntos, “Peligros” con 4 puntos, “Poco peligroso” con 3 puntos, “Seguro” con 2 puntos y “No tengo idea” con 1 punto. Aplicar los intervalos de tipo

Likert permite aplicar los métodos de análisis de datos ANOVA y la correlación de Pearson, para la interpretación de los resultados obtenidos como es mencionado por (Boone et al., 2012) al trabajar con escalas de datos.

Muestra seleccionada para la investigación

La encuesta fue enviada a todas las personas que conforman parte de la Universidad de las Fuerzas Armadas ESPE por medio del correo institucional. La Universidad ESPE se caracteriza en ser una universidad líder en la gestión del conocimiento y de la tecnología en el Sistema de Educación Superior del país. Se puede comprobar el listado del personal que completo la encuesta en los resultados de las Tablas 11, 12 y 13.

Del total de las encuestas enviadas a la universidad se logró recolectar 168 respuestas, luego, de estas respuestas que fueron analizadas se eliminaron 15 por no estar completadas en el tiempo establecido para el análisis. Esta acción redujo el número de respuestas a 153 validas de las encuestas enviadas.

Recolección de datos

Para realizar esta recolección, fue diseñada la encuesta con sus respectivas preguntas, en un formulario de Google Forms. Para la recolección de datos cuantitativos, las preguntas fueron respondidas por docentes, administradores, o estudiantes de la Universidad de las Fuerzas Armadas ESPE. Con el fin de analizar el conocimiento y comportamiento de los grupos de usuarios, se determinaron los elementos claves para medir la capacidad de las personas de actuar ante ataques de Ingeniería Social.

Las preguntas de la encuesta están conformadas por ocho secciones, lo que nos ayuda a poder clasificar a todos los grupos de personas a evaluar, además de encontrar las relaciones

entre las escalas de comportamiento de los usuarios. Las preguntas de la encuesta están seccionadas de la siguiente manera:

- Perfil de Usuario;
- Sección para docentes;
- Sección para estudiantes;
- Sección para Administrativos y Militares;
- Escala de Comportamiento de Riesgo (RPS);
- Escala Comportamiento Conservador (CBS);
- Escala de Exposición a delitos (EOS);
- Escala de Percepción del Riesgo (RPS).

Perfiles de Usuario

En la Tabla 2 se presentan las preguntas de la sección perfil de usuario. Estas permiten recolectar información que ayudó a seccionar rangos y verificar si existe una relación entre el usuario y las escalas. Las preguntas que se resaltan en esta sección son, si un usuario tiene experiencia en seguridad en Internet, ocupación y tiempo medio de uso de Internet. Las preguntas de la sección perfiles de usuario son:

Tabla 2

Preguntas para recolectar información de los usuarios encuestados

Preguntas	**Opciones**				
Seleccione su rango de edad	15-24 años	25-34 años	35-44 años	45-54 años	55 años en adelante

Preguntas	Opciones				
Seleccione su género	Masculino	Femenino	-	-	-
Elija su provincia de residencia	-	-	-	-	-
¿Alguna vez ha tenido formación o experiencia en Seguridad en Internet?	Si	No	-	-	-
Tiempo medio de uso de Internet	1-5 horas/día	1-5 horas/día	1-5 horas/día	-	-
Escoja su ocupación	Estudiante	Docente	Administrativo	-	-

Sección para Docentes

La segunda sección contiene preguntas únicamente para el grupo de docentes que labora en la Universidad ESPE, estas preguntas se presentan en la Tabla 3, las cuales permiten identificar el nivel académico, el acceso y uso del Internet de los docentes. Este grupo de preguntas ayudó a encontrar y verificar si existe una relación entre grupos, y si ser docente influye en el comportamiento o percepción de riesgos al usar las TI.

Tabla 3

Preguntas para recolectar información de los Docentes encuestados

Preguntas	Opciones		
Nivel de educación	Tercer Nivel	Cuarto Nivel	-

Preguntas	Opciones		
Escoja el departamento, área de estudio o de trabajo al que pertenece.	-	-	-
¿Cómo accede a Internet desde fuera de su lugar de trabajo? (Puede marcar más de uno).	Usando datos Móviles	Red Wifi publica (Centros comerciales, Parques)	Red Wifi privada (Domicilio)

Sección para Estudiantes

En la Tabla 4 se presenta la sección de las preguntas que van dirigidas únicamente para los estudiantes de la Universidad ESPE. El objetivo es saber en qué departamento realizan sus estudios, el nivel en el que están actualmente y como acceden a Internet. Estas preguntas permiten establecer si existe una relación entre grupos y verificar si ser estudiante influye en el comportamiento o percepción del riesgo al usar las TI.

Tabla 4

Preguntas para recolectar información de los Estudiantes encuestados

Preguntas	Opciones		
Escoja su departamento o área de estudio	-	-	-
Nivel cursado	-	-	-
¿Cómo accede a Internet desde fuera de su lugar de trabajo? (Puede marcar más de uno).	Usando datos Móviles	Red Wifi publica (Centros	Red Wifi privada (Domicilio)

Preguntas	Opciones
	comerciales, Parques)

Sección para personal Administrativo

En la Tabla 5 se presentan las preguntas que están realizadas para que responda el personal administrativo y militar que labora en la Universidad ESPE. El objetivo es saber el cargo que ocupa, nivel de estudios y como acceden a Internet. Estas preguntas permiten establecer si existe una relación entre grupos y verificar si el cargo del personal administrativo influye en el comportamiento o percepción del riesgo al usar las TI.

Tabla 5

Preguntas para recolectar información del personal Administrativo y militar

Preguntas	Opciones			
Ingrese su cargo dentro de la Institución	-	-	-	-
Nivel de educación	Primer Nivel	Segundo Nivel	Tercer Nivel	Cuarto Nivel
¿Cómo accede a Internet desde fuera de su lugar de trabajo? (Puede marcar más de uno).	Usando datos Móviles	Red Wifi publica (Centros comerciales, Parques)	Red Wifi privada (Domicilio)	-

Escala de Comportamiento de Riesgo (RBS)

La escala RBS permite medir el riesgo que pueden tener los usuarios con respecto a sus comportamientos al hacer uso de las TI o casos en los que su información se encuentre comprometida al realizar acciones comunes en las que pueda haber una cierta vulnerabilidad de su información. Las conductas de riesgo de los usuarios al hacer uso de los dispositivos de TI según (Milne et al., 2009), se definen como un conjunto de acciones específicas que desarrollan los usuarios al hacer uso de dispositivos de TI en las que ellos mismo se ponen en riesgo. Los comportamientos más comunes de los usuarios son: hacer uso de redes sociales, de páginas en línea en las que saben que tendrán que compartir su información personal, compartir archivos confidenciales haciendo uso de plataformas en línea o hacer uso de redes Wifi sin contraseña en lugares públicos, de manera tal que ponen su información en peligro, corriendo el riesgo de que esta sea usada para fines delictivos o ser víctimas de un ciberataque, por lo que en esta escala se definen preguntas que permitan identificar los diversos comportamientos de riesgo que puedan tener los usuarios al hacer uso de Internet.

En la Tabla 6 se presenta la sección de preguntas con las que se mide el comportamiento y conductas que tienen las personas ante un riesgo mientras utilizan las TI. Estas conductas de riesgo son las que pueden generar que un usuario este expuesto a posibles ataques de Ingeniería Social, es por ello que con estas preguntas se pudo comprobar si el comportamiento de riesgo de un usuario tiene relación o influye en las otras escalas de comportamiento.

Tabla 6

Escala de Comportamiento de Riesgo (RBS)

Preguntas
¿Usted usa WhatsApp, Telegram, Messenger o programas de chat similares?
¿Usted usa Meet, Teams, Zoom o programas de reuniones similares?
¿Usted utiliza el correo electrónico?
¿Usted utiliza su dirección de correo electrónico Corporativo o Institucional para sus negocios personales?
¿Usted ingresa a links para postulaciones (estudio, trabajo, etc.) enviadas en redes sociales?
¿Usted usa la banca en línea?
¿Usted hace compras o pagos en Internet?
¿Usted utiliza sitios web que brindan servicios a la ciudadanía de manera electrónica (consultar de número de identidad, pago de servicios básicos, etc.)?
¿Usted juega video juegos en línea?
¿Usted ve videos o películas en línea?
¿Usted comparte su información personal en Internet cuando es necesario (nombre, apellido, fecha de nacimiento, correo electrónico, dirección, etc.)?
¿Usted transfiere archivos confidenciales en WhatsApp, Telegram o Messenger?
¿Usted utiliza la banca en línea en lugares donde hay acceso a Internet público?
¿Usted comparte sus contraseñas con otras personas?
¿Usted guarda sus contraseñas escribiéndolas en agendas o lugares que se pueden encontrar fácilmente?
¿Usted abre correos electrónicos de extraños o descarga los archivos adjuntos de esos correos?

Escala de Comportamiento Conservador (CBS)

Con la escala CBS, se mide que tan prudentes, reservados o conservadores pueden ser los usuarios al hacer uso de las TI o de los Sistemas de Información que manejen. Según (Öɪütçü et al., 2016a), esta escala es paralela a los comportamientos protectores por (Milne et al., 2009)

y a los comportamientos de seguridad de protección por (Ng et al., 2008), mencionando que los usuarios se basan en acciones que consideran que mantendrán segura su información y tener comportamientos que minimicen los riesgos o impactos que se tengan al encontrarse en situaciones en las que su información pueda estar comprometida. La escala CBS ayudo a identificar los comportamientos conservadores que tienen los usuarios al hacer uso de los dispositivos de TI o de Internet.

En esta sección de la encuesta se mide el actuar que los usuarios cuando está usando las TI, estas conductas conservadoras son las que pueden generar que un usuario evite posibles ataques de Ingeniería Social, es por ello que con estas preguntas se pudo comprobar si el comportamiento conservador de un usuario tiene relación o influye en las otras escalas de comportamiento.

Tabla 7

Escala de Comportamiento Conservador (CBS)

Preguntas
¿Usted usa software original con licencia en su computadora?
¿Usted utiliza programas como detección de virus, software espía, etc?
¿Usted elimina los archivos temporales de Internet y el historial de Internet antes de dejar un ordenador?
¿Usted utiliza contraseñas largas y complicadas que no se pueden adivinar fácilmente para sus cuentas en Internet y archivos personales?
¿Usted usa firma electrónica?
¿Usted tiene contraseña para acceder a su computadora?
¿Usted presta atención a los sitios web que visita, verificando si estos tienen el candado de HTTPS en la barra de dirección?
¿Usted a menudo cambia sus contraseñas?

Preguntas
¿Está usted consciente de que su información personal puede ser utilizada por otras personas de forma ilegal?

Escala de Exposición a ofensas (EOS)

La escala EOS, mide el nivel de exposición a incidentes que los usuarios puedan tener al hacer uso de los dispositivos de TI o de Internet, lo que permite evaluar, analizar e identificar ante que riesgos o amenazas han estado expuestos los usuarios y en los que su información ya sea personal u organizacional se ha visto comprometida. La base de las preguntas de esta escala se enfoca a si los usuarios han sido víctimas ante los diversos ataques de Ingeniería Social, obteniendo información sobre las posibles vulnerabilidades que los usuarios puedan presentar para encontrarse expuestos.

En esta sección se mide la exposición de los usuarios cuando se enfrentan a cualquier incidente de seguridad a causa de sus comportamientos, estas conductas son las que pueden generar un impacto negativo dentro de una organización, es por ello que con estas preguntas se pudo comprobar si la exposición a delitos de un usuario tiene relación o influye en las otras escalas de comportamiento.

Tabla 8

Escala de Exposición a Ofensas (EOS)

Preguntas
¿Usted ha tenido problemas debido a virus informáticos?
¿Usted ha experimentado pérdidas económicas como resultado de las compras en línea?
¿Usted ha tenido problemas por compartir su información personal en Internet?

Preguntas
¿Ha recibido usted alguna notificación de uso de su usuario y contraseña en Internet, sin su autorización?
¿Los archivos en su computadora han sido robados o eliminados en alguna ocasión?
¿Ha encontrado cuentas falsas que usen sus datos confidenciales o su perfil de usuario?
¿Usted utiliza alguna entidad que preserve los datos de su tarjeta de crédito en las compras en línea, como por ejemplo PayPal?

Escala de Percepción de Riesgos (RPS)

Por último, la escala RPS mide el grado de riesgo o peligro que el usuario percibe al usar las TI o un Sistema de Información. Estas preguntas permiten obtener información sobre como los usuarios asimilan temas relacionados con la Seguridad de la Información, permitiendo evaluar la capacidad que los usuarios tienen para evitar ser víctimas de Ingeniera Social. La percepción del riesgo del usuario está relacionada con el concepto abstracto y complejo de confianza (Horst et al., 2007), siento la confianza una característica a tener en cuenta en los usuarios que son vulnerables a ataques informáticos.

En esta sección las preguntas son formuladas para medir el grado de peligro que un usuario logra captar con una TI, es por ello que con estas preguntas se pudo comprobar si la percepción de riesgos de un usuario tiene relación o influye en las otras escalas de comportamiento.

Tabla 9

Escala de Percepción de Riesgos (RPS)

Preguntas
Virus informático
Carecer de Antivirus

Preguntas
Programas espías (Keylogger, Screenlogger, Trojan, etc.)
Programas de intercambio de archivos (Google Drive, Dropbox, Mega, etc.)
Programas de chat (WhatsApp, Telegram, Messenger.)
Correo electrónico no deseado, spam o correo basura
Juegos en línea
USB o Memorias externas.
Macros en aplicaciones de Microsoft Office (Word, Excel, etc.)
Uso de programas pirateados
Descarga de materiales como música, fotos o películas sin pagar nada.
Abrir correos electrónicos con contenido publicitario
Uso de banca en línea.
Compartir información con extraños en línea.
Compras en línea.
Uso de Wifi inalámbrico
Descarga y uso de programas gratuitos o sin licencia
Entrega de número de cédula de identidad o de carnet de conducir al personal de seguridad de la entrada de un edificio

Periodo de recolección de datos

La investigación se realizó mediante la divulgación de la encuesta por Google Forms, la cual tuvo una fase de obtención de los datos, la que tuvo una duración de 3 semanas. En este tiempo se monitorearon las respuestas de las personas que iban completando la encuesta, la cual tenía una duración para completar de aproximadamente 10 minutos.

Análisis de datos

El análisis de los datos se lo realizó una vez obtenidos los datos de la encuesta. Para ello, fue necesario analizar y comprender los valores obtenidos en cada variable, indicando si estos datos obtenidos cumplen con los objetivos planteados. Estos datos se analizan con la finalidad

de contestar las hipótesis propuestas. Para el análisis de estos datos, se utilizó el programa Microsoft Excel 2016 y su complemento XREALSTATS, que permitió desarrollar los análisis de varianza (ANOVA) y las pruebas Tukey.

Capítulo IV

Resultados y Discusión

Este capítulo consta de cuatro partes; la primera parte analiza los resultados obtenidos de los perfiles de los usuarios de sección docente, sección administrativos o militares y sección estudiantes; la segunda parte presenta los datos del análisis de ANOVA y la diferencia significativa entre las escalas de comportamiento (RBS, CBS, EOS, RPS), y grupos (Docentes, Administradores o Militares y Estudiantes); la tercera parte consta del análisis de los datos de la tiempo de uso de Internet en los grupos de encuestados.

Resultados de los datos demográficos

Una vez obtenidos los datos de la encuesta, se empezó a realizar la verificación y revisión de los datos de los encuestados. Se puede observar en la Tabla 10 Resultados de las preguntas de la sección Perfil de Usuario, que la mayor parte de las personas que llenaron la encuesta están en el rango de edad de 15-24 años, los que corresponde a un 76% del total, los encuestados con mayor representación en las muestras validas corresponden al género masculino con 101 (66%) encuestados a comparación de 52 (34%) del género femenino. Un dato importante a resaltar es que la mayor parte de encuestados residen en la provincia de Santo Domingo de los Tsáchilas con 117 encuestados correspondiente al 76%, seguido de la provincia de Pichincha con 19 encuestados correspondiente al 12%. El mayor tiempo medio de uso de Internet corresponde a 6-10 horas/día (49%) seguido de 11 horas o más/días con 69 (45%) encuestados y 1-5 horas/días con 9 (6%) encuestados.

Tabla 10

Resultados de las preguntas de la sección Perfil de Usuario

Preguntas	Opciones				
Seleccione su rango de edad	15-24 años 117 76%	25-34 años 15 10%	35-44 años 9 6%	45-54 años 9 6%	55 años en adelante 3 2%
Seleccione su género	Masculino 101 66%	Femenino 52 34%	-	-	-
¿Alguna vez ha tenido formación o experiencia en Seguridad en Internet?	Si 65 42%	No 88 58%	-	-	-
Tiempo medio de uso de Internet	1-5 horas/día 9 6%	6-10 horas/día 75 49%	11 o más horas/día 69 45%	-	-
Escoja su ocupación	Estudiante 128 84%	Docente 18 12%	Administrativo 7 4%	-	-

En base a los resultados presentados en la Tabla 10 de la sección Perfil de Usuarios podemos concluir que, el mayor número de personas que respondieron la encuesta reside en las provincias de Santo Domingo y Pichincha, el grupo con mayor cantidad de respuestas corresponde al grupo de estudiantes, el tiempo medio de uso de Internet está entre las 6 a 10 horas al día.

Resultados de los grupos Docentes, Administrativo y Estudiantes

En las tablas 11, 12 y 13 se presentan los resultados que corresponden a los grupos de Estudiantes con 128 (84%) encuestas validas, seguido de los Docentes con 18 (12%) encuestados y con la menor cantidad, el grupo correspondiente a Administrativo con 7 (4%) encuestados.

Tabla 11

Resultados de las preguntas de la sección Docentes

Preguntas		**Opciones**	
Nivel de educación	Tercer Nivel 18	Cuarto Nivel	-
Escoja el departamento, área de estudio o de trabajo al que pertenece.	-	-	-
¿Cómo accede a Internet desde fuera de su lugar de trabajo? (Puede marcar más de uno).	Usando datos Móviles	Red Wifi publica (Centros comerciales, Parques)	Red Wifi privada (Domicilio)

Tabla 12

Resultados de las preguntas de la sección Estudiantes

Preguntas			**Opciones**		
Escoja su departamento o área de estudio	Ciencias de la Computación 110	Ciencias Exactas 3	Ciencias de la Vida y la Agricultura 9	Eléctrica, Electrónica y Telecomunicaciones 2	Otro 4
Nivel cursado	Quinto Nivel 24	Sexto Nivel 18	Séptimo Nivel 8	-	-

Preguntas	Opciones				
¿Cómo accede a Internet desde fuera de su lugar de trabajo? (Puede marcar más de uno).	Usando datos Móviles	Red Wifi publica (Centros comerciales, Parques)	Red Wifi privada (Domicilio)	-	-

Tabla 13

Resultados de las preguntas de la sección Administrativos y militares

Preguntas	Opciones				
Ingrese su cargo dentro de la Institución	-	-	-	-	-
Nivel de educación	Primer Nivel	Segundo Nivel 1	Tercer Nivel 5	Cuarto Nivel 1	-
¿Cómo accede a Internet desde fuera de su lugar de trabajo? (Puede marcar más de uno).	Usando datos Móviles	Red Wifi publica (Centros comerciales, Parques)	Red Wifi privada (Domicilio)	-	-

Al haber obtenido los resultados de las tablas de los grupos encuestados podemos concluir que el grupo de los Estudiantes con mayor cantidad de respuestas validas, se encuentran realizando sus estudios en el área de Ciencias de la Computación, lo que significa que el 39,06% de los estudiantes encuestados tienen conocimientos sobre la Seguridad de la

Información al encontrarse en niveles en los que materias como Seguridad en TI, Gestión de la Seguridad son impartidas.

Resultados de las escalas (RBS, CBS, EOS, RPS)

A continuación, se muestran los resultados obtenidos de la encuesta aplicada por cada una de las escalas: RBS en la Tabla 14, CBS en la Tabla 15, EOS en la Tabla 16 y RPS en la Tabla 17.

Tabla 14

Resultados de las preguntas de la Escala de Comportamiento de Riesgo (RBS)

Preguntas	Siempre	Casi siempre	A veces	Casi nunca	Nunca	Siempre
¿Usted usa WhatsApp, Telegram, Messenger o programas de chat similares?	105 69%	37 24%	11 7%	0	0	
¿Usted usa Meet, Teams, Zoom o programas de reuniones similares?	105 69%	35 23%	10 6%	2 1%	1 1%	
¿Usted utiliza el correo electrónico?	91 59%	35 23%	24 16%	3 2%	0	

Preguntas	Siempre	Casi siempre	A veces	Casi nunca	Nunca	Siempre
¿Usted utiliza su dirección de correo electrónico Corporativo o Institucional para sus negocios personales?	25 15%	13 8%	21 14%	22 14%	72 47%	
¿Usted ingresa a links para postulaciones (estudio, trabajo, etc.) enviadas en redes sociales?	11 7%	25 16%	53 35%	34 22%	30 20%	
¿Usted usa la banca en línea?	34 22%	30 20%	35 23%	14 9%	40 26%	
¿Usted hace compras o pagos en Internet?	8 5%	22 15%	48 31%	23 15%	52 34%	
¿Usted utiliza sitios web que brindan servicios a la ciudadanía de manera electrónica (consultar de número de	16 11%	28 18%	57 37%	34 22%	18 12%	

Preguntas	Siempre	Casi siempre	A veces	Casi nunca	Nunca	Siempre
identidad, pago de servicios básicos, etc.)?						
¿Usted juega video juegos en línea?	25 16%	28 18%	32 21%	35 23%	33 22%	
¿Usted ve videos o películas en línea?	45 29%	36 24%	47 32%	17 11%	8 5%	
¿Usted comparte su información personal en Internet cuando es necesario (nombre, apellido, fecha de nacimiento, correo electrónico, dirección, etc.)?	11 7%	34 22%	65 42%	31 20%	12 8%	
¿Usted transfiere archivos confidenciales en WhatsApp, Telegram o Messenger?	14 9%	29 19%	39 25%	34 22%	37 24%	
¿Usted utiliza la banca en línea en	2 1%	4 3%	16 10%	27 18%	104 68%	

Preguntas	Siempre	Casi siempre	A veces	Casi nunca	Nunca	Siempre
lugares donde hay acceso a Internet público?						
¿Usted comparte sus contraseñas con otras personas?	1 1%	3 2%	19 12%	54 35%	76 50%	
¿Usted guarda sus contraseñas escribiéndolas en agendas o lugares que se pueden encontrar fácilmente?	7 5%	14 9%	28 18%	40 26%	64 42%	
¿Usted abre correos electrónicos de extraños o descarga los archivos adjuntos de esos correos?	1 1%	5 3%	12 8%	38 25%	97 63%	

Tabla 15

Resultados de las preguntas de la Escala de Comportamiento Conservador (CBS)

Preguntas	Siempre	Casi siempre	A veces	Casi nunca	Nunca
¿Usted usa software original con licencia en su computadora?	42 28%	31 20%	31 20%	28 18%	21 14%
¿Usted utiliza programas como detección de virus, software espía, etc?	47 31%	35 23%	34 22%	24 16%	13 8%
¿Usted elimina los archivos temporales de Internet y el historial de Internet antes de dejar un ordenador?	37 24%	23 15%	40 26%	36 24%	17 11%
¿Usted utiliza contraseñas largas y complicadas que no se pueden adivinar fácilmente para sus cuentas en	47 31%	52 34%	38 25%	10 6%	6 4%

Preguntas	Siempre	Casi siempre	A veces	Casi nunca	Nunca
Internet y archivos personales?					
¿Usted usa firma electrónica?	14 9%	13 9%	20 13%	28 18%	78 51%
¿Usted tiene contraseña para acceder a su computadora?	Si 107 70%	No 46 30%	-	-	-
¿Usted presta atención a los sitios web que visita, verificando si estos tienen el candado de HTTPS en la barra de dirección?	50 33%	32 21%	36 23%	24 16%	11 7%
¿Usted a menudo cambia sus contraseñas?	Cada semana 2 1%	Cada mes 13 8%	Cada 6 meses 66 43%	Casi nunca 62 41%	Nunca 10 7%
¿Está usted consciente de que su información personal puede ser utilizada por otras	Si 137 90%	No 10 6%	No lo sé 6 4%	-	-

Preguntas	Siempre	Casi siempre	A veces	Casi nunca	Nunca
personas de forma ilegal?					

Tabla 16

Resultados de las preguntas de la Escala de Exposición a Ofensas (EOS)

Preguntas	Siempre	Casi siempre	A veces	Casi nunca	Nunca
¿Usted ha tenido problemas debido a virus informáticos?	1 1%	8 5%	33 21%	73 48%	38 25%
¿Usted ha experimentado pérdidas económicas como resultado de las compras en línea?	Si 20 13%	No 121 79%	No lo sé 12 8%	-	-
¿Usted ha tenido problemas por compartir su información personal en Internet?	Si 20 13%	No 114 75%	No lo sé 19 12%	-	-

Preguntas	Siempre	Casi siempre	A veces	Casi nunca	Nunca
¿Ha recibido usted alguna notificación de uso de su usuario y contraseña en Internet, sin su autorización?	Si 28%	No 98 64%	No lo sé 12 8%	-	-
¿Los archivos en su computadora han sido robados o eliminados en alguna ocasión?	Si 9 6%	No 128 84%	No lo sé 16 10&	-	-
¿Ha encontrado cuentas falsas que usen sus datos confidenciales o su perfil de usuario?	Si 23 15%	No 112 73%	No lo sé 18 12%	-	-
¿Usted utiliza alguna entidad que preserve los datos de su tarjeta de crédito en las compras en línea, como por ejemplo PayPal?	Si 44 29%	No 96 63%	No lo sé 13 8%	-	-

Tabla 17

Resultados de las preguntas de la Escala de Percepción del Riesgo (RPS)

Ítems	Muy peligroso	Peligroso	Poco peligroso	Seguro	No tengo idea
Virus informático	93 61%	51 33%	5 3%	1 1%	3 2%
Carecer de Antivirus	50 33%	67 44%	22 14%	12 8%	2 1%
Programas espías (Keylogger, Screenlogger, Trojan, etc.)	79 51%	46 30%	12 8%	1 1%	15 10%
Programas de intercambio de archivos (Google Drive, Dropbox, Mega, etc.)	5 3%	25 16%	74 49%	43 28%	6 4%
Programas de chat (WhatsApp, Telegram, Messenger.)	11 7%	41 27%	76 50%	20 13%	5 3%
Correo electrónico no deseado, spam o correo basura	36 23%	64 42%	41 27%	4 3%	8 5%

Ítems	Muy peligroso	Peligroso	Poco peligroso	Seguro	No tengo idea
Juegos en línea	17 11%	31 20%	72 47%	21 14%	12 8%
USB o Memorias externas.	28 18%	45 30%	66 43%	9 6%	5 3%
Macros en aplicaciones de Microsoft Office (Word, Excel, etc.)	6 4%	15 10%	56 36%	49 32%	27 18%
Uso de programas pirateados	48 31%	69 45%	29 19%	1 1%	6 4%
Descarga de materiales como música, fotos o películas sin pagar nada.	17 11%	71 47%	54 35%	3 2%	8 5%
Abrir correos electrónicos con contenido publicitario	36 23%	67 44%	40 26%	4 3%	6 4%
Uso de banca en línea.	12 8%	34 22%	64 42%	27 18%	16 10%

Ítems	Muy peligroso	Peligroso	Poco peligroso	Seguro	No tengo idea
Compartir información con extraños en línea.	104 68%	36 23%	9 6%	1 1%	3 2%
Compras en línea.	17 11%	55 36%	66 43%	7 5%	8 5%
Uso de Wifi inalámbrico	4 3%	34 22%	74 48%	27 18%	14 9%
Descarga y uso de programas gratuitos o sin licencia	20 13%	69 45%	54 35%	1 1%	9 6%
Entrega de número de cédula de identidad o de carnet de conducir al personal de seguridad de la entrada de un edificio	20 13%	38 25%	61 40%	20 13%	14 9%

Uno de los hallazgos más importantes que se pudo encontrar, es la relación que existe entre las escalas de comportamiento.

En la Tabla 18 podemos visualizar que la media de la escala RBS = 2,87091, la media de la escala CBS= 2,71604, la media correspondiente de la escala EOS= 1,94864 y para la escala RPS= 3,53703. Con lo que podemos concluir que, con el promedio obtenido en la escala RBS y CBS los grupos encuestados tienen cierta conciencia ante situaciones de riesgo, en el caso de la escala EOS los grupos encuestados tienen poca exposición a situaciones de riesgo, y en base al promedio de la escala RPS, los encuestados tienen conocimientos sobre el peligro que conlleva usar servicios en Internet, dispositivos de TI, entre otros.

Tabla 18

Promedio de las respuestas de las escalas (RBS, CBS, EOS, RPS)

Escala	Número de preguntas	Promedio
RBS	16	2,87091503
CBS	9	2,71604938
EOS	7	1,94864613
RPS	18	3,53703704

Prueba de Hipótesis

Prueba de H1: No hay diferencia significativa entre las escalas {RBS, CBS, EOS, RPS} con respecto a su promedio.

Para probar H1 se hizo uso del análisis de varianza o ANOVA, el cual permite identificar la diferencia significativa de los resultados obtenidos en la encuesta desarrollada, con lo que se puede aceptar o rechaza la hipótesis propuesta. Para desarrollar el análisis ANOVA entre las escalas {RBS, CBS, EOS, RPS}, se hizo uso de un $\alpha = 0.05$, de manera que si el valor de P menor al α, se rechaza la H1 y se demostrará que existe una diferencia significativa entre las escalas. La

Tabla 19 muestra los valores obtenidos al realizar el ANOVA entre cada una de las escalas de comportamiento.

Tabla 19

Cálculo ANOVA entre las escalas {RBS, CBS, EOS, RPS}

Origen de las variaciones	SS	DF	MS	F	P
Entre grupos	13,81396474	3	4,604654914	7,397832118	0,000
Dentro de grupos	28,63191847	46	0,62243301		
Total	42,44588321	49	0,866242514		

Donde SS = Suma de cuadrados; DF = Grados de libertad; MS = Promedio de los cuadrados; F = Error; P = Probabilidad

Analizando la Tabla 19, se puede observar que existe una diferencia significativa entre las escalas analizadas con ANOVA, razón por la que para identificar cual escala es el que genera la diferencia, se hace necesario complementar el estudio, mediante el desarrollo de una prueba de Tukey. En la Tabla 20 se presentan la descripción de las escalas que son comparadas para identificar entre cuales se crea la diferencia.

Tabla 20

Descripción general de las escalas (RBS, CBS, EOS, RPS)

Grupos	media	n	SS	df	q-cirt
RBS	2,87091	16	15,09825		0,000
CBS	2,71604	9	8,018720		
EOS	1,94864	7	0,077955		
RPS	3,53703	18	5,436990		
		50	28,63191	46	3,769869

Con la comparación de las escalas en la prueba Tukey, se pueden observar los intervalos en que existe una diferencia significativa, ya que se comparan todas las escalas, y se puede observar de manera más precisa donde existe la diferencia, de manera que se logre determinar las escalas donde existe un valor menor a α=alfa, como se presentan los datos obtenidos en la Tabla 21.

Tabla 21

Resultados de la prueba de Tukey entre las escalas (RBS, CBS, EOS, RPS)

Grupo 1	Grupo 2	media	std err	p-value
RBS	CBS	0,15486	0,232444	0,965
RBS	EOS	0,922268	0,252805	0,061
RBS	RPS	0,666122	0,191678	0,080
CBS	EOS	0,767403	0,281138	0,229
CBS	RPS	0,820987	0,227748	0,065
EOS	RPS	1,588390	0,24849	0,000

Los resultados obtenidos para probar H1, demuestran que existe una diferencia significativa entre las escalas EOS y RPS, rechazando H1, y se acepta que hay una diferencia significativa entre las escalas propuestas, con lo que podemos concluir que la escala RPS influye de manera positiva sobre los grupos encuestados. En conclusión, al tener una mejor percepción del riesgo, los usuarios estarán menos expuestos a ataques de Ingeniería Social.

Prueba de H2: No hay diferencia significativa entre los grupos encuestados (docentes, administrativos o militares, estudiantes) con respecto a su promedio.

Para probar H2, la diferencia significativa entre los grupos encuestados (docentes, administrativos o militares, estudiantes), se desarrolla el análisis ANOVA entre los grupos y las

escalas propuestas, haciendo uso de un α = 0,05, de tal manera que si existe una diferencia significativa entre los grupos encuestados, el valor de la probabilidad deberá ser menor a α y en el caso de existir dicha diferencia rechazaremos la hipótesis nula y aceptaremos que no todas las medias de los grupos encuestados son iguales. El análisis de los grupos encuestados y las escalas propuestas se presenta en la Tabla 22.

Tabla 22

ANOVA entre los grupos Docente, Estudiante, Administrativo y Militar

Escalas		**SS**	**df**	**MS**	**F**	**P**
Escala de Comportamiento de riesgo	Entre Grupos	0,11266	2	0,056330	0,232678	0,792
	Dentro de Grupos	36,3144	150	0,242096	-	-
	Total	36,4271	152	0,239652	-	-
Escala de Comportamiento Conservador	Entre Grupos	2,526840	2	1,263420	5,608321	0,004
	Dentro de Grupos	33,79140	150	0,225276	-	-
	Total	36,31824	152	0,238935	-	-
Escala de Exposición a Ofensas	Entre Grupos	0,083294	2	0,041647	0,690758	0,502
	Dentro de Grupos	9,043822	150	0,060292	-	-
	Total	9,127117	152	0,060046	-	-
Escala de Percepción de Riesgo	Entre Grupos	1,829963	2	0,914981	3,946024	0,021
	Dentro de Grupos	34,78114	150	0,231874	-	-
	Total	36,61111	152	0,240862	-	-

En la Tabla 22, de acuerdo a las diferencias encontradas, se determinó que el grupo de docentes tiene diferencias con el grupo del personal administrativo y con el grupo de los estudiantes, en cuanto a los resultados obtenidos. Al ser el valor de P=0,004 en el caso de la

escala CBS y con un valor de P=0,021 en el caso de la escala RPS, como se presenta en la Tabla 22, se demuestra que existe una diferencia significativa entre los grupos encuestados. Para encontrar los grupos que generan esta diferencia se recurrió a la prueba Tukey entre las escalas y los grupos para identificar donde se genera esta diferencia, encontrando que el grupo de los encuestados que genera la diferencia en la escala CBS como se presenta en la Tabla 23 y en la Tabla 24 en el caso de la escala RPS es el grupo de los docentes.

Tabla 23

Resultados de la prueba de Tukey entre los grupos (Docentes, Administrativo y Estudiantes) y la escala (CBS)

Grupo 1	Grupo 2	media	std err	p-value
Docente	Admin	0,38536	0,14949	0,165
Docente	Estudiante	0,39949	0,08448	0,002
Admin	Estudiante	0,01413	0,13027	0,996

Tabla 24

Resultados de la prueba de Tukey entre los grupos (Docentes, Administrativo y Estudiantes) y la escala (RPS)

Grupo 1	Grupo 2	media	std err	p-value
Docente	Admin	0,01278	0,151668	0,998
Docente	Estudiante	0,29214	0,085712	0,044
Admin	Estudiante	0,30493	0,132167	0,235

Para concluir, se puede observar que existe diferencia significativa en la media obtenida (de 1 al 5) entre estos grupos encuestados. Así, en la escala CBS, los docentes tienen un comportamiento más conservador al encontrarse en situaciones de riesgo, pues cuentan con

una media = 3,067. En el caso de la escala RPS, los docentes obtuvieron una media = 3,780, indicando que ellos tienen una mejor percepción del riesgo, al hacer uso de Internet o de dispositivos de TI, en comparación a los demás grupos encuestados. Vale resaltar que en el estudio realizado por (Öɬütçü et al., 2016a) se encontró que el estudiante era el que generaba la diferencia significativa entre los grupos encuestados.

Prueba de H3: La exposición de horas/día que tienen los usuarios al usar el Internet afecta el promedio de las escalas {RBS, CBS, EOS, RPS}.

En el caso de H3, se agruparon los datos de acuerdo a las horas/día de uso de Internet de los usuarios encuestados. Para el desarrollo del análisis ANOVA, se tuvo en cuenta el α= 0,05, para verificar si existe una diferencia significativa entre los usuarios encuestados de acuerdo al tiempo de uso de Internet. El análisis ANOVA que se presenta en la Tabla 25, demuestra que sí existe una diferencia significativa entre el tiempo de uso de Internet de los encuestados, por esta razón se rechaza H3 y se acepta que el tiempo de uso de Internet de los usuarios encuestados, afecta al promedio de las escalas propuestas. En la Tabla 25, se identifica que existe una diferencia significativa en el caso de la escala RBS con un valor de P= 0,003.

Tabla 25

ANOVA del Tiempo medio de uso de Internet entre los grupos Docente, Estudiante, Administrativo y Militar

Escalas		SS	df	MS	F	P
Escala de Comportamiento de riesgo	Entre Grupos	2,67715	2	1,33857	5,94923	0,003
	Dentro de Grupos	33,7499	150	0,22499	-	-
	Total	36,4271	152	0,23965	-	-

Escalas		SS	df	MS	F	P
Escala de Comportamiento Conservador	Entre Grupos	0,11809	2	0,05904	0,24467	0,783
	Dentro de Grupos	36,2001	150	0,24133	-	-
	Total	36,3182	152	0,23893	-	-
Escala de Exposición a Ofensas	Entre Grupos	0,10191	2	0,05095	0,84691	0,430
	Dentro de Grupos	9,02520	150	0,06016	-	-
	Total	9,12711	152	0,06004	-	-
Escala de Percepción de Riesgo	Entre Grupos	0,65682	2	0,328411	1,37011	0,257
	Dentro de Grupos	35,9542	150	0,239695	-	-
	Total	36,6111	152	0,240862	-	-

Para identificar donde se genera esta diferencia, se desarrolló la prueba Tukey entre los grupos que hacen uso de Internet, en los tres rangos: de 1 a 5 horas/día, 6 a 10 horas/día y 11 o más horas/día y la escala RBS como se presenta en la Tabla 26.

Tabla 26

Resultados de la prueba de Tukey entre el tiempo medio de uso de Internet y la escala (RBS)

Grupo 1	Grupo 2	media	std err	p-value
1-5 horas/día	6-10 horas/día	0,137222	0,118321	0,691
1-5 horas/día	11 ó más horas/día	0,380736	0,118871	0,063
6-10 horas/día	11 ó más horas/día	0,243514	0,055950	0,006

En conclusión, los resultados obtenidos demuestran que en la escala RBS los encuestados del grupo de 11 o más horas/día con una media=3,012 se encuentran más expuestos y son más tolerantes ante situaciones de riesgo, en comparación a los grupos que hacen uso de un menor tiempo de Internet. Estos resultados coinciden con los resultados obtenidos por (Ö‡ütçü et al., 2016a), quienes encontraron que se genera la diferencia significativa en la escala RBS.

Prueba de H4: Existe una correlación significativa entre los promedios de las escalas {RBS, CBS, EOS, RPS}.

Finalmente, para probar H4, se desarrolló la correlación de Pearson para probar que existe una correlación ya sea positiva en el caso de que el valor obtenido al comparar las escalas sea mayor que 0 y menor que 1, o negativa en el caso de que el valor obtenido al comparar las escalas sea menor que 0 y mayor que -1. Los datos obtenidos al comparar las escalas al usar la correlación de Pearson se presentan en la Tabla 27.

Tabla 27

Resultados de la Correlación de Pearson

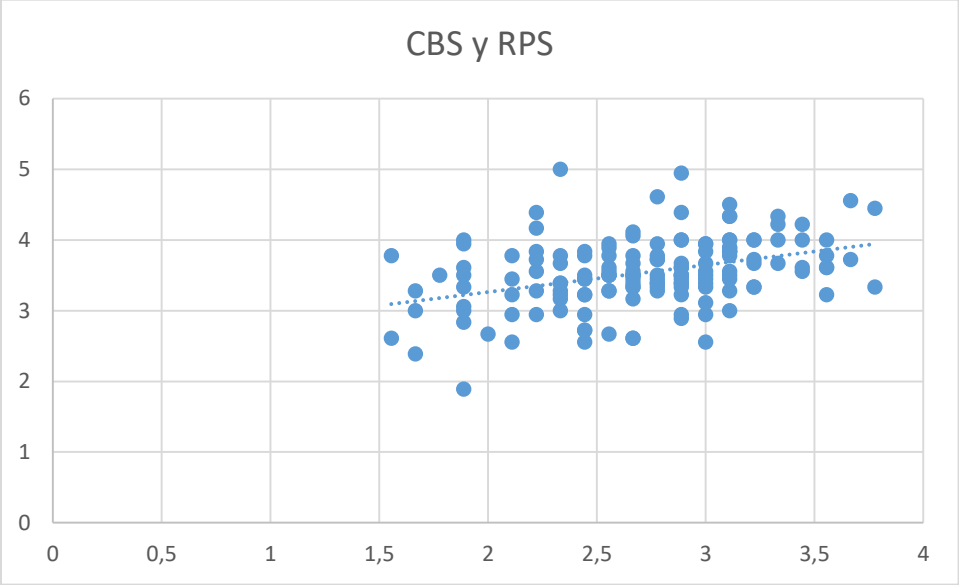
Escalas		RBS	CBS	EOS	RPS
Escala de Comportamiento de riesgo (RBS)	r	1	0,175544	0,007053	0,23947
Escala de Comportamiento Conservador (CBS)	r	0,17554	1	-0,20972	0,381002
Escala de Exposición a Ofensas (EOS)	r	0,007053	-0,20972	1	-0,12996
Escala de Percepción de Riesgo (RPS)	r	0,239474	0,381002	-0,12996	1

A continuación, se describen las correlaciones obtenidas:

En la Figura 2 se muestra el gráfico de dispersión obtenido, con una línea de tendencia entre las escalas CBS y RPS que muestra una correlación positiva con un r= 0,38, tal como se presenta en la Tabla 24, siendo las escalas con el coeficiente de correlación más alto obtenido en la investigación.

Figura 2

Relación existente entre las escalas CBS y RPS, obtenido del proceso de la correlación de Pearson



En el caso de las escalas CBS y EOS se obtuvo un r= -0,20, como se presenta en la Tabla 27. Este resultado también se ve reflejado en la Figura 3, donde se presenta el grafico de dispersión con una línea de tendencia negativa, y en el caso de las escalas EOS y RPS como se observa en la Figura 4, tiene una línea de tendencia negativa al obtener coeficiente de correlación r= -0,12, como se presenta en la Tabla 24, lo que indica que, al aumentar la

exposición ante posibles situaciones de riesgo, los usuarios tendrán una menor percepción del riesgo.

Figura 3

Dispersión entre las escalas CBS y EOS

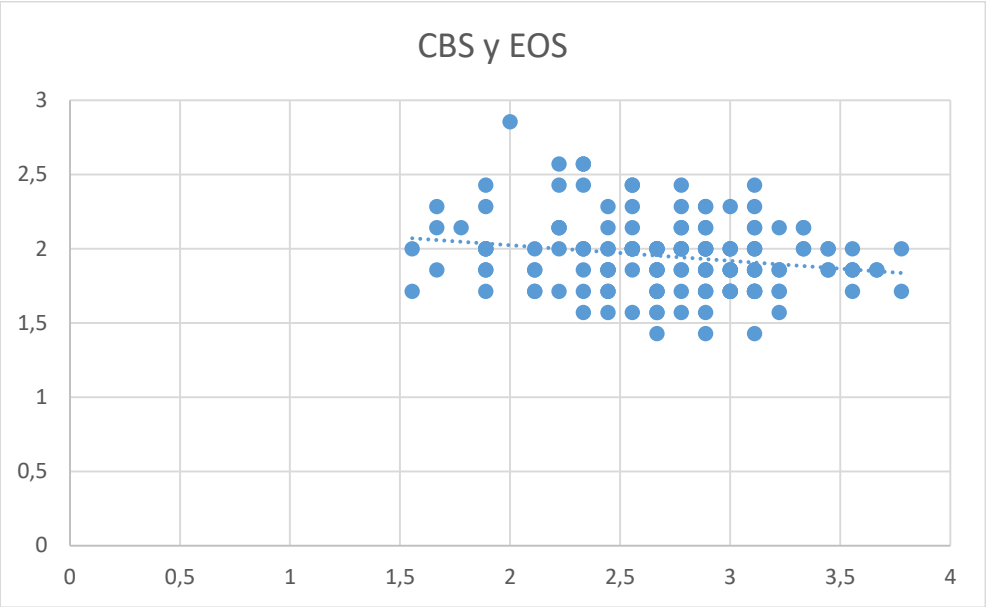
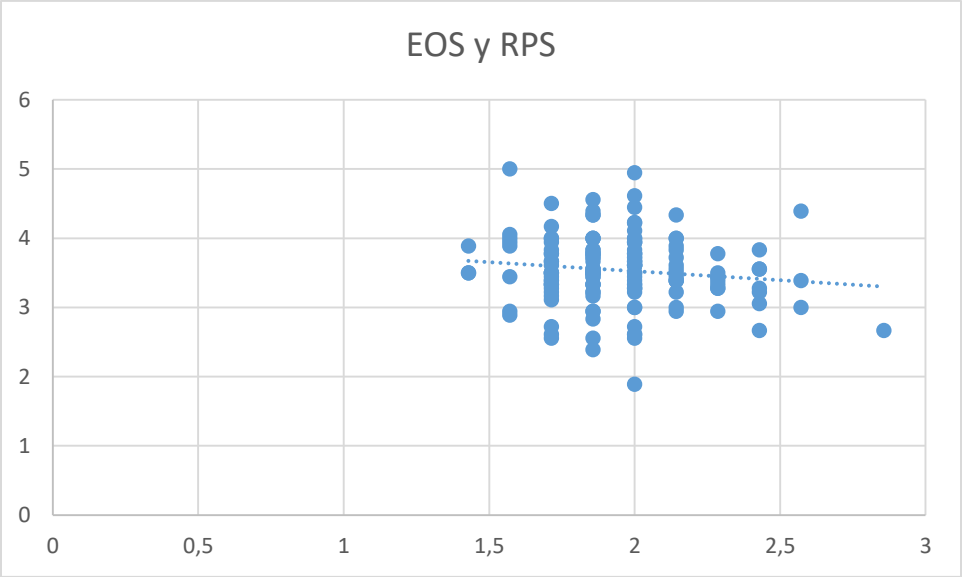


Figura 4

Dispersión entre las escalas EOS y RPS



La correlación de Pearson permitió encontrar tanto correlaciones positivas como negativas, lo que no sucedió en el estudio desarrollado por (Ö↯ütçü et al., 2016a). Los resultados expuestos en la Tabla 24 demuestran la correlación positiva más alta al comparar las escalas CBS y RPS, obteniendo un r = 0,38, lo que significa que en caso que el promedio de CBS aumente, también lo hará el promedio de RPS, es decir qué, si en un usuario aumenta el comportamiento conservador, este tendrá una mejor percepción del riesgo al hacer uso de Internet o de dispositivos de TI. Por otro lado, las correlaciones negativas obtenidas al desarrollar la correlación de Pearson, se dieron entre las escalas CBS y EOS con un r = -0,20 y entre las escalas EOS y RPS con un r = - 0,12, indicando así que en caso que el promedio de CBS aumente, el promedio de la escala EOS disminuirá, lo que quiere decir que, si en un usuario aumenta el comportamiento conservador estará menos expuesto a posibles riesgos al hacer uso de Internet o de dispositivos de TI. Haciendo el mismo análisis con el caso de las escalas EOS y RPS, si la exposición a ofensas o riesgos de un usuario aumenta, su percepción de riesgo disminuirá.

Capítulo V

Conclusiones, Trabajo Futuro y Recomendaciones

Conclusiones

La encuesta realizada al personal de la Universidad de las Fuerzas Armadas ESPE permitió categorizar al personal que es más propenso a recibir ataques de Ingeniería Social. En el presente proyecto se logró identificar que el grupo de estudiantes es más propenso a recibir ataques de Ingeniería Social, debido a su exceso de confianza y falta de experiencia, el grupo de docentes, administradores y militares al manejar información clasificada y estar al tanto de los peligros de perder cualquier tipo de información, se encuentran en el grupo de personas con menos índice de recibir ataques de Ingeniería Social.

El análisis de los resultados entre las escalas (RBS, CBS, EOS, RBS) de los grupos encuestados, se encontró que uno de los grupos presenta diferencia sobre los demás, determinando que los grupos tienen diferentes tipos de comportamientos y percepciones del riesgo al hacer uso de la Internet o dispositivos de TI, lo que permite identificar a los grupos de usuarios que necesitan adquirir conocimientos y habilidades sobre los ataques de Ingeniería Social.

Se comprobó en este estudio que, a mayor cantidad de horas de exposición de un usuario a un dispositivo digital, es mayor el peligro de ser víctima de un ataque; y si adicionalmente a esto, el usuario es más permisivo o poco cauto, el riesgo del ataque aumenta considerablemente.

Trabajo Futuro

Se plantea recopilar alrededor de 10.000 encuestas similares a la realizada en este trabajo, con la finalidad de comprobar la exactitud en la detección de la correlación entre el

comportamiento de las personas y los ataques, por medio de implementar un algoritmo de Machine Learning.

Realización de un sitio web, que ofrezca libremente la realización de la encuesta, y el análisis automático de los resultados, con la finalidad de que sea utilizada abiertamente por las instituciones que la necesiten.

Recomendaciones

Realizar capacitaciones periódicas en el tema de Seguridad de la Información al grupo de estudiantes, docentes, administradores y militares, con el fin de que reflexionen sobre los aspectos de la información que comparten.

Capacitar a los usuarios que hacen uso de Sistemas de Información o dispositivos de TI al estar en su lugar de trabajo o área estudio, para que estos identifiquen a los riesgos que están expuestos y que actúen adecuadamente, de manera que el riesgo a perder información ya sea personal u organizacional sea mitigado o reducido.

Aplicar las normas de Seguridad de la Información en la Universidad ESPE, ayudará a prevenir que el personal realice acciones indebidas y comprometa la información confidencial de cada usuario.

Bibliografía

Boone, H. N., Associate Professor, J., & Boone Associate Professor, D. A. (2012). *Analyzing Likert Data* (Vol. 50). http://www.joe.org/joe/2012april/tt2p.shtml[8/20/20129:07:48AM]

Causado Rodríguez, E., García Guiliany, J., Martínez Ventura, J., & Herrera Flórez, A. (2015). *Tecnologías de información y comunicación en el sector hotelero*. https://repositorio.cuc.edu.co/handle/11323/3184

Edwards, M., Larson, R., Green, B., Rashid, A., & Baron, A. (2017). Panning for gold: Automatically analysing online social engineering attack surfaces. *Computers and Security*, *69*, 18–34. https://doi.org/10.1016/j.cose.2016.12.013

Egele, M., Kruegel, C., Kirda, E., & Song, D. (2007). Dynamic Spyware Analysis. *Analysis*, 233–246. https://doi.org/http://portal.acm.org/citation.cfm?id=1364403

Ficarra, F. (2002). *Los virus informáticos* . https://www.redalyc.org/pdf/160/16007810.pdf

García, F., Portillo, J., Romo, J., & Benito, M. (2007). Nativos digitales y modelos de aprendizaje. *CEUR Workshop Proceedings*, *318*.

Horst, M., Kuttschreuter, M., & Gutteling, J. M. (2007). Perceived usefulness, personal experiences, risk perception and trust as determinants of adoption of e-government services in The Netherlands. *Computers in Human Behavior*, *23*(4), 1838–1852. https://doi.org/10.1016/j.chb.2005.11.003

ISO/IEC 27000. (2018). *ISO 27000 punto por punto - Glosario de términos ISO 27001*. https://normaiso27001.es/referencias-normativas-iso-27000/#def310

Lee, M. J. W., Institute of Electrical and Electronics Engineers. New South Wales Section, IEEE Education Society, University of Wollongong, Charles Sturt University, & Institute of Electrical and Electronics Engineers. (2018). Proceedings of 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE) : date and venue, 4-7 December 2018, Novotel Wollongong Northbeach Hotel, Wollongong, NSW, Australia. *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, *December*, 401–407.

López, G. C. E., & Salvador, G. R. (2015). Ingeniería social: el ataque silencioso. *Revista Tecnológica*, *8*(1), 8.

Lubeck, L. (2021). *En 2020 se duplicaron las detecciones de ataques de ingeniería social | WeLiveSecurity*. https://www.welivesecurity.com/la-es/2021/01/07/2020-duplico-detecciones-ataques-ingenieria-social/

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). *Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices*. *43*(3).

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2008). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*, 815–825. https://doi.org/10.1016/j.dss.2008.11.010

Orgill, G. L., Romney, G. W., Bailey, M. G., & Orgill, P. M. (2004). The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. *SIGITE 2004 Conference*, 177–181. https://doi.org/10.1145/1029533.1029577

Öȶütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016a). Analysis of personal information security behavior and awareness. *Computers and Security*, *56*, 83–93. https://doi.org/10.1016/j.cose.2015.10.002

Öȶütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016b). Analysis of personal information security behavior and awareness. *Computers and Security*, *56*, 83–93. https://doi.org/10.1016/j.cose.2015.10.002

Park, J.-Y., & Huh, E.-N. (2020). *A Cost-Optimization Scheme Using Security Vulnerability Measurement for Efficient Security Enhancement*. https://doi.org/10.3745/JIPS.02.0128

Quiroz, S., & Macias, D. (2017). *Seguridad en informática: consideraciones Computer security: considerations*. *3*(5), 676–688. https://doi.org/10.23857/dom.cien.pocaip.2017.3.5.agos.676-688

Rodriguez Rincón, E. Y., & García Valdés, Á. M. (2018). *Metodologías de Ingeniería Social*. 65.

Soriano, M. (n.d.). *Seguridad en redes y seguridad de la información*. Retrieved July 12, 2021, from http://improvet.cvut.cz

Suárez, D., & Ávila, A. (2015, September 10). *Vista de Una forma de interpretar la seguridad informática*. http://repository.lasallista.edu.co:8080/ojs/index.php/jet/article/view/1015/1072

Torres, G. (2021, May 6). *¿Qué es un virus informático? | Guía sobre virus informáticos | AVG*. https://www.avg.com/es/signal/what-is-a-computer-virus

Warikoo, A. (2014). Proposed Methodology for Cyber Criminal Profiling. *Information Security Journal*, *23*, 172–178. https://doi.org/10.1080/19393555.2014.931491

Wilcox, H., & Bhattacharya, M. (2016). A framework to mitigate social engineering through social media within the enterprise. *Proceedings of the 2016 IEEE 11th Conference on Industrial Electronics and Applications, ICIEA 2016*, 1039–1044. https://doi.org/10.1109/ICIEA.2016.7603735

Ye, Z., Guo, Y., Ju, A., Wei, F., Zhang, R., & Ma, J. (2020). A risk analysis framework for social engineering attack based on user profiling. *Journal of Organizational and End User Computing*, *32*(3), 37–49. https://doi.org/10.4018/JOEUC.2020070104

Zhou, Q., Shahidehpour, M., Alabdulwahab, A., & Abusorrah, A. (2020). A Cyber-Attack Resilient Distributed Control Strategy in Islanded Microgrids. *IEEE Transactions on Smart Grid*, *11*(5), 3690–3701. https://doi.org/10.1109/TSG.2020.2979160