Recibido: Nov. 19, 2023 | Aceptado: Feb. 16, 2024 | Publicado: Abr. 1, 2024.

Ingeniería Social

Social engineering

DOI: https://doi.org/10.21803/ingecana.3.3.740

José Hernando López Torres[1] y Jasson Esteban Torres Buitrago[2]

1. Ingeniero en Telecomunicaciones y Especialista En Seguridad Informática, Fundación Universitaria San Mateo, correo: jhlopez@sanmateo.edu.co, Orcid: https://orcid.org/0000-0001-7163-6725
2. Ingeniero en Telecomunicaciones y Especialista En Seguridad Informática, Fundación Universitaria San Mateo, Correo: jestebantorres@sanmateo.edu.co. Orcid: https://orcid.org/0009-0001-1022-4863

Resumen

La ingeniería social es una técnica la cual se utiliza para engañar y manipular a las personas con el fin de tener información confidencial, se basa en aprovechar la psicología humana y toda la interacción social posible para lograr los objetivos, es por esto que a través de esta manipulación los que realizan ingeniería social se infiltran en los distintos tipos de sistemas y organizaciones. La ingeniería social en el entorno de la seguridad de la información representa un gran desafío pues la sociedad debe tomar medidas para educarse sobre todos los riesgos que esto abarca, fomentando la conciencia de seguridad y estableciendo ciertos criterios para garantizar la protección de la información.

Palabras clave: Abarca; Aprovechar; Datos; Desafío; Engañar; Estafadores; Información.

Abstract

Social engineering is a technique which is used to deceive and manipulate people in order to have confidential information, it is based on taking advantage of human psychology and all possible social interaction to achieve the objectives, which is why through Through this manipulation, those who perform social engineering infiltrate different types of systems and organizations. Social engineering in the information security environment represents a great challenge since society must take measures to educate itself about all the risks that this encompasses, promoting security awareness and establishing certain criteria to guarantee the protection of information.

Keywords: *Encompasses; Leverage; Data; Challenge; Deceive; Scammers; Information.*

Cómo citar este artículo:
J. H. López-Torres, J. E. Torres-Buitrago, «Ingeniería Social». Ingente Americana, vol. 3, n°3, e-740, 2023. DOI: https://doi.org/10.21803/ingecana.3.3.740

Introducción

El ser humano siempre ha tenido la necesidad de conocer de una forma u otra la información relevante para poder tener la ventana en algún ámbito, ya sea en guerras, en un negocio, en una competencia o a nivel empresarial. Por esta razón, han surgido diferentes técnicas de espionaje, infiltración o hacking, realizadas por diferentes personas brillantes a lo largo de la historia en áreas como la criptografía, física o matemáticas, en donde se ha buscado obtener a cualquier precio las contraseñas, o códigos secretos para ganar las guerras, sobre todo.

A raíz de eso, se han venido desarrollando técnicas para obtener esa información secreta, como son: el hackeo, el espionaje, la infiltración, la criptografía, entre otras. Una de las más usadas es la ingeniería social, que es una técnica psicológica en la cual se busca la manera de manipular a otras personas para obtener información importante, ya sea con engaños o habilidades sociales, para que realice alguna acción específica y lograr la meta o beneficio.

En este trabajo, se explorarán los fundamentos de la Ingeniería Social, comprendiendo su relación con la psicología humana y cómo se aprovecha de la interacción social para llevar a cabo sus actividades, principalmente ilegales o maliciosas. Analizaremos distintos tipos de Ingeniería Social, como el phishing, donde los estafadores se hacen pasar por entidades confiables para obtener datos personales y financieros, entre otras técnicas bastante usadas por los ciberdelincuentes.

Con la realización de este trabajo podremos entender la importancia de la ingeniería social en el ámbito de la seguridad de la información, con todos los desafíos que plantea y teniendo en cuenta las medidas que se pueden adoptar para poder proteger los datos. A través de la educación se puede fortalecer la seguridad, ya que en el mundo en que vivimos uno como personal del común es cada vez más vulnerable, pues la conectividad a la red desde los diversos dispositivos deja a las personas más expuestas a estos tipos de ataques.

II. MARCO TEÓRICO

La ingeniería social se basa en una premisa básica: los humanos son más fáciles de manejar que las máquinas. Para llevar a cabo este tipo de ataques se utilizan técnicas de manipulación psicológica con el objetivo de que los usuarios revelen información confidencial o realicen cualquier tipo de acción que pueda beneficiar a los ciberdelincuentes.

A. Historia de la Ingeniería Social

La ingeniería social tiene sus raíces en la antigüedad, cuando los líderes políticos y militares

usaban tácticas de manipulación para obtener información estratégica; sin embargo, no era conocida con este nombre en ese momento. Gracias a esas técnicas o tácticas de manipulación y engaño, los ejércitos pudieron ganar guerras y llevar a su pueblo a la victoria; por esta razón, siempre ha sido muy importante en la vida del ser humano.

El nombre de Ingeniería Social como tal, surgió para el año 1945 gracias al filósofo Karl Popper, quien en su momento lo nombró un elemento psicológico y sociológico para mejorar estructuras sociales, con el pensamiento que al ser humano se le podía optimizar al igual que a una máquina. Para el año de 1970, los sucesores de Popper incluyeron a lo que había definido él, el concepto de engaños psicológicos. [1]

Con el paso de los años, a este concepto de engaños psicológicos se le ha sumado la manipulación y la suplantación, convirtiendo a la ingeniería social en uno de los ataques más usados por los ciberdelincuentes para obtener información valiosa y hacer ataques a empresas reconocidas a nivel mundial.

Con la llegada de la era digital, la ingeniería social ha evolucionado y se ha vuelto más sofisticada. Hoy en día, los ciberdelincuentes y los estafadores utilizan la tecnología de la comunicación y todos los avances tecnológicos que han surgido en los últimos años, como lo es: la conectividad a internet, el uso de correo electrónico, el uso del celular, las compras en línea, el internet de las cosas, entre otros; para llevar a cabo ataques de ingeniería social.

B. Importancia de su afectación

Debido a la creciente dependencia de la tecnología y las interconexiones digitales, la ingeniería social es muy importante para nuestra sociedad moderna, sobre todo para las empresas, en donde la información es el activo más importante de su negocio. Los ataques de ingeniería social pueden tener consecuencias graves, incluido el robo de identidad, la pérdida de datos confidenciales y pérdidas financieras. Es muy importante comprender las técnicas utilizadas por los ingenieros sociales y comprender los riesgos involucrados en la protección de nuestra información personal y la de nuestra organización, para poder estar preparados ante cualquier posible ataque de este tipo.

III. Algunos ejemplos de ataques con el uso de la Ingeniería Social que se han realizado a lo largo de los años.

1) La estafa nigeriana o estafa 419.

Surgió para la época de los 90. En esta estafa, los usuarios recibían un correo en donde se le informaba que habían sido ganadores de una herencia de un príncipe de Nigeria, gracias a un sorteo que había realizado. Para poder acceder al premio, la persona debía consignar una buena suma de dinero, que en comparación con el premio resultaba insignificante y por esto, es que muchos cayeron en esa estafa. Con el pasar de los años, se han venido desarrollando estafas similares, pero un poco más elaboradas y de diversa índole.

2) Scams relacionados a muertes de celebridades.

Con este tipo de ataque se juega con el morbo de las personas, enviando una noticia falsa que, por lo general, tiene que ver con la muerte de una celebridad en trágicas circunstancias, en busca que la gente quiera saber más sobre esto y haga clic en el enlace que viene en el mensaje, el cual es malicioso.

3) Falsas noticias alarmantes en Facebook

Se realiza a través de un usuario anónimo que

simplemente publica una noticia en la red social, por lo general en la biografía de alguna persona, indicando, por ejemplo, que Microsoft va a cambiar de color el entorno de la página y para evitar que se realice, se debía ingresar a un enlace que contenía el mensaje, el cual redireccionaba a un sitio infectado. Ahí también había variantes como cambiar la noticia que se iba a cambiar el color a rosa y colocar que se generó una actualización y ya se podía tener el botón "No me gusta". Para poder tenerlo, se debía acceder de igual manera a un enlace relacionado en la publicación.

4) Fotos y videos íntimos de famosos

En este método de estafa, los ciberdelincuentes publicaban una noticia en la que había fotos y videos íntimos de famosos como Jenifer Lawrence, Ariana Grande, Kim Kardashian y hasta Shakira para la región de Latinoamérica. [2]

V. TIPOS DE INGENIERÍA SOCIAL

Los ataques de ingeniería social se dividen en dos, dependiendo del número de interacciones que debe realizar el ciberdelincuente:

A. Hunting

Este tipo de ataque intenta afectar al máximo número de usuarios teniendo una única comunicación. Son habituales en campañas de phishing, como las dirigidas a entidades energéticas o bancarias. Algunos ejemplos son:

- Ojo si recibes una devolución de Endesa, esto es phishing
- ¡Ten cuidado de no morder! Detectada campaña de phishing suplantando a Bankia
- Campaña de phishing suplantando al banco BBVA

También se utilizan en ataques dirigidos a realizar campañas de infección de malware, como las que realizan ataques de ransomware:

- Enviar presupuestos falsos como archivos adjuntos maliciosos en Excel
- Se ha detectado una oleada de correos con facturas para infectar tu ordenador.
- La nueva ola de ransomware afecta a varias computadoras.

B. Farming

En un ataque de Farming, los ciberdelincuentes entablan diversas comunicaciones con las víctimas hasta que logran su objetivo u obtienen la mayor cantidad de información posible. Algunos ejemplos de este tipo de ataques son aquellos que intentan infundir miedo a sus víctimas a través de videos supuestamente privados o futuros ataques a sus empresas:

- Campaña de correo electrónico chantajea a los llamados videos privados
- Ondas de correo electrónico que amenazan con atacar a su empresa

En otros casos, como el fraude de CEO o, más recientemente, el fraude de recursos humanos, los ciberdelincuentes se hacen pasar por miembros de la empresa y utilizan diferentes técnicas de ingeniería social para lograr sus objetivos:

- Fraude del director ejecutivo
- Fraude de recursos humanos [3]

VI. ESTADÍSTICAS DE ATAQUES DE INGENIERÍA SOCIAL

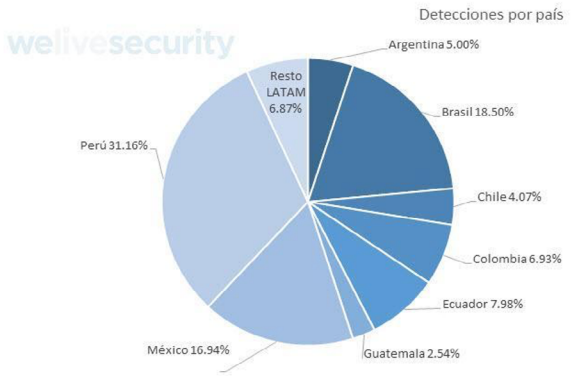

Fig 1. Imagen sobre las detecciones de ataques de ingeniería social en América Latina en 2020. [4]

Fig 2. Incremento de la Ingeniería Social en el año 2021 respecto a otros ciberataques. [5]

VII. PRINCIPIOS BÁSICOS DE LA INGENIERÍA SOCIAL

A. Respeto a la autoridad: Como regla general, nosotros, como trabajadores y ciudadanos en general, respetamos la autoridad de nuestros superiores, tanto dentro de nuestras organizaciones como en nuestra vida diaria. Este tipo de ataque se basa en nuestro respeto por los responsables y por autoridades como las Fuerzas de Seguridad Nacional y la Legión.

B. Voluntad de ayudar: Especialmente en un ambiente de trabajo, los empleados a menudo están dispuestos a ayudar a sus colegas en cualquier forma posible. Por este motivo, los ciberdelincuentes pueden hacerse pasar por empleados de la empresa. Otra variación utilizada es hacerse pasar por un técnico informático para instalar herramientas de acceso remoto no autorizadas.

C. Miedo a perder el servicio. Esta técnica se utiliza a menudo en campañas de phishing. Con el pretexto de repetidos accesos no autorizados, cambios de política o cualquier otro engaño, los ciberdelincuentes obligan a las víctimas a acceder a sitios web maliciosos, en donde se aprovechan para robar información.

D. Respeto Social: En algunos casos, las tácticas de los ciberdelincuentes se basan en el miedo de los usuarios a no ser aceptados por la sociedad o perder su reputación. Esto es común en los correos electrónicos de sextorsión, donde los ciberdelincuentes amenazan con publicar videos supuestamente privados que en realidad no existen.

E. Gratis: Este tipo de engaño se basa en ofrecer un producto o servicio gratuito a cambio de información privada. Este fraude suele llevarse a cabo a través de páginas web emergentes, que suelen aparecer al navegar por sitios web no legítimos. También es habitual en mensajes de redes sociales o apps de mensajería. [3]

VIII. ALGUNOS CIBERATAQUES DE INGENIERÍA SOCIAL

A. Phishing

En este tipo de ataque se utiliza el correo para enviar un mensaje que puede ofrecer un premio, solicitar la verificación del correo para evitar su cierre o simplemente solicitando datos personales, en busca que la víctima acceda a un enlace que

está relacionado en el mensaje, el cual dirige a un sitio web malicioso en donde los atacantes pueden obtener acceso a los datos del usuario. Normalmente los mensajes suplantan al remitente y se hacen pasar por algún jefe, si el entorno es laboral, o por organizaciones como bancos o entidades privadas que requieren algo con urgencia para que el receptor actúe sin pensar ni confirmar los datos.

B. Spear phishing

Este ataque es parecido al phishing; sin embargo, en este los ataques van dirigidos a empresas o personas especiales como gerentes, famosos, personas públicas o con poder, a los cuales buscan engañar a través de correos electrónicos para que accedan a enlaces maliciosos, así instalar un malware que permita acceder a información valiosa con la que causan mucho daño a las víctimas.

C. Vishing

Hace parte de la línea del phishing, pero en este tipo de ataque se usan llamadas y mensajes de voz, para engañar a las personas haciéndose pasar por alguien de confianza como personal de un banco, asesores de empresas con las que se tiene algún servicio o hasta un compañero de trabajo del área de tecnología o IT. Durante la llamada el atacante solicita información o datos privados haciendo preguntas con la excusa de mejorar sus servicios o ayudarle con algún inconveniente técnico.

D. Scareware

Es un malware que usan los ciberdelincuentes para asustar a las víctimas y hacerles creer que su computador o dispositivo está infectado con un virus al aparecer como ventana emergente, en la cual colocan información sobre cómo eliminar el virus que presenta el equipo. De esta manera, cuando las personas acceden al enlace, ingresan a un sitio web infectado que propicia la instalación del verdadero malware sin darse cuenta.

E. Scamming

Es similar al phishing de correo electrónico, pero en este se usan mensajes de texto SMS para enviar notificaciones, indicando que se han ganado un premio o que deben revisar algo importante de algún servicio que tengan. [6-9]

IX. MEDIDAS PARA PREVENIR LA INGENIERÍA SOCIAL

Debido a que, cada día los ciberdelincuentes son más capaces y diestros en técnicas de manipulación y engaño usando la ingeniería social, es demasiado importante que las personas del común se capacitan en seguridad informática y estén atentos a cualquier signo o intento de ingeniería social.

Las siguientes son algunas buenas prácticas que se pueden utilizar:

A. Tener mucho cuidado con la información personal que se comparte en la red, evitando que se filtre con personas desconocidas o en equipos públicos.

B. Configurar el correo de tal manera que no se reciban mensajes spam o correo no deseado en la bandeja de entrada, sino en la carpeta correspondiente de correo no deseado, así evitar acceder a enlaces maliciosos que contengan esos mensajes, los cuales pueden poner en riesgo los equipos y la información.

C. Tener una lista de correos legítimos de personas con las que se habla diaria o frecuentemente, así si se recibe un mensaje de parte de uno de ellos con otro correo o dirección electrónica desconocida, es una señal de alerta para tomar medidas.

D. Siempre dudar o desconfiar de correos electrónicos o mensajes de texto en los que

se ofrezcan premios o recompensas por una pequeña inversión.

E. Si se recibe un mensaje que sea de un remitente dudoso o desconocido, verificar su procedencia o consultar en internet alguna información importante que permita validar los datos o llamar directamente a la entidad que supuestamente se está comunicando.

F. Ante una llamada sospechosa, solicitar a la persona que llama que se identifique y tratar de obtener la mayor información.

G. Si se es una empresa, es muy importante que se implementen políticas de seguridad estrictas que permitan controlar los riesgos y las posibilidades de sufrir un ataque. Se recomienda el uso de contraseñas seguras y el correcto manejo de los activos de información. [6]

X. PRÁCTICA

Se procede a usar la herramienta llamada "zphisher" en el sistema operativo kali Linux se genera una URL de suplantación de Facebook para lograr obtener datos confidenciales el cual se asemeja a las campañas de pishing que realizan lo mismo buscando obtener datos en los formularios del portal web como lo son tarjetas de crédito, contraseñas entre otros.

El primer paso fue la instalación de la herramienta la cual se realiza con la ayuda de git clone:

Fig 3. Instalación Zphisher

Luego al iniciar la herramienta buscamos la opción que queremos atacar, para nuestro ejemplo sería el número 1 pues vamos a suplantar la web de Facebook:

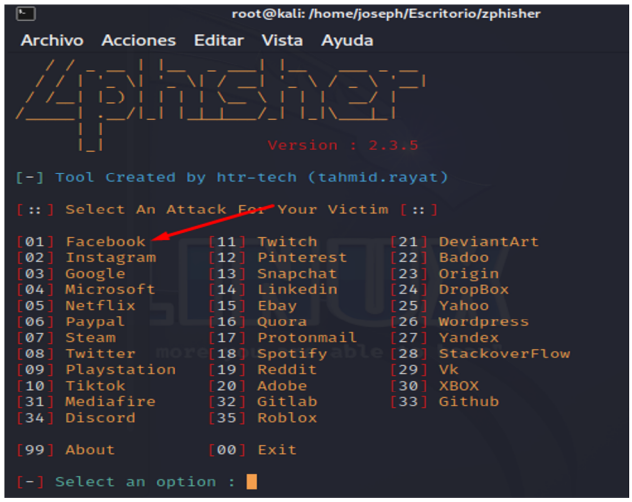

Fig 4. Seleccionar Facebook

A manera de ejemplo y al ser un laboratorio controlado escogemos la opción de localhost ya que no vamos a publicar la URL atacante en internet:

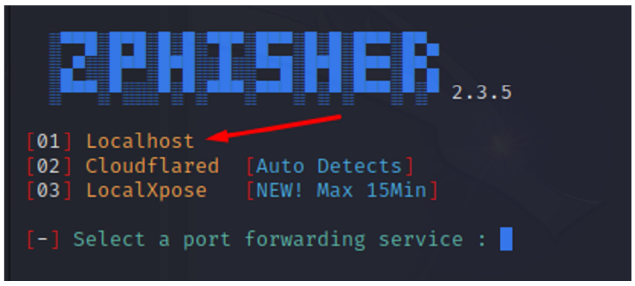

Fig 5. Seleccionar LocalHost

Con esto la herramienta nos entrega una URL falsa que será entregada a nuestra víctima:

Fig 6. Seleccionar URL falsa

Cuando la víctima ingresa a la URL el portal que vera será el mismo de Facebook e ingresará los datos:

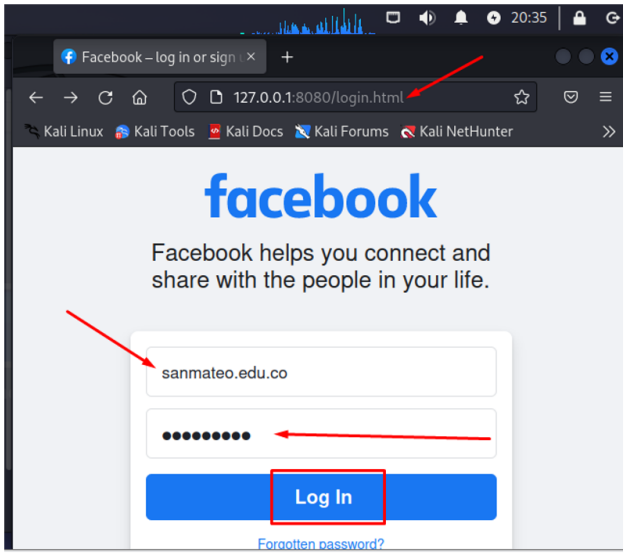

Fig 7. Interfaz facebook

Cuando finalice y de al botón “Login” la información se enviará y será capturada en nuestro servidor con la herramienta corriendo y nos mostrará en texto plano esta data: II. MÉTODO

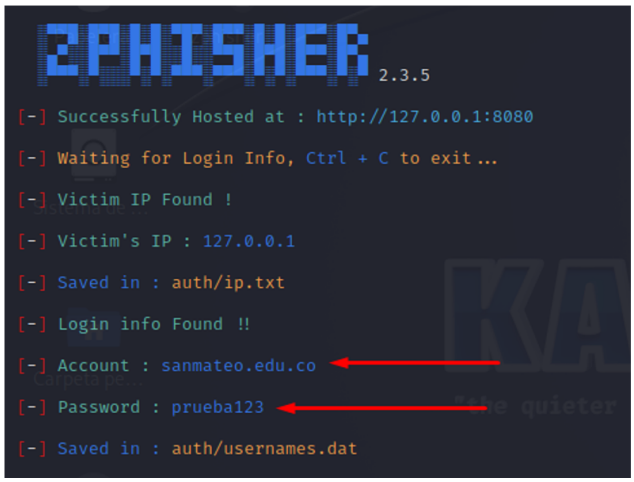

Fig 8. Dar ingreso

La metodología del trabajo anterior se basa en una revisión de la literatura para comprender la historia y los conceptos clave de la ingeniería social. Además, se utiliza un análisis de casos reales de ataques de ingeniería social para ilustrar los conceptos discutidos. También se incluye una demostración práctica en la que se utiliza la herramienta "zphisher" en un entorno de laboratorio controlado para crear una URL de suplantación de Facebook y capturar datos, lo que permite comprender cómo funcionan estos ataques en la práctica.

III. CONCLUSIONES

- La ingeniería social es una preocupación cada vez más importante en nuestra era digital. Conocer su historia, entender sus métodos y estar alerta ante posibles ataques nos permite proteger nuestra privacidad y seguridad. Es fundamental educarnos sobre los riesgos asociados con la ingeniería social y tomar medidas para salvaguardar nuestra información personal y organizacional.

- Se deben tomar medidas contra la ingeniería social como: concientizar, monitorear y capacitar con el fin de no caer en estos tipos de ataques.

- Con la velocidad y los avances tecnológicos que han permitido a los ciberdelincuentes ser cada vez más astutos en técnicas de manipulación a las personas, es demasiado importante conocer cómo funciona la ingeniería social, sus técnicas y diferentes ataques, para estar preparados y no caer en estafas.

REFERENCIAS

[1] Ymant Servicios Informáticos, "Ymant Servicios Informáticos," Dec. 13, 2022. [Online]. Available: https://www.ymant.com/blog/ingenieria-social/. [Accessed: Jun. 12, 2023].

[2] S. Pagnotta, "WeliveSecurity," Dec. 01, 2015. [Online]. Available: https://www.welivesecurity.com/la-es/2015/12/01/historias-de-ingenieria-social-ridiculas/. [Accessed: Jun. 12, 2023].

[3] INCIBE, "INCIBE - Instituto Nacional de Ciberseguridad," Sep. 05, 2019. [Online]. Available: https://www.incibe.es/empresas/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse. [Accessed: Jun. 13, 2023].

[4] L. Lubeck, "Welivesecurity," Jan. 07, 2021. [Online]. Available: https://www.welivesecurity.com/la-es/2021/01/07/2020-duplico-detecciones-ataques-ingenieria-social/. [Accessed: Jun. 13, 2023].

[5] J. M. Mesia, "Agenda tecnologia web," Feb. 27, 2021. [Online]. Available: https://agendatecnologicaweb.com/marsh-y-microsoft-ingenieria-social-o-phishing-es-el-ciberataque-que-mas-aumento-en-peru-a-raiz-de-la-pandemia/. [Accessed: Jun. 13, 2023].

[6] M. Jimenez, "Pirani Risk," Oct. 12, 2022. [Online]. Available: https://www.piranirisk.com/es/blog/ingenieria-social-ciberataques-y-prevencion?hs_amp=true&utm_term=&utm_campaign=Matriz+de+Riesgos+-+General+-+Julio+2022&utm_source=adwords&utm_medium=ppc&hsa_acc=9508207643&hsa_cam=17802451156&hsa_grp=138377008319&hsa_ad. [Accessed: Jun. 13, 2023].

[7] N. Cardeño Portela, E. J. Cardeño Portela, y E. Bonilla Blanchar, «TIC y transformación académica en las universidades», Región Científica, vol. 2, n.º 2, p. 202370, jul. 2023.

[8] M. Ripoll Rivaldo, «El emprendimiento social universitario como estrategia de desarrollo en personas, comunidades y territorios», Región Científica, vol. 2, n.º 2, p. 202379, jul. 2023.

[9] F. Machuca-Contreras, C. Canova-Barrios, y M. F. Castro, «Una aproximación a los conceptos de innovación radical, incremental y disruptiva en las organizaciones», Región Científica, vol. 2, n.º 1, p. 202324, ene. 2023.