Horizonte Académico
Revista Multidisciplinaria
Recibido: 08/01/2025 Aprobado: 18/02/2025

DOI: https://doi.org/10.70208/3007.8245.v5.n1.79

Análisis de la Ingeniería social utilizada en redes sociales: Técnicas más utilizadas, estadísticas y percepción en el casco urbano de la ciudad de Loja – Ecuador

Cristian Fabián Guerrero Espinosa
cristian.f.guerrero@unl.edu.ec
https://orcid.org/0009-0008-6778-8548
Universidad Nacional de Loja
Ecuador-Loja

John Jossimar Tucker Yépez
jtucker@unl.edu.ec
https://orcid.org/0009-0004-3429-2045
Universidad Nacional de Loja
Ecuador-Loja

RESUMEN

En un entorno digital cada vez más interconectado y en constante evolución, el ciberespacio ha experimentado un crecimiento exponencial en el uso de redes sociales, propiciando un terreno fértil para la propagación de ataques cibernéticos basados en ingeniería social, entendiéndose como técnicas sofisticadas de manipulación psicológica que aprovechan la confianza y falta de conocimiento de los cibernautas. La falta de comprensión de estas técnicas representa una amenaza significativa para la seguridad y privacidad de los usuarios tanto "on-line" como "off-line", dejando tanto a individuos como a organizaciones expuestos a riesgos muchas veces incuantificables, desde la filtración de datos o información confidencial hasta la vulneración de sistemas y cortes de servicios. Esta investigación tiene como objetivo principal analizar los mecanismos de la ingeniería social, evaluar su impacto y proponer estrategias de prevención y mitigación. Para ello, se realizó un estudio exhaustivo que combinó el análisis de casos de estudio, encuestas a usuarios, así como la revisión de la literatura académica relacionada al tema. Los resultados del presente trabajo de investigación buscan contribuir al conocimiento científico y práctico sobre la ingeniería social, sentando las bases para el desarrollo de programas de capacitación y herramientas tecnológicas que permitan a individuos y organizaciones blindarse de manera efectiva contra este tipo de amenazas. Al generar conciencia sobre los peligros y estrategias de prevención, este trabajo aspira a empoderar a los usuarios y mejorar sustancialmente la seguridad en el entorno digital en constante evolución.

Palabras clave: ciberseguridad, redes sociales, ciberespacio, ingeniería social, ciberataques

Analysis of social engineering used in social networks: Most common techniques, statistics, and perception in the urban area of Loja – Ecuador

ABSTRACT

In an increasingly interconnected and constantly evolving digital environment, cyberspace has experienced exponential growth in the use of social networks, creating a fertile ground for the proliferation of cyberattacks based on social engineering. These attacks involve sophisticated psychological manipulation techniques that exploit users' trust and lack of awareness. The lack of understanding of these techniques poses a significant threat to both online and offline security and privacy, leaving individuals and organizations exposed to often immeasurable risks, ranging from data breaches and confidential information leaks to system intrusions and service disruptions.This research aims to analyze the mechanisms of social engineering, assess its impact, and propose prevention and mitigation strategies. To achieve this, an in-depth study was conducted, combining case study analysis, user surveys, and a review of academic literature related to the topic. The findings of this research seek to contribute to both the scientific and practical understanding of social engineering, laying the groundwork for the development of training programs and technological tools that enable individuals and organizations to effectively safeguard themselves against such threats. By raising awareness of the dangers and prevention strategies, this study aspires to empower users and significantly enhance security in the ever-evolving digital landscape.

***Keywords**:* cybersecurity, social networks, cyberspace, social engineering, cyberattacks

INTRODUCCIÓN

En la era digital actual, la creciente interconexión y dependencia de las tecnologías de la información y la comunicación han transformado drásticamente la forma en que nos relacionamos, trabajamos y accedemos a la información.

El ciberespacio, ese entorno virtual donde convergen estas actividades digitales, se ha convertido en un campo fértil para nuevas oportunidades y emprendimientos, pero también en un entorno vulnerable a diversos factores de riesgo. Este artículo examina los aspectos críticos de la ingeniería social y los ciberataques. Se analizan los resultados de la investigación relacionados con estas temáticas, con el propósito de destacar la importancia de comprender, prevenir y mitigar los riesgos y amenazas asociados a la ingeniería social que afectan a los usuarios del ciberespacio.

Para contextualizar la relevancia de este tema, es importante destacar que, según datos recientes, los ciberataques han alcanzado cifras históricas, con pérdidas que suman 10.000 millones de euros en el 2024, doblando así las del año anterior, viéndolo de otra manera, si los cibercriminales se reunieran y formaran un país, fueran las tercera potencia económicamente hablando (Staff, 2024) , la introducción de la inteligencia artificial ha jugado un rol muy importante al hacer los ataques más precisos y personalizados, y la ingeniería social sigue siendo una técnica habitual, con métodos como el phishing o el vishing (Macchi, 2024).

Además, el 74% de todas las brechas de seguridad incluyen el elemento humano, lo que resalta la importancia de abordar las vulnerabilidades relacionadas con la ingeniería social (*101 de las últimas estadísticas de violaciones de datos para 2024*, s. f.).

Ingeniería social

La ingeniería social es el arte de la manipulación psicológica y la explotación de la confianza de las personas para la obtención de información confidencial o la ejecución de acciones no autorizadas. Los ciberdelincuentes en lugar de descubrir y explotar posibles vulnerabilidades tecnológicas emplean este arte para aprovecharse de las debilidades humanas como los sentimientos y la confianza para obtener

información o datos relevantes de personas declaradas como objetivo de ataque (Salahdine & Kaabouch, 2019) (*Las Redes Sociales: ¿Privacidad Al Descubierto?*, s. f.) (Chetioui et al., 2022).

El crecimiento del Internet y los avances tecnológicos han facilitado la comunicación e interacción entre seres humanos, volviéndola fácil e instantánea. Sin embargo, esta conveniencia también ha expuesto la información personal y sensible de cada usuario en la red, especialmente a través de las redes sociales. Lamentablemente, estas plataformas no siempre mantienen un nivel adecuado de seguridad, convirtiendo la información en un objetivo de gran interés para los ciberdelincuentes (Ariza et al., 2023) (Albladi & Weir, 2016) (Arenaldi, 2020).

Ciclo de vida típico de un ataque de ingeniería social

Los ataques de ingeniería social buscan establecer una conexión entre el atacante y la víctima, en donde el atacante intenta manipular a la víctima para que le entregue información sensible y se comprometa (Chetioui et al., 2022) (Gallegos-Segovia et al., 2017) (Alonso, 2020).

El ciclo de vida típico de un ataque ingeniería social está conformado por diversas etapas estratégicamente planificadas:

1) Definición: Es la etapa inicial, el atacante selecciona a la víctima, determina el objetivo del ataque y elabora un plan de ataque detallado.

2) Investigación: Siguiendo al plan establecido, el atacante estudia a su víctima con el fin de identificar posibles lazos de conexión y puntos de vulnerabilidad.

3) Enganche: Una vez recopilada la información necesaria, el atacante se acerca a su víctima, tratando de establecer una conexión y trabajando para ganarse su confianza de manera efectiva.

4) Juego: Con la confianza de la víctima asegurada, el atacante la manipula hábilmente hasta la consecución del objeto del ataque.

5) Salida: Finalmente, una vez logrado el objetivo del ataque, el atacante se retira, desapareciendo de la escena sin dejar rastro.

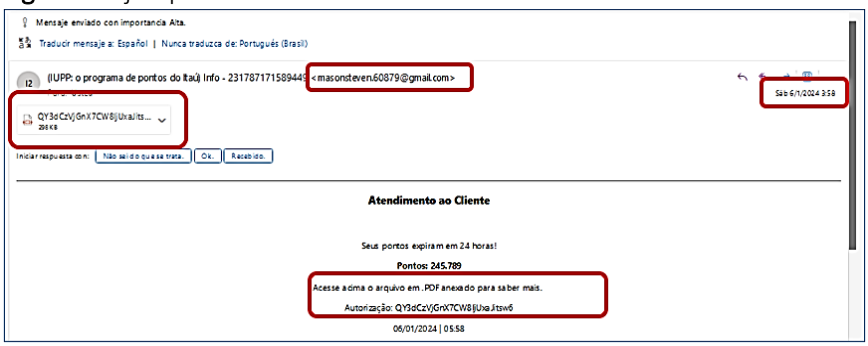
Ciberataques basados en ingeniería social social

Existen diferentes tipos de ciberataques basados en ingeniería social, a continuación, se analizarán los más utilizados y se presentan ejemplos de su aplicación:

Malware: Es un término que se usa para describir cualquier tipo de software malicioso, como spyware, ransomware, virus y gusanos. Este tipo de programas dañinos se infiltran en las redes, generalmente cuando un usuario hace click en enlaces o archivos adjuntos procedentes de correos electrónicos, mensajes de texto o redes sociales que no son de confianza (Cisco, 2024) (*New IoT-malware grew three-fold in H1 2018*, s. f.) (Gallegos-Segovia et al., 2017).

El malware puede llegar a bloquear el acceso a componentes clave de la red, llegando incluso a volver inoperativo el equipo afectado. Por lo tanto, los usuarios deben mantener una actitud cautelosa al interactuar con contenidos de procedencia desconocida, ya que esto puede derivar en la infección del sistema.

Figura 1: Ejemplo de malware



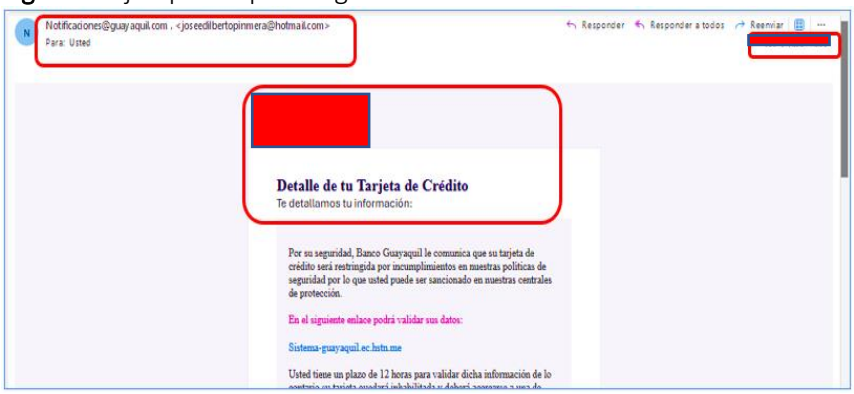
Fuente Autores

1. **Phishing**: Es una práctica fraudulenta que consiste en el envío de comunicaciones que aparentan provenir de fuentes confiables, generalmente a través de correos electrónicos. El objetivo principal de estos ataques es robar datos sensibles de los usuarios, como credenciales de inicio de sesión y números de tarjetas de crédito. Adicionalmente, los ataques de phishing también pueden tener como fin la instalación de malware en los dispositivos de las víctimas (Cisco, 2024) (Cisco, 2024) (Ariza et al., 2023).

Este tipo de engaños se aprovecha de la confianza de los usuarios en marcas y entidades conocidas para obtener información confidencial o acceder de manera no autorizada a sistemas y cuentas. Por lo tanto,

es crucial que los usuarios mantengan una actitud crítica y desconfíen de cualquier comunicación sospechosa, incluso si parece provenir de fuentes aparentemente legítimas (Ramzan, 2010) (Gupta et al., 2016).

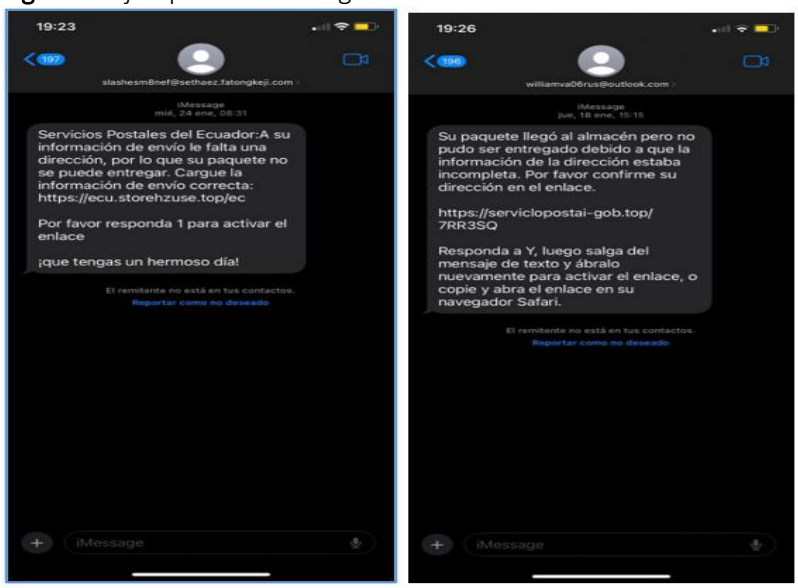
Figura 2: Ejemplo de phishing



Fuente: Autores

2. **Smishing:** Al igual que en los ataques de phishing, el objetivo del smishing es engañar a los usuarios para que revelen información confidencial o caigan en la instalación de malware. Estos mensajes de texto a menudo incluyen sistemas automatizados de respuesta que intentan persuadir a la víctima a que proporcione datos sensibles de manera inmediata (Balim & Gunal, 2019) (Kang et al., 2014).

Figura 3: Ejemplo de smishing –



fuente: Autores

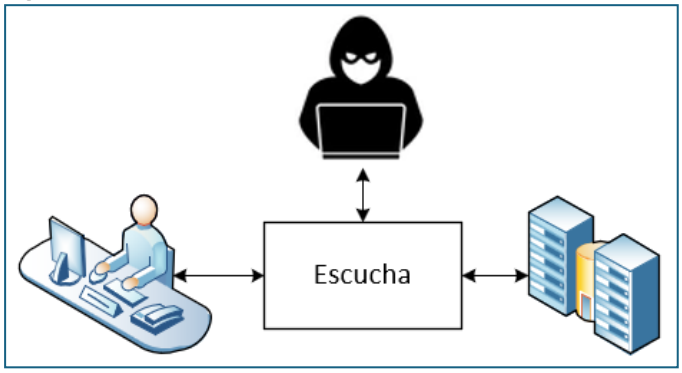
3. **Grooming:** Consiste en un proceso en el cual el atacante emplea una serie de tácticas y engaños para lograr un acercamiento con menores de edad, ganarse su confianza, y finalmente conseguir un encuentro físico con el objetivo de cometer abusos de naturaleza sexual. Este es un mecanismo sumamente dañino y manipulador que explota la vulnerabilidad de los niños y adolescentes. Implica un abuso de poder, confianza y autoridad por parte del atacante, quien utiliza trucos y mentiras para satisfacer sus propios intereses perversos (FGE-Ecuador, 2022) (Zambrano et al., 2019) (Michalopoulos & Mavridis, 2010).

Ejemplo: En mayo de 2022, después de seis meses de investigaciones, impulsados por la Fiscalía General del Estado ecuatoriano, se logró identificar al sujeto que se hacía pasar por mujer para obtener las fotografías de una menor de edad, quien denunció que el hombre la amenazaba sino enviaba dichas imágenes. En el celular del implicado se encontró material pornográfico (FGE-Ecuador, 2022).

4. **Ataque de intermediario:** Los ataques de intermediario, también conocidos como ataques de escucha (man-in-the-middle), ocurren cuando los ciberdelincuentes se insertan en las transacciones que se llevan a cabo entre dos partes. Una vez que los atacantes logran interrumpir el tráfico de comunicación, pueden filtrar los datos de interés y proceder a robarlos (Conti et al., 2016).

Este tipo de ataques se aprovecha de la confianza entre las partes que participan en la comunicación o transacción. Al posicionarse en el medio, los delincuentes pueden interceptar y manipular la información que se transmite, comprometiendo así la confidencialidad y la integridad de los datos.

Figura 4: Ejemplo de ataque intermediario



Fuente: Autores

5. **Ataque de denegación de servicio (DoS):** Tienen como objetivo saturar los sistemas, servidores o redes con un tráfico excesivo, con el fin de agotar los recursos y el ancho de banda disponibles. Como resultado de esta sobrecarga, el sistema no puede completar las solicitudes legítimas de los usuarios. Estos ataques representan una amenaza significativa, ya que pueden interrumpir el funcionamiento normal de sitios web, aplicaciones y servicios en línea, impactando gravemente la disponibilidad y accesibilidad para los usuarios legítimos (Pelechrinis et al., 2011).

En algunos casos, los atacantes utilizan múltiples dispositivos comprometidos, formando una red de equipos infectados conocida como botnet, para lanzar estos ataques de denegación de servicio a gran escala. Al emplear una gran cantidad de fuentes de tráfico malicioso, los ciberdelincuentes logran abrumar y colapsar los sistemas y servicios afectados.

Ejemplo: En octubre de 2021, el Banco de Pichincha, una importante institución financiera ecuatoriana, sufrió un ciberataque que impactó negativamente en parte de sus servicios. Como consecuencia del ataque, la página web del banco quedó inhabilitada temporalmente (Harán, s. f.).

Estadísticas de ciberdelitos en el cantón Loja

En la Tabla 1, se presenta la información proporcionada por la Dirección de Estadística y Sistemas de Información de la Fiscalía General del Estado ecuatoriano, referente a las Noticias del Delito (NDDs), relacionadas con ciberdelitos correspondientes al cantón Loja. El periodo analizado comprende desde enero de 2023 hasta marzo de 2024.

Tabla 1 Noticias del delito por año de registro en el cantón loja

Noticias del Delito	**Total 2023**	**Total Ene-Mar 2024**	**Total NDDs**	**Porcentaje**
Estafa	644	136	780	71.49 %
Suplantación de identidad	86	25	111	10.17 %
Violación a la intimidad	55	10	65	5.96 %
Apropiación fraudulenta por medios electrónicos	33	13	46	4.22 %
Acoso sexual	19	3	22	2.02 %

Hostigamiento	17	2	19	1.74 %
Actos lesivos a la propiedad intelectual	6	3	9	0.82 %
Terrorismo	4	4	8	0.73 %
Transferencia electrónica de activo patrimonial	5	2	7	0.64 %
Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	5	1	6	0.55 %
Interceptación ilegal de datos	0	6	6	0.55 %
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	0	5	5	0.46 %
Pornografía con utilización de niñas, niños o adolescentes	3	0	3	0.27 %
Aprovechamiento ilícito de servicios públicos	1	1	2	0.18 %
Falsificación informática	1	0	1	0.09 %
Revelación de secreto o información personal de terceros	1	0	1	0.09 %
Total Noticias Del Delito:	880	211	1 091	100.00 %

Los datos del cantón Loja revelan una predominancia de ciberdelitos estrechamente vinculados con la ingeniería social. Las estafas en línea representan el 71.49% de los casos, seguidas por la suplantación de identidad (10.17%), la violación a la intimidad (5.96%), la apropiación fraudulenta por medios electrónicos (4.22%) y el acoso sexual (2.02%). Estos crímenes evidencian el uso de técnicas de manipulación psicológica basadas en la ingeniería social, que buscan explotar la información personal de los usuarios en redes sociales. La alta incidencia de estos delitos subraya la urgente necesidad de fortalecer la educación en ciberseguridad y la concienciación sobre las tácticas de ingeniería social entre los usuarios, lo cual podría tener un impacto significativo en la reducción de la ciberdelincuencia en la región.

MATERIALES Y MÉTODOS

Para el desarrollo del presente proyecto de investigación se utilizó la metodología de avance por fases, definiendo tres fases, las cuales se detallan a continuación:

- **Fase inicial:** Comprendió la investigación y recopilación de información esencial para el desarrollo del proyecto. Para la ejecución de esta fase, se llevó a cabo el análisis de artículos, publicaciones científicas y notas periodísticas con el objetivo de obtener la mayor cantidad de información y, a partir de esto se generaron aportes fundamentados.
- **Fase de Desarrollo:** En esta etapa se ejecutaron encuestas, físicas y en línea, a la población urbana de la ciudad de Loja, que permitió determinar la eficacia de la aplicación de las técnicas más utilizadas de ingeniería social y establecer el nivel de conciencia y conocimiento sobre la posible vulneración de información personal en redes sociales.
- **Fase final:** Se ejecutó el análisis de los resultados obtenidos de las encuestas realizadas. Con base en este análisis, se propuso estrategias adecuadas para la prevención y mitigación de ataques relacionados a la aplicación de la ingeniería social en redes sociales.

Con el empleo de esta metodología se integró la investigación teórica, la recopilación de datos empíricos y la evaluación práctica para proporcionar un análisis completo de la ingeniería social en el contexto de las redes sociales, con el objetivo final de contribuir al conocimiento y fortalecer las defensas contra este tipo de amenazas.

Aspectos de interés

Para la ejecución de las encuestas, se definió un formato que aborda los siguientes aspectos fundamentales:

¿Cuál es el sexo y la edad de la persona encuestada?

¿Tiene conocimiento sobre el ciberespacio?

¿Se considera miembro activo en el ciberespacio?

¿Qué tiempo promedio se encuentra en línea y cuál es la actividad que realiza?

¿Sabe lo que son las redes sociales? ¿Qué cantidad de redes sociales posee?

¿Las credenciales o preguntas para acceso a sus redes sociales están relacionadas con algún familiar, fecha especial, color favorito, comida favorita, mascotas, o algún tópico personal?

¿Alguna vez ha configurado la privacidad de su información personal, laboral, fotos y publicaciones que comparte en sus redes sociales?

¿Alguna vez el usuario se ha sentido interrogado, acosado o intimidado por personas desconocidas en redes sociales? ¿Se atrevió a denunciar este comportamiento?

¿Cree haber sido víctima de algún ciberataque?

¿Alguna vez ha hecho click en enlaces enviados por personas desconocidas?

¿Alguna vez perdió el control o acceso a algunas de sus redes sociales?

¿Tiene conocimiento sobre la ingeniería social?

¿Ha sido capacitado en temas relacionados a la seguridad informática, seguridad de la información o ciberseguridad? ¿Cuándo fue la última vez que fue capacitado?

De esta manera, el cuestionario busca recopilar información relevante sobre el nivel de conocimiento, participación y experiencias de los usuarios en el ciberespacio y las redes sociales, con el objetivo de analizar su grado de conocimiento, exposición y vulnerabilidad ante posibles amenazas de ingeniería social.

La recolección de datos mediante encuestas se llevó a cabo en la zona urbana de Loja, abarcando las parroquias El Sagrario, Sucre, El Valle, San Sebastián, Punzara y Carigan. Según datos del Instituto Nacional de Estadística y Censos (INEC, 2023), la población urbana de Loja asciende a 203,496 habitantes.

Para garantizar la representatividad estadística de la muestra con respecto a la población total, se utilizó la fórmula para población finita. Como resultado de este cálculo, se determinó que el tamaño mínimo de la muestra debía ser de 384 participantes. En la presente investigación, se aplicaron un total de 390 encuestas, lo que asegura la validez de los datos obtenidos.

La recolección de información se realizó durante el mes de mayo de 2024, empleando dos modalidades de aplicación: 136 encuestas en formato digital y 254 encuestas de manera presencial, logrando así un total de 390 muestras.

Dado que la población objetivo está conformada por residentes urbanos de Loja con acceso a redes sociales y una distribución demográfica similar, se utilizó la fórmula de margen de error para poblaciones finitas, considerando un nivel de confianza del 95 % y una proporción esperada del 50 %.

Aplicando la siguiente ecuación:

$$ME = Z \times \sqrt{\frac{P\,(1-P)}{n}}$$

Donde:

ME= Margen de error.

Z= 1.96 (para un nivel de confianza del 95%)

P= 0.5 (máxima variabilidad)

N= 390 (tamaño de la muestra)

Se obtiene un *margen de error de aproximadamente ±5 %,* lo que garantiza una precisión estadística aceptable dentro de los estándares de investigación.

Consistencia interna y confiabilidad de la encuesta

Para evaluar la confiabilidad de los instrumentos de medición, se realizó un análisis de consistencia interna mediante la prueba de *Alfa de Cronbach*, cuyos resultados se detallan a continuación:

Preguntas clave sobre Ingeniería Social:

Se obtuvo un Alfa de Cronbach de 0.7460, lo que indica un nivel de consistencia interna aceptable. Este resultado refleja que los ítems dentro de esta categoría están alineados y miden de manera coherente el constructo subyacente, garantizando la fiabilidad de los datos recopilados.

Totalidad de las preguntas de la encuesta:

Se obtuvo un Alfa de Cronbach de 0.6718. Si bien este valor es ligeramente inferior, aún representa un nivel de confiabilidad válido y utilizable, lo que sugiere que el cuestionario en su conjunto mantiene una

correlación adecuada entre sus ítems, aunque con oportunidades de mejora en términos de precisión y alineación temática.

Estos resultados certifican que la encuesta utilizada en esta investigación cumple con estándares aceptables de fiabilidad, proporcionando datos sólidos y coherentes para el análisis de la percepción de la población urbana de Loja frente a las amenazas de ingeniería social en redes sociales.

RESULTADOS Y DISCUSIÓN

De las a 390 personas encuestadas, 168 (43.1 %) son de sexo femenino y 222 (56.9 %) corresponden a sexo masculino y la categoría de edad se distribuye de la siguiente manera:

- 262 (67.2 %) Adultos menores (20 a 59 años).
- 75 (19.2 %) Adolescente (12 a 19 años).
- 53 (13.6 %) Adultos mayores (mayores a 60 años).

En los resultados se establece que 250 personas (64.1 %) conocen lo que es el ciberespacio, mientras que 140 (35.9 %) no. De las 250 personas que tienen conocimiento sobre el ciberespacio, 234 (93.6 %) se consideran miembros activos, mientras que 16 (6.4 %) personas no se consideran así. No obstante, entre las 140 personas que desconocen sobre el ciberespacio, 18 se consideran miembros activos.

El 69.3 % de los adolescentes (52), el 60.7 % de los adultos menores (159) y el 43.4 % de los adultos mayores (23) saben lo que es el ciberespacio y se consideran miembros activos.

En total, 252 personas se consideran miembros activos en el ciberespacio, representando el 64.6 % de las personas encuestadas.

El tiempo promedio que las personas encuestadas se encuentran en línea o hacen uso de Internet es de 6 horas y 17 minutos al día. A continuación, se muestran los resultados para cada grupo de interés:

Desglose por sexo:

- Para el sexo masculino el tiempo promedio al día es: 6 horas con 15 minutos.
- Para el sexo femenino el tiempo promedio al día es: 6 horas con 21 minutos.

Desglose por grupos de edad:

- Para los adolescentes el tiempo promedio al día es: 7 horas con 20 minutos.

- Para los adultos menores el tiempo promedio al día es: 6 horas con 28 minutos.
- Para los adultos mayores el tiempo promedio al día es: 3 horas con 57 minutos.

Entre las principales actividades a las cuales las personas dedican su tiempo en línea son:

- Redes sociales y comunicación (76.7 %).
- Educación y aprendizaje (54.6 %).
- Actividades de entretenimiento (51 %).
- Trabajo (32.6 %).
- Otras: Programación y diseño, juegos en línea, trading, etc. (1.2 %)

En cuanto a redes sociales, el 99 % de las personas sabe lo que son las redes sociales, solamente 4 personas no tienen el conocimiento. Los resultados indican que:

- 197 personas (50.5 %) tienen de 1 a 3 redes sociales.
- 150 personas (38.5 %) tienen de 3 a 5 redes sociales.
- 43 personas (11 %) poseen más de 5 redes sociales.

El 83,1 % (324 personas) relacionan sus credenciales o preguntas de acceso a sus redes sociales con tópicos personales. Analizando por grupo de interés:

Desglose por sexo:

- El sexo femenino las relaciona en un: 86.3 % (145 personas).
- El sexo masculino las relaciona en un: 80.6 % (179 personas).

Desglose por grupos de edad:

- Los adolescentes las relaciona en un: 85.3 % (64 personas).
- Los adultos menores las relaciona en un: 82.1 % (215 personas).
- Los adultos mayores las relaciona en un: 84.9 % (45 personas).

El 69,2 % (270 personas) han configurado o realizado ajustes en las opciones de privacidad de sus redes sociales. Analizando por grupo de interés:

Desglose por sexo:

- El sexo femenino: 66.7 % (112 personas).

- El sexo masculino: 71.2 % (158 personas).

Desglose por grupos de edad:

- Los adolescentes: 69.3 % (52 personas).
- Los adultos menores: 80.5 % (211 personas).
- Los adultos mayores: 13.2 % (7 personas).

El porcentaje de personas que se han sentido interrogados, acosados o intimidados por personas desconocidas en sus redes sociales es de 41.5 % (162 personas). Analizando por grupo de interés. Analizando por grupo de interés:

Desglose por sexo:

- El sexo femenino: 51.8 % (87 personas).
- El sexo masculino: 33.8 % (75 personas).

Desglose por grupos de edad:

- Adolescentes: 56 % (42 personas).
- Adultos menores: 37.4 % (98 personas).
- Adultos mayores: 41.5 % (22 personas).

De las 162 personas que indican haberse sentido interrogados, acosados o intimidados el 32.7 % (53 personas) se atrevió a denunciar de manera formal este tipo de comportamiento. Analizando por grupo de interés. Analizando por grupo de interés:

Desglose por sexo:

- Sexo femenino: 33.3 % (29 personas).
- Sexo masculino: 32 % (24 personas).

Desglose por grupos de edad:

- Adolescentes: 19 % (8 personas).
- Adultos menores: 43.9 % (43 personas).
- Adultos mayores: 9.1 % (2 personas).

De todas las muestras obtenidas, el 35.6 % (139 personas) cree que pudo haber sido víctima de un ataque cibernético. Analizando por grupo de interés:

Desglose por sexo:

- Sexo femenino: 41.7 % (70 personas).
- Sexo masculino: 31.1 % (69 personas).

Desglose por grupos de edad:

- Adolescentes: 48 % (36 personas).
- Adultos menores: 30.5 % (80 personas).
- Adultos mayores: 43.4 % (23 personas).

Los resultados indican que el 40.5 % (158 personas) ha hecho click en enlaces compartidos por personas desconocidas. Analizando por grupo de interés:

Desglose por sexo:

- Sexo femenino: 39.3 % (66 personas).
- Sexo masculino: 41.4 % (92 personas).

Desglose por grupos de edad:

- Adolescentes: 42.7 % (32 personas).
- Adultos menores: 38.2 % (100 personas).
- Adultos mayores: 49.1 % (26 personas).

El 43.6 % (170 personas) de las personas encuestadas reportan haber perdido el control o acceso a sus redes sociales. Analizando por grupo de interés:

Desglose por sexo:

- Sexo femenino: 49.4 % (83 personas).
- Sexo masculino: 39.2 % (87 personas).

Desglose por grupos de edad:

- Adolescentes: 48 % (36 personas).
- Adultos menores: 42 % (110 personas).

- Adultos mayores: 45.3 % (24 personas).

Respecto a ingeniería social, solamente el 17.9 % (70 personas) tiene conocimiento, mientras que el 82.1 % (320 personas) no. El desglose por grupos de edad que sabe lo que es la ingeniería social se conforma de la siguiente manera: El 16.0 % de los adolescentes (12 personas), el 21.0 % de los adultos menores (55 personas) y el 5.7 % correspondiente a los adultos mayores (3).

Finalmente, el 35.6 % (139 personas) del total de las personas encuestadas ha recibido capacitación en temas referentes a seguridad informática, seguridad de la información o ciberseguridad, mientras que el 64.4 % (251 personas) no. Analizando por grupo de interés:

Desglose por sexo:

- Sexo femenino: 35.7 % (60 personas).
- Sexo masculino: 35.6 % (79 personas).

Desglose por grupos de edad:

- Adolescentes: 38.7 % (29 personas).
- Adultos menores: 39.3 % (103 personas).
- Adultos mayores: 13.2 % (7 personas).

De las 139 personas que afirman haber sido capacitadas:

- 19.48 % (27 personas) recibieron capacitación en un periodo menor a 6 meses.
- 30.9 % (43 personas) en un periodo menor a 1 año.
- 45.3 % (63 personas) fueron capacitadas hace más de un año.

Existen 6 personas (4.3 %) que afirmaron haber sido capacitadas en temas relacionados, sin embargo, respondiendo “nunca” en la encuesta.

Discusión de resultados

Los resultados expuestos anteriormente brindan una perspectiva reveladora sobre el impacto de las técnicas de ingeniería social en la seguridad de la información y la privacidad de los usuarios de redes sociales en la zona urbana de Loja. Los datos recopilados respaldan la hipótesis planteada inicialmente, la cual establece que un bajo nivel de conciencia y conocimiento sobre las técnicas empleadas en la

ingeniería social se correlaciona con una mayor exposición y vulnerabilidad a los ciberataques en plataformas sociales en línea.

En primer lugar, los resultados muestran un alto grado de desconocimiento generalizado sobre el concepto de "ingeniería social", con solo el 17.9 % de los encuestados afirmando conocerlo. Esto sugiere una falta de concienciación significativa en la población estudiada, lo cual podría facilitar la efectividad de los ataques basados en estas técnicas.

En consecuencia, debido a la falta de conocimiento, los datos revelan que un porcentaje considerable de los encuestados (35.6 %) cree haber sido víctima de un ciberataque, lo cual podría estar relacionado con técnicas basadas en ingeniería social como el phishing o la suplantación de identidad. Además, el 41.5 % reportó haber sido interrogado, acosado o intimidado por desconocidos en redes sociales, un comportamiento que a menudo se utiliza en ataques de ingeniería social para obtener información sensible o comprometer las cuentas de los usuarios.

Otro hallazgo preocupante es que el 43.6 % de los encuestados perdió en algún momento el control o acceso a sus redes sociales, lo cual podría ser consecuencia de cuentas comprometidas mediante técnicas de ingeniería social. Estos resultados respaldan la premisa de que un bajo nivel de conciencia sobre estas amenazas conduce a una mayor exposición y vulnerabilidad, como se planteó en la hipótesis inicial.

Además, los datos obtenidos sugieren que las técnicas de ingeniería social han demostrado ser efectivas al engañar a los usuarios. Por ejemplo, el 40.5 % de la población encuestada admitió haber hecho “click” en enlaces compartidos por personas o usuarios desconocidos, una práctica comúnmente explotada en ataques basados en ingeniería social. Asimismo, el 83.1 % relaciona sus credenciales con datos personales, lo que facilita los ataques basados en pretextos o manipulación psicológica.

Es preocupante que, a pesar del alto riesgo de exposición y las consecuencias negativas reportadas, solo el 35.6 % de los encuestados ha recibido capacitación en seguridad informática o ciberseguridad. Esto refuerza la idea de que un conocimiento limitado sobre estrategias preventivas aumenta la propensión a sufrir impactos adversos en la seguridad y privacidad, como se proyectó en la hipótesis.

Un aspecto positivo para destacar es que el 69.2 % de los encuestados ha configurado las opciones de privacidad en sus redes sociales, lo cual mitiga parcialmente los riesgos asociados con la ingeniería social. Sin embargo, estas medidas pueden ser insuficientes si no se complementan con una comprensión sólida de las amenazas en línea.

En general, los resultados obtenidos respaldan la hipótesis planteada y subrayan la necesidad urgente de abordar la falta de conciencia y conocimientos sobre las técnicas basadas en ingeniería social en la población estudiada. La investigación ha demostrado una correlación clara entre el bajo nivel de conciencia y la mayor exposición y vulnerabilidad a ciberataques en redes sociales, lo que resalta la importancia de implementar programas de concientización y capacitación para mitigar estos.

CONCLUSIONES

Esta investigación ha expuesto la problemática de la ingeniería social y su impacto en la seguridad de la información y privacidad de los usuarios de redes sociales en la zona urbana de Loja. A partir de los hallazgos obtenidos, se pueden extraer las siguientes conclusiones principales:

- Existe un bajo nivel de conciencia generalizado en la población estudiada sobre las técnicas de ingeniería social y sus implicaciones en la seguridad de la información que comparten los usuarios en sus redes sociales. Únicamente el 17.9 % de los encuestados afirmó conocer el concepto, lo que representa una vulnerabilidad significativa ante estas amenazas.
- La falta de conocimientos sobre la ingeniería social se correlaciona directamente con una mayor exposición y vulnerabilidad a ciberataques en redes sociales, tal como se planteó en la hipótesis inicial. Los datos revelan altos porcentajes de usuarios que han sido víctimas de acoso, interrogatorios, pérdida de control de cuentas y posibles ataques cibernéticos.
- Las técnicas de ingeniería social como el phishing, suplantación de identidades y la manipulación psicológica han demostrado ser altamente efectivas para engañar a los usuarios, aprovechando prácticas inseguras como hacer “click” en enlaces de usuarios desconocidos o utilizar información personal como credenciales.

- A pesar de los riesgos evidentes, una gran mayoría de los encuestados (64.4 %) no ha recibido capacitación en temas de seguridad informática o ciberseguridad, lo que perpetúa el ciclo de vulnerabilidad y exposición a amenazas relacionadas con la ingeniería social.
- Si bien algunos usuarios han implementado medidas básicas de privacidad en sus redes sociales, estas acciones aisladas son insuficientes para mitigar los riesgos si no se complementan con una comprensión profunda de las amenazas y las prácticas de seguridad.
- Los resultados sugieren una necesidad de implementar programas de concientización y capacitación enfocados en la ingeniería social, sus técnicas y métodos de prevención. Esto permitiría empoderar a los usuarios con los conocimientos necesarios para identificar y mitigar estos ataques, fortaleciendo así la seguridad de la información y la privacidad de los usuarios en el entorno de las redes sociales.

Finalmente, esta investigación ha logrado cumplir con los objetivos planteados, proporcionando una descripción detallada de las técnicas de ingeniería social más utilizadas en ataques a redes sociales, analizando su impacto en la población estudiada y evaluando el nivel de conciencia y conocimientos existentes. Los hallazgos resaltan la importancia crítica de abordar esta problemática mediante la implementación de estrategias efectivas de concientización y capacitación, con el fin de fortalecer la seguridad digital y salvaguardar la privacidad de los usuarios en plataformas en línea.

Recomendaciones

Teniendo como base los hallazgos obtenidos en esta investigación y las conclusiones derivadas, se formulan las siguientes recomendaciones con el objetivo de fortalecer la seguridad de la información y la privacidad de los usuarios de redes sociales frente a las amenazas de la ingeniería social:

- Implementar programas de concientización y capacitación obligatorios sobre ingeniería social, dirigidos a todos los segmentos de la población, con especial énfasis en grupos vulnerables como adolescentes y adultos mayores. Estos programas deben estar diseñados por expertos en ciberseguridad y abordar temas como técnicas de ingeniería social comunes, posibles ataques,

identificación de amenazas, mejores prácticas de seguridad y protección de la privacidad en redes sociales.

- Promover la educación en seguridad cibernética desde etapas tempranas, incorporando contenidos relacionados con la ingeniería social y la protección de la información en los planes de estudio de instituciones educativas de todos los niveles. Esto sentará las bases para una cultura de seguridad sólida y fomentará la adopción de hábitos seguros desde una edad temprana.
- Desarrollar campañas de sensibilización masivas, utilizando diversos canales de comunicación, como redes sociales, medios tradicionales y plataformas digitales, para difundir información relevante sobre ingeniería social, sus riesgos y estrategias de mitigación. Estas campañas deben ser diseñadas con un enfoque atractivo y accesible para el público general.
- Fomentar la colaboración entre autoridades gubernamentales, organizaciones de ciberseguridad, empresas de tecnología y la sociedad civil para establecer un marco regulatorio y normativo que aborde de manera integral la problemática de la ingeniería social en el entorno digital. Este marco debe contemplar medidas preventivas, protocolos de respuesta ante incidentes y mecanismos de denuncia y sanción para los perpetradores de estos ataques.
- Incentivar a las empresas y organizaciones públicas y privadas a implementar políticas y controles de seguridad robustos, incluyendo la capacitación periódica de sus empleados en temas de ingeniería social y la adopción de tecnologías de seguridad avanzadas, como soluciones de detección y prevención de amenazas basadas en inteligencia artificial y aprendizaje autónomo o redes neuronales.
- Promover la investigación continua en el campo de la ingeniería social, con el fin de mantenerse al tanto de las técnicas emergentes y desarrollar estrategias de mitigación efectivas. Esta investigación debe ser multidisciplinaria, involucrando a expertos en ciberseguridad, psicología, sociología y otras áreas relevantes.
- Fomentar la adopción de buenas prácticas de seguridad por parte de los usuarios de redes sociales, como el uso de contraseñas robustas, la activación de la autenticación robusta o multifactor,

la configuración adecuada de las opciones de privacidad y la verificación de la identidad de los contactos antes de compartir información sensible.

- Alentar a las plataformas de redes sociales a implementar medidas de seguridad más estrictas, como la detección y bloqueo automático de cuentas sospechosas, la verificación de identidad de los usuarios y la implementación de controles de seguridad avanzados para proteger la privacidad y la integridad de los datos.

La implementación efectiva de estas recomendaciones requerirá de un esfuerzo coordinado y sostenido por parte de todos los actores involucrados, incluyendo autoridades gubernamentales, políticas públicas, organizaciones de ciberseguridad, empresas de tecnología, instituciones educativas y la sociedad civil. Solo mediante un enfoque integral y proactivo podremos mitigar los riesgos asociados con la ingeniería social y fortalecer la seguridad de la información y la privacidad en el entorno digital.

REFERENCIAS BIBLIOGRÁFICAS

101 de las últimas estadísticas de violaciones de datos para 2024. (s. f.). Secureframe. Recuperado 19 de marzo de 2025, de https://secureframe.com/blog/data-breach-statistics

Albladi, S., & Weir, G. R. S. (2016). Vulnerability to social engineering in social networks: A proposed user-centric framework. *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, 1-6. https://doi.org/10.1109/ICCCF.2016.7740435

Alonso, R. (2020, diciembre 9). *Timo del CEO: El ciberataque con el que se roban millones haciendo una sola llamada*. Diario ABC. https://www.abc.es/tecnologia/redes/abci-timo-ciberataque-roban-millones-haciendo-sola-llamada-202012090135_noticia.html

Arenaldi, S. (2020). *Las Redes Sociales como nuevo espacio público: Su impacto y efecto en la sociedad actual*. http://repositorio.unab.cl/xmlui/handle/ria/17837

Ariza, M., Azambuja, A. J. G. de, Nobre, J. C., & Granville, L. Z. (2023). Automated Social Engineering Attacks using ChatBots on Professional Social Networks. *Workshop de Gerência e Operação de Redes e Serviços (WGRS)*, 43-56. https://doi.org/10.5753/wgrs.2023.747

Balim, C., & Gunal, E. S. (2019). Automatic Detection of Smishing Attacks by Machine Learning Methods. *2019 1st International Informatics and Software Engineering Conference (UBMYK)*, 1-3. https://doi.org/10.1109/UBMYK48245.2019.8965429

Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of Social Engineering Attacks on Social Networks. *Procedia Computer Science*, *198*, 656-661. https://doi.org/10.1016/j.procs.2021.12.302

Cisco. (2024). *Productos y soluciones de seguridad de Cisco*. Cisco. https://www.cisco.com/site/mx/es/products/security/index.html

Conti, M., Dragoni, N., & Lesyk, V. (2016). A Survey of Man In The Middle Attacks. *IEEE Communications Surveys & Tutorials*, *18*(3), 2027-2051. IEEE Communications Surveys & Tutorials. https://doi.org/10.1109/COMST.2016.2548426

FGE-Ecuador. (2022). *Fiscalía General del Estado | Fiscalía procesa a detenido por el delito de 'grooming'*. https://www.fiscalia.gob.ec/fiscalia-procesa-a-detenido-por-el-delito-de-grooming/

Gallegos-Segovia, P. L., Bravo-Torres, J. F., Larios-Rosillo, V. M., Vintimilla-Tapia, P. E., Yuquilima-Albarado, I. F., & Jara-Saltos, J. D. (2017). Social engineering as an attack vector for ransomware. *2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)*, 1-6. https://doi.org/10.1109/CHILECON.2017.8229528

Gupta, S., Singhal, A., & Kapoor, A. (2016). A literature survey on social engineering attacks: Phishing attack. *2016 International Conference on Computing, Communication and Automation (ICCCA)*, 537-540. https://doi.org/10.1109/CCAA.2016.7813778

Harán, J. (s. f.). *Banco Pichincha sufrió ataque informático que afectó parte de sus servicios*. Recuperado 13 de marzo de 2025, de https://www.welivesecurity.com/la-es/2021/10/14/banco-pichincha-sufrio-ataque-informatico/

Kang, A., Dong Lee, J., Kang, W. M., Barolli, L., & Park, J. H. (2014). Security Considerations for Smart Phone Smishing Attacks. En H. Y. Jeong, M. S. Obaidat, N. Y. Yen, & J. J. (Jong H. Park (Eds.),

Advances in Computer Science and its Applications (pp. 467-473). Springer. https://doi.org/10.1007/978-3-642-41674-3_66

Las Redes Sociales: ¿Privacidad Al Descubierto? (s. f.). Recuperado 13 de marzo de 2025, de https://ideas.repec.org/a/erv/coccss/y2012i2012-0718.html

Macchi, F. (2024, diciembre 31). *2024 bate récords históricos en ciberataques, que con ayuda de la IA son cada vez más precisos*. El País. https://elpais.com/tecnologia/2024-12-31/2024-bate-records-historicos-en-ciberataques-que-con-ayuda-de-la-ia-son-cada-vez-mas-precisos.html

Michalopoulos, D., & Mavridis, I. (2010). Towards risk based prevention of grooming attacks. *2010 International Conference on Security and Cryptography (SECRYPT)*, 1-4. https://ieeexplore.ieee.org/abstract/document/5741645

New IoT-malware grew three-fold in H1 2018. (s. f.). Recuperado 12 de marzo de 2025, de https://www.kaspersky.com/about/press-releases/new-iot-malware-grew-three-fold-in-h1-2018

Pelechrinis, K., Iliofotou, M., & Krishnamurthy, S. V. (2011). Denial of Service Attacks in Wireless Networks: The Case of Jammers. *IEEE Communications Surveys & Tutorials*, *13*(2), 245-257. IEEE Communications Surveys & Tutorials. https://doi.org/10.1109/SURV.2011.041110.00022

Ramzan, Z. (2010). Phishing Attacks and Countermeasures. En P. Stavroulakis & M. Stamp (Eds.), *Handbook of Information and Communication Security* (pp. 433-448). Springer. https://doi.org/10.1007/978-3-642-04117-4_23

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11*(4), Article 4. https://doi.org/10.3390/fi11040089

Staff, F. (2024, junio 1). *Cibercrimen: La tercera economía del mundo, solo por detrás de Estados Unidos y China*. Forbes Colombia. https://forbes.co/2024/06/01/actualidad/cibercrimen-la-tercera-economia-del-mundo-solo-por-detras-de-estados-unidos-y-china/

Zambrano, P., Torres, J., Tello-Oquendo, L., Jácome, R., Benalcázar, M. E., Andrade, R., & Fuertes, W. (2019). Technical Mapping of the Grooming Anatomy Using Machine Learning Paradigms: An

Information Security Approach. *IEEE Access*, *7*, 142129-142146. IEEE Access. https://doi.org/10.1109/ACCESS.2019.2942805