ISSN-E: 2697-3650

Minerva Journal
Vol.3, Spec. Issue N°1, (pp. 34-41)

https://doi.org/10.47460/minerva.v1iSpecial.77

Modelo de gestión de seguridad en los dispositivos móviles en la comunidad universitaria

Rivadeneira Fabricio
https://orcid.org/0000-0001-6663-0070
Fabricior.rivadeneira@uleam.edu.ec
Universidad Laica Eloy Alfaro de Manabí
Chone - Ecuador

Macías Ángel
https://orcid.org/0000-0002-2557-0267
angel.anhely@gmail.com
Universidad Laica Eloy Alfaro de Manabí
Chone - Ecuador

Garcés Mercedes
https://orcid.org/0000-0001-8677-4274
mercedescatalin@outlook.com
Universidad Laica Eloy Alfaro de Manabí
Chone - Ecuador

Bravo Holger
https://orcid.org/0000-0002-7595-6248
Kiritosama1999@gmail.com
Universidad Laica Eloy Alfaro de Manabí
Chone - Ecuador

Andrade Martha
https://orcid.org/0000-0002-8481-2406
martty2596@hotmail.com Universidad
Laica Eloy Alfaro de Manabí
Chone - Ecuador

Recibido(11/05/2022), Aceptado(13/07/2022)

Resumen. - La declaratoria de emergencia sanitaria a nivel mundial, por la pandemia del COVID-19 incrementó el uso de los dispositivos móviles, para realizar diferentes actividades, pero asociado a su utilización vienen riesgos de seguridad de la información. Conociendo que el ser humano es el encargado de operar los dispositivos móviles, y siendo este el eslabón más débil en la cadena de seguridad, al no gestionar de forma correcta la seguridad podría ser víctima de ataques de ingeniería social. Con esta investigación se determinó, como la comunidad universitaria gestiona, la seguridad en los dispositivos móviles, para lo cual se aplicaron 310 encuestas a estudiantes, docentes, personal administrativo y de servicio, para el análisis de resultado, se aplicó el método estadístico, de análisis descriptivo, obteniendo como resultado que el 89% de encuestados gestionan de forma correcta los riesgos asociados a la seguridad, aunque la universidad no realiza capacitaciones, ni difunde mecanismos de protección para evitar ataques de ingeniería social.

Palabras clave: Seguridad móvil, ingeniería social, gestión de seguridad.

Security management model for mobile devices in the university community

Abstract. - The declaration of a global health emergency, due to the COVID-19 pandemic, increased the use of mobile devices to carry out different activities but associated with their use come information security risks. Knowing that the human being is in charge of operating mobile devices, and this being the weakest link in the security chain, by not managing security correctly, it could be a victim of social engineering attacks. With this research, it was determined how the university community manages security in mobile devices, for which 310 surveys were applied to students, teachers, administrative and service personnel, for the analysis of the result, the statistical method was applied, descriptive analysis, obtaining as a result that 89% of respondents correctly manage the risks associated with security, although the university does not carry out training, nor does it disseminate protection mechanisms to avoid social engineering attacks.

Keywords: mobile security, social engineering, security management.

I. INTRODUCCIÓN

El estudio propuesto brindará antecedentes sobre la seguridad informática después de la pandemia a un nivel superior esto es importante ya que será beneficioso para ver dónde hay brechas y brindar un mejor servicio y revisar las vulnerabilidades en los procesos, convirtiéndose en la norma para otras organizaciones.
A lo largo del tiempo la sociedad ha incrementado a nivel exponencial la tecnología como medio de uso cotidiano, haciendo que elementos como los dispositivos móviles permitan a las personas emplearla de manera fácil y efectiva en todos los ámbitos. Los dispositivos móviles representan nuevas oportunidades para que los usuarios accedan a la información. Sin embargo, una mala gestión de estos dispositivos por parte de los usuarios puede provocar un problema de seguridad más aún si contiene información y acceso a aplicaciones para el desarrollos de sus actividades en la universidad, el presente estudio acerca de la Ingeniería Social y la Gestión de riesgos en dispositivos móviles puede permitirnos distinguir con claridad los potenciales problemas que hacen a los usuarios no identificar el ser víctimas; y de esta manera presentar como dar resolución a problemas concretos, en un área de actividad específica.

A nivel mundial el uso de dispositivos móviles para 2016 fue el 2.5, pero el 2021 ascendió a un 3.8% lo que representó un incremento de 1.371 millones de unidades, la cual ha seguido incrementándose a pesar del estancamiento del mercado, debido al creciente precio medio de venta de los teléfonos. Además, cabe denotar que la población mundial es de 7.400 millones de personas, valor que aparenta ser medianamente alto aun cuando se toma en consideración que el mundo tiene actualmente 7.700 millones de suscripciones a teléfonos móviles, es decir, hay más dispositivos móviles que habitantes. Otros datos es que ocho de cada 10 personas tienen cobertura móvil en el mundo, casi la mitad de la población mundial (3.600 millones de personas) usa Internet y tiene ordenador con conexión en casa [1].

Ecuador es uno de los países latinoamericanos con mayores repercusiones debido a la propagación de los dispositivos móviles. Su población urbana es tan solo del 64,3% (de un total de 17.77 millones de habitantes) lo que marca una diferencia significativa respecto a otros países latinoamericanos y nos dice mucho sobre el acceso de la población a internet ya que del 35,7% de su población rural solo el 16% cuenta con acceso a internet. Pese a esto, Ecuador experimenta un crecimiento en el acceso a internet y a redes sociales: un 10.17 millones de usuarios de internet y 14 millones de perfiles en redes sociales. De acuerdo con los datos del último análisis del incremento de dispositivos móviles se revela que cerca del 79.4% de usuarios poseen un aparato móvil con conexión perenne a internet; conllevando así a un aumento del 92% con usuarios que ingresan a medios sociales y as u vez haciendo que a diarios se sumen 16.7% de usuarios nuevos, lo que suma a 2 millones de perfiles nuevos [2].

El artículo está estructurado de la siguiente forma en la sección de desarrollo se encuentran temas como los dispositivos móviles, gestión de seguridad informática y la ingeriría social; a continuación, en la sección de la metodología se describe el método aplicado y el instrumento que se aplicó para la recolección de datos y la formula como se pondero para la clasificación de la gestión de riesgo, Buena, Regular y Mala. En la última sección se hace un análisis de los resultados obtenidos por medio del programa SPSS y se hace referencia a una investigación futura.

II. DESARROLLO

El fundamento de que el ser humano es el eslabón más difícil cuando nos referimos a seguridad informática toma mayor relevancia según se dan nuevos avances en los medios digitales y electrónicos, pues la dependencia de permanecer constantemente conectados por factores organizativos e interpersonales en la actualidad es bien percibida. La consecuencia de ser víctimas de un ataque puede significar no solo un gran impacto a nivel personal sino económico debido al costo oculto que puede desarrollarse para corregir la brecha de seguridad. Entre las consecuencias de ser víctimas de un ataque se encuentran la perdida de credenciales, suplantación de red y fallos de restricción acceso de URL malignos, lo cual involucra la perdida intelectual; además de los gastos para recuperar la operatividad de una persona y/o institución [3].

De acuerdo con un estudio las TICS en el periodo del COVID-19, los temas de seguridad se volvieron fundamentales para todas las empresas a nivel nacional; según datos del Ministerio de telecomunicaciones en el año 2019 se registró un 41.05% de personas que usan computadoras y el 59.9%; de personas que tienen teléfono celular así mismo un 45.5% de personas con acceso a internet [4].

Los dispositivos móviles son aparatos de tamaño pequeño que cuentan con características tales como es el concepto de movilidad, los dispositivos móviles son pequeños para poder portarse y ser fácilmente empleados durante su transporte. En muchas ocasiones pueden ser sincronizados con algún sistema de la computadora para actualizar aplicaciones y datos [5].

Este tipo de dispositivos se comportan como si estuvieran directamente conectados a una red mediante un cable, dando la impresión al usuario que los datos están almacenados en el propio dispositivo.

Los conceptos de móvil y sin cables muchas veces se confunden. Un PDA con datos en él y aplicaciones para gestionarlos, puede ser móvil, pero no tiene por qué ser inalámbrico, ya que puede necesitar un cable para conectarse a la computadora y obtener o enviar datos y aplicaciones [6]. Por otro lado, un teléfono móvil equipado con un pequeño navegador puede hacer uso de Internet, considerándose inalámbrico, pero no móvil ya que no dispone de un valor agregado que aporte como característica extra alguna función en las aplicaciones del dispositivo cuando éste no está conectado a otros sistemas tales como: Computadoras, cámaras, etc. Si el PDA es capaz de conectarse a una red para obtener datos "en medio de la calle", entonces también se considera inalámbrico [7].

a) Paginadores.
b) Comunicadores de bolsillo.
c) Internet Screen Phones.
d) Sistemas de navegación de automóviles.
e) Sistemas de entretenimiento.
f) Sistemas de televisión e Internet (WebTV).
g) Teléfonos móviles.
h) Organizadores y asistentes personales digitales (Personal Digital Assistant).

Considerando el análisis detallado de la evolución de la Ingeniería Social y el impacto en los principales medios electrónicos y sociales del mundo durante el período 2015-2020, así como la indagación acerca del modo en que los hackers percibían la situación del sistema, permite visualizar los mecanismos que posibilitaron el desarrollo de un ataque no solo a dimensiones personales sino a nivel corporativo como la que vivió el mundo a partir del año 2020 [8]. La Ingeniería Social es usada en política con varios sentidos, uno relacionado a esfuerzos para la influencia de actitudes, relación o acciones sociales sobre la población de un país o región y el otro es implementado en programas de transformaciones sociales. [9].

Históricamente el termino ingeniería social fue apoyado por empresas para referirse a la persona que tenía función de mediador en la resolución de conflictos con intermediación racional entre el capital y el trabajo. [10] Sin embargo, en el año 1945 sufre una reintroducción por parte de Karl Popper donde llega a ser un método o técnica para el logro de multiplicidad de resultados, es decir se deja el concepto de ser un instrumento para resolución de conflictos para transformarse en manipulación de personas [11].

Por ello, ante esta situación es evidente que nos encontramos en una era donde virus, hacker, técnicas de phishing, ciberataque, fraudes y por falta de conocimiento y aplicación de técnicas, nos lleva a la importancia de generar una cultura de seguridad informática, para evitar la pérdida de información de importante y vital para nosotros y a la empresa que pertenecemos [12].

En la encuesta realizada por ESET a finales de 2020, el 87,6% de los participantes opinó que los cibercriminales han visto una oportunidad en el incremento del trabajo remoto para lanzar ataques dirigidos a las empresas, especialmente de ransomware, luego de comprometer los accesos remotos [13]. Adicionalmente con base en la telemetría de ESET, las empresas de Brasil (26,4%) fueron las más afectadas por casos de phishing durante 2020, seguidas por las empresas de Perú (22,8%), México con un (12%), Argentina (13,3%), Colombia (10,6%), Perú (8,9%) y finalmente Ecuador (5.8%) [13].

La ingeniería social puede entenderse como un tipo ataque (informático o telefónico) hacia un usuario y/o institución con la finalidad de recolectar información personal mediante el uso de técnicas de engaño [14]. Una definición clara del término Ingenieria Social se describe como el arte de manipular personas para eludir los sistemas de seguridad, consiste en obtener información de los usuarios por teléfono, correo electrónico, correo tradicional o contacto directo. Entre las formas de ataque podemos encontrar el Pretexting, tailgaiting, Baiting y el sextorsion [15].

La gran mayoría de ataques a empresas y/o persones naturales conllevan algún tipo de ataque de ingeniera social; por ejemplo, los clásicos correos electrónicos de “phishing” con estafas de tipo suplantaría (personal y/o institución), inserción de virus [16]. Para esto es evidente considerar que el primer paso para que inicie un proceso de protección contra ataques de ingeniera social se debe dar desde la educación en instituciones y a través de medios electrónicos; de esta manera impulsando campañas de este tipo se lograría formas de aprendizaje de como nunca dar clic en enlaces de origen desconocidos enviados a medios sociales y proteger las credenciales de los usuarios [17].

III. METODOLOGÍA

Como primer punto, se realizó una revisión sistemática de la literatura enfocada al campo de estudio, para poder realizar una encuesta dentro de un formulario de Google Forms, la cual fue dirigida a la Universidad laica Eloy Alfaro de Manabí extensión Chone y así permita observar y analizar la gestión de riesgo de la comunidad universitaria, la cual fue enviada por medio del correo institucional a la población de estudio, por consiguiente se depuraron las encuestas que estaban incompletas y se volvió a aplicar a otros usuarios hasta obtener el total de la muestra, la cual fue valorada por expertos, en este sentido se emplearon 20 preguntas para conocer la manera en que la comunidad universitaria gestiona la seguridad informática, se consideró una población de 1609 personas que conforman el personal administrativo, personal del código de trabajo, docentes de nombramiento, docentes de contrato y estudiantes. Además, se aplicó la ecuación (1) correspondiente al cálculo de la muestra finita.

$$n = \frac{(Z)^2 * p * q * N}{e^2 (N-1) + Z^2 (p * q)} \quad (1)$$

Esto se refiere a:

n = Tamaño de la muestra.
N = Tamaño de la población (1609).
p = Probabilidad a favor (0.5).
e = Error de muestra (5% = 0.05).
q = Probabilidad en contra (0.5).
Z = Nivel de confianza (95% = 1.96).

Una vez que se obtuvo la muestra esta fue distribuida en 247 estudiantes, 11 docentes de contrato, 25 docentes de nombramiento, 3 del personal del código de trabajo y 24 del personal administrativo. Se utilizó para el análisis estadístico la aplicación SPSS para hacer depuración de los resultados, para comprender el nivel de la gestión de riesgos de los miembros de la comunidad universitaria se ponderó cada pregunta de la encuesta por Buena=3, Regular =2 y Malo=1; estos valores se multiplicaron por el número de respuestas contestadas, por un grupo de 20 preguntas, que arroja un total máximo de 60 puntos por miembro, donde el resultado menor de 35 puntos da a conocer que posee una mala gestión de riesgo, menos de 45 puntos gestiona de forma regular los riesgos en los dispositivos móviles y mayor a 46 puntos gestiona de buena forma los riesgos en los dispositivos móviles.

IV. RESULTADOS

Una vez realizado el estudio, se pueden describir los siguientes resultados basados en la encuesta de 20 preguntas que incluían consultas sobre el tipo de contraseña empleada, uso apropiado de contraseñas, uso apropiado de descargas, uso de gestores de contraseñas, la frecuencia del cambio de contraseñas en el dispositivo y las diferentes cuentas que en el administra el mismo. Lo cual muestra los siguientes resultados.

Los resultados mostraron que el uso del correo no se hace con la debida seguridad, pero se respetan ciertas normas que permiten tener una seguridad moderada, sin embargo, cuando se trata de redes sociales, la seguridad es mínima, ya que se abren enlaces sin las previsiones necesarias y se realizan descargas de forma indiscriminada de forma regular. Así mismo se observó que un alto porcentaje, correspondiente al 76% de las personas encuestadas, mantiene la sesión iniciada de sus redes sociales de forma permanente, mientras que solo el 7% cierra la sesión oportunamente. Estos datos observados permiten afirmar que la seguridad de las personas que conforman la comunidad universitaria no es la más idónea y están expuestos a posibles situaciones de riesgos, lo cual refleja además que es importante hacer énfasis en la seguridad en los entornos universitarios.

Por otro lado, se observó que las actualizaciones de los dispositivos generan una brecha de inseguridad ya que la mayoría desconoce si su sistema operativo se encuentra en su última actualización, esto se debe también a la poca cultura tecnológica que está brindando la universidad a todos los miembros de la comunidad universitaria. Otro de los datos que nos hace énfasis en la inseguridad de la información es que el 88% de los encuestados desconocen si han sido víctimas de un ciberataque, lo cual nos deja en duda los métodos que los miembros de la comunidad universitaria usan para proteger sus equipos y cuentas antes de ser atacados por un ciber delincuente, incluso ponen en riesgo la integridad de su información personal y la información de la organización a la que ellos pertenecen.

Analizando los datos se obtiene que el 4% de los encuestados pose una buena gestión de riesgos en sus diferentes dispositivos, el 75% de los encuestados dio a conocer que posee una regular gestión de riesgos, y el 21% pose una gestión mala de los riesgos, por tanto, se pudo identificar que aunque la universidad no capacite o no difunda estrategias para mitigar ataques de ingeniería social a los miembros de la comunidad universitaria, estos de forma empírica o por conocimiento general el personal universitario gestiona medianamente los riesgos de seguridad en sus dispositivos móviles. En base se plantea para futuras investigaciones el uso de un modelo de concientización para gestionar de forma eficiente la seguridad de la información en los dispositivos móviles elaborado por los autores, el mismo que a continuación se propone.

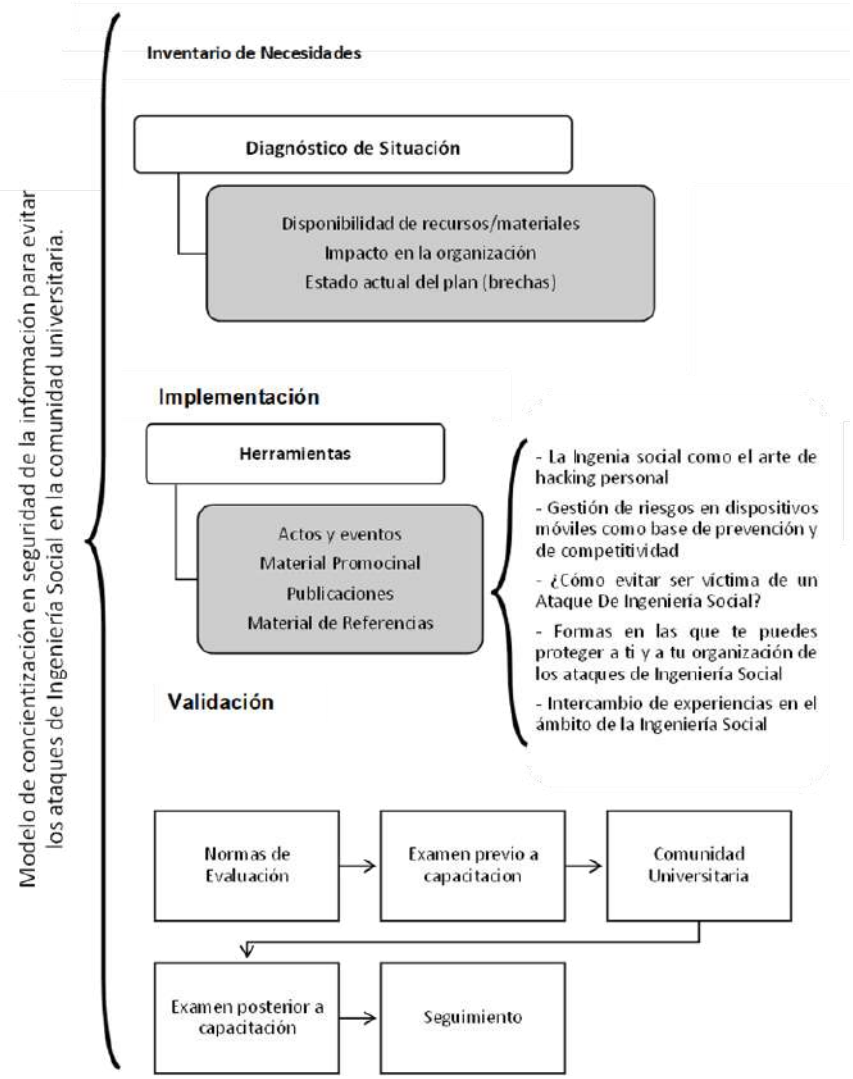

Fig. 1. Esquema del plan de concientización.

IV. CONCLUSIONES

El del uso de los dispositivos móviles a nivel mundial viene incrementando año tras año, pero con la pandemia del COVID-19 su uso tanto parta actividades personales como laborales sufrió un crecimiento considerable, pero asociado al manejo de estos dispositivos vienen riesgos de seguridad que si no se gestionan de forma adecuada pueden ser aprovechados por personas inescrupulosas que pudiesen afectar socialmente a los usuarios, a través un vector de ataque efectivo y poniendo en un riesgo alto la confidencialidad, integridad y disponibilidad de la informaciónde la comunidad universitaria.

La comunidad universitaria de la Universidad Laica Eloy Alfaro de Manabí en su gran mayoría desconocen el término de ingeniería social y no saben cómo actuar si son víctimas de un ciberdelito pero aun así gestiona de forma regular y empírica los riesgos de seguridad en sus dispositivos móviles, por eso es importante que se cree un plan de concientización y difusión de los riesgos asociados a la ingeniería social y les permita ser el primer firewall en la protección de datos almacenados en sus equipos.

El uso apropiado de los dispositivos móviles, manteniendo los niveles de seguridad, puede ser una herramienta útil para la gestión de múltiples actividades de la vida diaria, desde una clase virtual, una actividad bancaria, la comunicación familiar, entre otras, que son necesarias en la vida moderna. Sin embargo, estas actividades pueden verse perjudicadas debido al alto impacto que puede generar un ciberataque en nuestro dispositivo, desde acceder a nuestros datos bancarios, información personal y sobre todo abrir paso para que las personas detrás de este ataque obtengan información privilegiada de la institución a la que pertenecen.

La importancia de esta investigación justamente radica en solucionar un problema existente el cuál es la brecha de inseguridad de la información que existe en la comunidad universitaria, y nuestra investigación propone un plan de concientización para poder así mejorar la gestión de riesgos en los dispositivos móviles y poder minimizar ataques de ciber delincuentes que quieran perjudicar la información privada de la institución y lucrarse a costa de una mala seguridad por que los miembros de la comunidad universitaria, que no saben cómo actuar ante un ciber ataque.

REFERENCIAS

[1] Rosa Fernández, «Número de usuarios de smartphones a nivel mundial desde 2016 hasta 2021,» https://es.statista.com, 14 02 2022. [En línea]. Available: https://es.statista.com/estadisticas/636569/usuarios-de-telefonos-inteligentes-a-nivel-mundial/. [Último acceso: 12 07 2022].
[2] J. P. Del Alcázar Ponce, «Estado Digital Oct/21,» MENTINNO, 31 10 2021. [En línea]. Available: https://drive.google.com/file/d/1HIrELN8_t38AAwvS7zGgEFWsuhMhKq7D/view. [Último acceso: 12 07 2022].
[3] Y. S. Pascuas Rengifo, J. A. García Quintero y M. A. Mercado Varela, «Dispositivos móviles en la educación: tendencias e impacto para la innovación,» Revista Politécnica, vol. 16, nº 31, pp. 97-109, 2020.
[4] Instituto Nacional de Estadística y Censos, «Encuesta de seguimineto al plan nacional de desarrollo,» Encuesta Multipropósito - TIC, Quito, 2020.
[5] M. Jiménez Morales, M. Montaña y P. Medina Bravo, «Uso infantil de dispositivos móviles: influencia del nivel socioeducativo materno,» repositori.upf.edu, vol. 21, nº 8, p. 64, 2020.
[6] D. W. Herrera Chávez, «Diseño e implementación de un prototipo de seguridad para control domótico basado en IoT bajo ambientes de dispositivos móviles con Android,» 07 05 2020. [En línea]. Available: https://bibdigital.epn.edu.ec/handle/15000/20857. [Último acceso: 12 07 2022].
[7] G. Rueda, P. P. Laura Patricia y M. Lina, « Uso de dispositivos móviles como mediadores didácticos para fortalecer los recursos de aprendizaje de las ciencias naturales para el currículo de transición institución educativa Valentín García Granada-Meta,» Corporación Universitaria Minuto de Dios, Villavicencio-Colombia., 2019.
[8] A. Méndez Carvajal, «Estudio de metodologías de ingeniería social,» 12 2018. [En línea]. Available: http://openaccess.uoc.edu/webapps/o2/handle/10609/90305. [Último acceso: 11 07 2021].
[9] J. J. SEDANO PINZÓN, «LA INGENIERÍA SOCIAL, EL ANTES Y EL AHORA DE UN,» UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA, COLOMBIA, 2019.
[10] D. Berenguer Serrato, «Estudio de metodologías de ingeniería social,» 01 06 2018. [En línea]. Available: http://openaccess.uoc.edu/webapps/o2/handle/10609/81273. [Último acceso: 12 07 2022].
[11] C. BAUTISTA LIZ, «UN CIBERATAQUE BASADO EN LA INGENERIA SOCIAL,» prcrepository.org, PUERTO RICO, 2021.
[12] M. Domingo Prieto, Seguridad en dispositivos móviles, España: Universitat Oberta de Catalunya, 2019.
[13] ESET Security Report (ESR), «SECURITY REPORT Latinoamerica,» ESET, 2021.
[14] E. Y. Rodriguez Rincón, «Metodologias de la Ingeneria social,» 01 Junio 2018. [En línea]. Available: https://solutecsos.com/documts/metodologia_ingeniera%20social.pdf. [Último acceso: 12 07 2022].
[15] J. P. Prado Díaz, «Ingeniería social, un ejemplo práctico,» ODIGOS, vol. 2, nº 3, p. 30, 2021.

[16] N. A. Camacho Nieto, «Una breve mirada a la ingeniería social,» 10 10 2016. [En línea]. Available: http://repository.unipiloto.edu.co/handle/20.500.12277/2712. [Último acceso: 12 07 2022].
[17] J. J. Sedano Pinzón, «La ingeniería social, el antes y el ahora de un problema global,» 26 07 2019. [En línea]. Available: https://repository.unad.edu.co/handle/10596/28152. [Último acceso: 12 07 2022].

Fabricio Rivadeneira, Ingeniero en Sistemas desde el 2010, Magister en Gerencia de Proyectos Educativos y Sociales, Docente de la Universidad Laica Eloy Alfaro de Manabí Extensión Chone. Docente Investigador acreditado por la SENESCYT REG-INV-18-02050.

Ángel Macías, Estudiante de Ingeniería en Sistemas, realice una tesis con el tema: Gestión de riesgos en dispositivos móviles para minimizar ataques de ingeniería social en la Comunidad Universitaria de la Universidad Laica Eloy Alfaro de Manabí Extensión Chone. Soy un "Auditor y Pentester de Redes Wi-Fi", certificado.

Mercedes Garces, Estudiante de Ingeniería en Sistemas, realizando una tesis con el tema: Gestión de riesgos en Cloud Computing para la continuidad de los servicios de las Instituciones Públicas del cantón Chone en la Universidad Laica Eloy Alfaro de Manabí, realice una certificación de Analista de sistemas y Marketing digital.

Josué Bravo, Estudiante de Ingeniería en sistemas, realizando una tesis con el tema: Gestión de riesgos en dispositivos móviles para mitigar ataques de ingeniería social en la comunidad universitaria Universidad Laica Eloy Alfaro de Manabí Extensión Chone. Poseo certificaciones de Hacking ético y Pentester.

Martha Andrade, Estudiante de Ingeniería en sistemas, realizando una tesis con el tema: Evaluación operativa del uso de pantalla táctil como tecnología de Información en las aulas del Área Técnica en la Universidad Laica Eloy Alfaro de Manabí Extensión Chone, realice una certificación como Analista de sistemas.