Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), enero-febrero 2024,
Volumen 8, Número 1.

https://doi.org/10.37811/cl_rcm.v8i1

ANÁLISIS DE LOS ATAQUES DE INGENIERÍA SOCIAL EN ECUADOR

ANALYSIS OF SOCIAL ENGINEERING ATTACKS IN ECUADOR

Carlos Santiago Garzón Ibarra
Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional del Ecuador

Christian Andrés Navas Tapia
Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional del Ecuador

Angélica María Illicachi Tene
Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional del Ecuador

Rocío Janeth Espinoza Toapanta
Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional del Ecuador

Gabriela Sofia Estrella Ormaza
Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional del Ecuador

DOI: https://doi.org/10.37811/cl_rcm.v8i1.9777

Análisis de los Ataques de Ingeniería Social en Ecuador

Carlos Santiago Garzón Ibarra[1]
santy0810@yahoo.es
https://orcid.org/0009-0002-9822-5605
Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional del Ecuador

Christian Andrés Navas Tapia
cantchris@gmail.com
https://orcid.org/0009-0001-1005-9925
Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional del Ecuador

Angélica María Illicachi Tene
aillicachi@outlook.es
https://orcid.org/0009-0000-5036-3537
Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional del Ecuador

Rocío Janeth Espinoza Toapanta
chio2085@hotmail.com
https://orcid.org/0009-0007-7238-7709
Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional del Ecuador

Gabriela Sofia Estrella Ormaza
gaby92estrella@gmail.com
https://orcid.org/0009-0002-8184-8283
Dirección Nacional de Tecnologías de la Información y Comunicación de la Policía Nacional del Ecuador

RESUMEN

Este estudio se enfoca en analizar y comprender la naturaleza y el impacto de los ataques de ingeniería social en Ecuador. Su objetivo principal es identificar las tácticas específicas empleadas en dichos ataques, evaluar sus efectos en diversos sectores de la sociedad ecuatoriana y proponer estrategias efectivas de prevención y respuesta. Para alcanzar este fin, se adoptó un enfoque metodológico cualitativo y documental, permitiendo una exploración detallada y contextualizada de los ataques. Esto incluye el análisis exhaustivo de una variedad de fuentes documentales, como informes gubernamentales, estudios académicos, estadísticas de ciberseguridad y registros de incidentes. Los hallazgos del estudio indican un aumento preocupante en la frecuencia y sofisticación de los ataques de ingeniería social en Ecuador, destacando una la falta de conciencia y preparación general frente a estas amenazas. Se observa que, mientras el sector privado ha comenzado a implementar medidas de seguridad avanzadas, el sector estatal aún muestra limitaciones en su capacidad de respuesta y prevención. Este contraste subraya la necesidad urgente de fortalecer las estrategias de seguridad cibernética en todo el país, involucrando a múltiples actores, incluidos el gobierno, el sector privado, la academia y la sociedad civil.

Palabras clave: ingeniería social, ataques, ciberseguridad, Ecuador

[1] Autor principal
Correspondencia: santy0810@yahoo.es

Analysis of Social Engineering Attacks in Ecuador

ABSTRACT

This study focuses on analyzing and understanding the nature and impact of social engineering attacks in Ecuador. Its main objective is to identify the specific tactics used in such attacks, evaluate their effects on various sectors of Ecuadorian society, and propose effective prevention and response strategies. To achieve this, a qualitative and documentary methodological approach was adopted, allowing for a detailed and contextualized exploration of the attacks. This includes an exhaustive analysis of a variety of documentary sources, such as government reports, academic studies, cybersecurity statistics, and incident records. The study's findings indicate a worrying increase in the frequency and sophistication of social engineering attacks in Ecuador, highlighting a general lack of awareness and preparedness against these threats. It is observed that, while the private sector has begun to implement advanced security measures, the state sector still shows limitations in its response and prevention capabilities. This contrast underscores the urgent need to strengthen cybersecurity strategies across the country, involving multiple actors, including the government, private sector, academia, and civil society.

***Keywords*:** social engineering, attacks, cybersecurity, Ecuador

Artículo recibido 27 diciembre 2023
Aceptado para publicación: 31 enero 2024

INTRODUCCIÓN

El presente artículo aborda un tema de creciente importancia en el ámbito de la seguridad cibernética: el análisis de los ataques de ingeniería social en Ecuador. Esta temática cobra relevancia en un contexto donde la interacción digital se ha intensificado, incrementando la exposición a diversas formas de ciberdelincuencia. Los ataques de ingeniería social, caracterizados por la manipulación psicológica para obtener información confidencial o inducir a acciones específicas, representan una amenaza significativa en este panorama. Según Alza (2023), la ingeniería social se ha convertido en una de las técnicas más empleadas por ciberdelincuentes, aprovechando la tendencia humana a confiar y cooperar. En Ecuador, al igual que en otras partes del mundo, la digitalización acelerada ha traído consigo vulnerabilidades emergentes (Sancho et al., 2023). Estos ataques no solo capitalizan fallos tecnológicos, sino que explotan las debilidades humanas, convirtiendo a cualquier usuario en un potencial blanco. La ingeniería social, en este sentido, se aleja de los tradicionales ataques informáticos basados en software malicioso, centrándose en el "factor humano" como el eslabón más débil en la cadena de seguridad (Díaz, 2021).

Por tanto, una comprensión profunda de estos ataques, su naturaleza y sus implicancias en el contexto ecuatoriano no solo es pertinente, sino necesaria para desarrollar estrategias efectivas de prevención y respuesta. La presente investigación se enfoca en desentrañar estas dinámicas, proporcionando un análisis detallado que contribuya a la creciente literatura en este campo y ofrezca perspectivas útiles para profesionales de la seguridad, responsables de políticas y el público en general.

El núcleo de esta investigación se orienta hacia un problema crucial y aun insuficientemente explorado: la manifestación y el impacto de los ataques de ingeniería social en Ecuador. A pesar de la creciente conciencia sobre la ciberseguridad a nivel global, persiste una brecha significativa en el conocimiento específico acerca de cómo estos ataques afectan a individuos y organizaciones dentro del marco ecuatoriano. Según datos del Informe del Banco Interamericano de Desarrollo (2020); Ecuador y otros países de América Latina han experimentado un aumento en los incidentes de ciberseguridad, incluidos los ataques de ingeniería social, lo que destaca la necesidad de una comprensión más profunda de este fenómeno a nivel local.

La importancia de investigar este tema radica en la naturaleza única de los ataques de ingeniería social,

que explotan las vulnerabilidades humanas más que las tecnológicas. Como señala Gutierrez (2020), mientras que la tecnología puede ser fortalecida contra ataques, el elemento humano sigue siendo vulnerable. Este aspecto es crítico en Ecuador, donde la adopción de tecnologías digitales avanza a gran velocidad, pero la conciencia sobre seguridad y medidas preventivas pueden no estar al mismo nivel.

Además, entender cómo se manifiestan estos ataques en el contexto ecuatoriano es vital para desarrollar estrategias efectivas de prevención y respuesta. Por lo tanto, esta investigación busca contribuir a ese esfuerzo.

La relevancia de investigar los ataques de ingeniería social en Ecuador se fundamenta tanto en su impacto actual como en las potenciales consecuencias futuras para la sociedad y la economía del país. La importancia de este tema reside en que, más allá de los daños tecnológicos, los ataques de ingeniería social afectan directamente a los individuos, manipulando su comportamiento y comprometiendo su seguridad personal y profesional (Díaz, 2021).

En el contexto ecuatoriano, el impacto de estos ataques se extiende más allá de las pérdidas económicas directas, afectando la confianza en el ecosistema digital, un aspecto crucial para el desarrollo económico y social del país. Un estudio realizado por Mendoza (2020) resalta que los incidentes de ingeniería social no solo causan pérdidas financieras a empresas y consumidores, sino que también generan desconfianza en los sistemas de banca en línea y otras plataformas digitales, lo que puede retrasar la adopción de tecnologías y servicios digitales esenciales.

Por lo tanto, este estudio no solo busca llenar un vacío en el conocimiento existente, sino también proporcionar una base para el desarrollo de políticas, estrategias de seguridad y programas de concienciación que puedan proteger efectivamente a los ciudadanos y las instituciones de Ecuador.

El objetivo general de este estudio es analizar y comprender la naturaleza y el impacto de los ataques de ingeniería social en Ecuador. A través de esta investigación, se busca identificar las tácticas específicas utilizadas en estos ataques, evaluar su efecto en diferentes sectores de la sociedad ecuatoriana, y proponer estrategias efectivas de prevención y respuesta.

Este enfoque tiene como finalidad no solo llenar el vacío existente en la literatura sobre ciberseguridad en Ecuador, sino también contribuir a la creación de un entorno digital más seguro y resiliente en el país.

METODOLOGÍA

Este estudio adopta un enfoque metodológico cualitativo, enfocado en proporcionar una comprensión detallada y contextualizada de los ataques de ingeniería social en Ecuador. La elección de este enfoque se debe a su capacidad para profundizar en las percepciones, experiencias y motivaciones humanas, aspectos fundamentales en el estudio de la ingeniería social, un área donde los factores humanos son críticos.

Además, se ha optado por un enfoque documental dentro de la metodología cualitativa, ya que permite analizar y sintetizar una amplia gama de fuentes documentales, incluyendo informes gubernamentales, estudios académicos, estadísticas de ciberseguridad y registros de incidentes. Este enfoque es vital para comprender el alcance y la naturaleza de los ataques de ingeniería social en Ecuador, un área donde la información cuantitativa puede ser limitada o no reflejar completamente la complejidad del problema. Según Hernández (2014), el análisis documental ofrece una visión profunda y multifacética de los temas investigados, lo cual es esencial para abordar la naturaleza multidimensional de la ingeniería social.

Este estudio se clasifica como una investigación documental, un enfoque que implica el análisis exhaustivo y sistemático de documentos y materiales escritos relacionados con los ataques de ingeniería social en Ecuador (Zúñiga et al., 2023). La elección de esta clasificación responde a la necesidad de recopilar y analizar datos provenientes de una variedad de fuentes documentales, como informes de seguridad cibernética, artículos académicos, legislación relacionada con ciberdelitos y estudios de caso específicos (Cedeño et al., 2023). Al centrarse en el análisis documental, la investigación se beneficia de una perspectiva amplia y detallada del fenómeno, permitiendo una comprensión profunda de las tendencias, patrones y consecuencias de los ataques de ingeniería social en el contexto ecuatoriano.

Las consideraciones éticas juegan un papel crucial en la investigación documental, especialmente cuando se abordan temas sensibles como los ataques de ingeniería social. Uno de los principales aspectos éticos es el manejo responsable de la información sensible y confidencial.

Esto implica asegurar que cualquier dato personal o información identificable recopilada durante la investigación se trate con el máximo cuidado y respeto a la privacidad. Además, es esencial obtener el consentimiento adecuado para el uso de información privada, incluso en un contexto documental donde los datos ya son públicos o accesibles.

RESULTADOS Y DISCUSIÓN

En Ecuador, la prevalencia de los ataques de ingeniería social, según Competencia (2022), se ha intensificado debido a la meticulosa fase de investigación que realizan los atacantes, enfocándose en recolectar información personal para planificar y ejecutar sus engaños eficazmente. Este meticuloso enfoque ha resultado en un incremento notable de estafas en todo el país, destacándose los 6.086 casos de suplantación de identidad reportados en 2021. Esta situación pone de manifiesto la urgente necesidad de fortalecer las medidas de seguridad cibernética a nivel nacional.

En este contexto, Toala (2021) señala que, a nivel global, Ecuador ocupa el puesto 66 entre 193 países en un ranking de compromiso con la prevención de ciberataques, tal como lo indica la Unión Internacional de Telecomunicaciones. Este posicionamiento sugiere que, aunque Ecuador ha logrado avances significativos y ha desarrollado estudios en el campo de la ciberseguridad, aún enfrenta desafíos, especialmente a nivel estatal. Contrariamente, el sector privado del país demuestra un enfoque más proactivo, adoptando protocolos de seguridad avanzados, lo cual resalta la disparidad entre los esfuerzos gubernamentales y los del sector privado en materia de ciberseguridad.

Ecuador ocupa el puesto 119 de 182 países en vulnerabilidad a ataques cibernéticos, incluyendo malware, phishing, ingeniería social y troyanos, según el Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones, y se destaca la importancia de la precaución en el uso de información bancaria, advirtiendo sobre los ataques de phishing, que engañan a los usuarios para obtener datos sensibles como contraseñas y números de cuentas, y resalta que las entidades financieras nunca solicitan claves o información confidencial por correo electrónico o mensajes de texto, y recomienda no responder a correos sospechosos (Asobanba, 2023).

La creciente incidencia de ciberdelitos en Ecuador, como señala Gonzalo García de la Unidad Nacional de Ciberdelitos según Notimundo (2022), muestra un aumento alarmante de casos, escalando de 682 en 2020 a 1.852 en 2021, y continuando con 393 hasta la fecha en 2022. Este incremento se atribuye a la falta de cultura digital en el país, donde, aunque un alto porcentaje de la población (75.6%) utiliza internet, solo una pequeña fracción (10%) posee conocimientos digitales suficientes. Delitos comunes como la apropiación fraudulenta y la suplantación de identidad, penalizados por el Código Integral

Penal (COIP) de Ecuador, reflejan la necesidad de una mayor concienciación y educación en seguridad digital.

En línea con esto, la Policía Nacional del Ecuador (2023) y Toala (2021) identifican diversos tipos de estafas cibernéticas en el país, como el phishing, spear phishing y smishing, que buscan engañar a los usuarios para acceder a su información confidencial. A esto se suman otros delitos graves como violación de la intimidad, interceptación ilegal de datos y ataques a sistemas informáticos, con penas de hasta siete años. El aumento de denuncias de estas estafas durante la pandemia subraya la urgencia de adoptar medidas preventivas y seguir recomendaciones de seguridad para proteger la información personal de los ciudadanos ecuatorianos. Estos hallazgos revelan una brecha significativa en la capacidad de respuesta y prevención frente a las amenazas cibernéticas en el Ecuador.

Asobanca (2023) señala que los clientes bancarios suelen ser el eslabón más débil en ciberseguridad, subrayando la necesidad de educación digital para evitar ser víctimas de ciberdelincuencia. En 2022, en Ecuador se reportaron pagos a cibercriminales por más de 7.8 millones de dólares, con ataques. Además, la Unidad de Ciberdelitos de la Policía Nacional registró 1.340 casos de ataques cibernéticos, principalmente en provincias como Guayas, Pichincha, Manabí, Imbabura, Carchi y Azuay.

Estos ataques pueden variar en su método, pero su objetivo común es obtener información personal para cometer fraudes. Otros ejemplos incluyen engaños a través de correos electrónicos personales y corporativos, ofertas de mensajería puerta a puerta, viajes ganados y promociones, donde la clave de su éxito radica en la personalización del engaño para hacerlo creíble y convincente. Un ejemplo común en Ecuador involucra el uso de aplicaciones como WhatsApp, Messenger o SMS, donde los atacantes, previamente informados sobre los nombres del usuario y de sus familiares y conocidos, así como de sus actividades en redes sociales, simulan ser un conocido en el extranjero. A través de mensajes, engañan a la víctima haciéndole creer que necesitan ayuda con su equipaje en el aeropuerto, llevando eventualmente a solicitar datos personales y una copia de la cédula, lo cual resulta en el robo de identidad.

De acuerdo con SR Radio (2023), la creciente conectividad en Ecuador, donde el 76% de la población tiene acceso a internet, amplía el riesgo de ataques cibernéticos, especialmente a través de la ingeniería social. Sosa, de A3Sec, anticipa que para 2024, esta táctica se convertirá en la principal estrategia de

los ciberdelincuentes, afectando no solo a computadoras sino también a teléfonos y otros dispositivos conectados. La efectividad de estos ataques radica en la manipulación psicológica, extendiéndose desde las llamadas telefónicas tradicionales a correos electrónicos y mensajes instantáneos, y a menudo desemboca en ransomware. Con la evolución de estas técnicas, incluido el desarrollo de malware polimórfico, se espera que el riesgo de ataques de ingeniería social aumente significativamente en Ecuador.

Onofa (2022) destaca que Ecuador ha enfrentado varios ciberataques significativos, marcando un hito en la historia de la ciberseguridad del país. Incidentes como el ataque de ransomware al municipio de Quito, que comprometió el 20% de su base de datos, y el compromiso de la plataforma del CIES, que afectó a los subsistemas de Inteligencia de la Policía y Fuerzas Armadas, han sido cruciales. Estos ataques no solo han impactado a nivel gubernamental, sino también al sector privado, como lo evidencia el ciberataque al Banco Pichincha en octubre de 2021, que paralizó sus operaciones. Estos sucesos han propulsado una respuesta nacional, involucrando al gobierno, sector privado, academia y sociedad civil, y la creación de un Comité de Ciberseguridad desde 2017.

En paralelo, Peña (2023) enfoca su estudio en la necesidad de reforzar las defensas contra la ingeniería social en el sector financiero ecuatoriano. Su investigación resalta la importancia de mantener actualizado el Sistema de Gestión de Seguridad de la Información en las instituciones financieras, en un esfuerzo por proteger datos sensibles de los clientes. Peña subraya que la mayor vulnerabilidad frente a la ingeniería social es el factor humano, lo que implica que no hay una solución única para contrarrestar estos ataques. La guía desarrollada busca elevar la conciencia sobre la gestión de información sensible, un paso crítico para mitigar el riesgo de ataques de ingeniería social. Este enfoque es vital para Ecuador, especialmente en el sector financiero que continúa enfrentando desafíos singulares en materia de ciberseguridad.

Sancho et al. (2023) realizaron un estudio sobre el impacto de la ingeniería social en la comunidad académica tecnológica de la provincia de El Oro, llegando a la conclusión de que existe un riesgo medio. A pesar de cierta conciencia sobre estos ataques, el estudio reveló una vulnerabilidad significativa: de 200 participantes, 25 (el 13%) cayeron en la trampa, registrando sus credenciales, mientras que el 87%

restante no lo hizo, lo que demuestra un conocimiento básico pero insuficiente sobre la ingeniería social en este ámbito académico.

Este análisis se ve acentuado por la observación de que, incluso después de que la institución afectada emitiera advertencias sobre los ataques, un grupo reducido de personas aún fue víctima en una tercera fase del experimento. Esto subraya la brecha en el conocimiento completo necesario para contrarrestar eficazmente tales técnicas de ataque. Sancho et al. (2023) enfatizan la importancia de una mayor educación y concienciación sobre las consecuencias de la ingeniería social, destacando la necesidad de una gestión rigurosa y responsable de la seguridad de la información y el uso de credenciales en aplicaciones y servicios en línea. Este enfoque subraya la necesidad crítica de fortalecer las defensas cibernéticas en el ámbito académico y más allá.

En enero de 2021, Alcázar (2021) informó que en Ecuador más de 14.25 millones de personas tenían perfiles en redes sociales, siendo Facebook e Instagram las más utilizadas. Este auge de las redes sociales va de la mano con nuevos desafíos en la protección de datos personales. Villalba (2017) resalta la importancia de considerar la transferencia de datos como un elemento clave del derecho a la intimidad y del control sobre la información personal.

Ante esta realidad, Ecuador ha tomado medidas proactivas, desarrollando un modelo de integración para la protección de datos personales, alineado con la propuesta de la Ley Orgánica sobre la Protección de Datos Personales y los principios de la Organización de Estados Americanos (OEA). Ordóñez (2017) destaca la importancia de este marco jurídico en la era globalizada, subrayando su papel crucial para asegurar los derechos de los ciudadanos en un entorno tecnológico y constitucional en constante cambio. Este enfoque evidencia la necesidad de adaptar las leyes y regulaciones a los desafíos que presenta el creciente mundo digital en Ecuador.

Desde 2019, el gobierno de Ecuador ha reforzado sus medidas de seguridad cibernética para proteger a sus ciudadanos, según señala Escobar (2022). Esta iniciativa comenzó con la elaboración de un plan de manejo de crisis y la colaboración con el Ministerio de Telecomunicaciones para desarrollar una Estrategia Nacional de Ciberseguridad, con el objetivo de fortalecer el entorno digital del país, como destaca el Gobierno de la República del Ecuador (2019). Este esfuerzo marca un progreso importante en la implementación de políticas que buscan minimizar los riesgos asociados a los ciberataques, tanto

para el estado como para los ciudadanos. Además, se han implementado medidas para controlar el uso indebido de información personal, incluyendo la creación de una guía de protección de datos y la aprobación de la Ley Orgánica de Protección de Datos Personales en mayo de 2021 (Ministerio de Telecomunicaciones, 2020).

En una línea similar, el gobierno ha establecido un marco de seguridad de la información, adoptando las Normas Técnicas Ecuatorianas para la Gestión de Seguridad de la Información y el Plan Nacional de Seguridad Integral 2014-2017. Recientemente, en asociación con el Ministerio de Educación, se ha desarrollado una política pública sobre internet seguro-dirigida a niñas, niños y adolescentes. Esta política busca promover comportamientos protectores frente a los riesgos asociados al uso de internet y establecer protocolos de atención para casos en los que se vulneren la integridad y dignidad de los menores (Ministerio de Telecomunicaciones, 2020), demostrando un compromiso integral del gobierno para salvaguardar a sus ciudadanos en el ámbito digital.

En su estudio de 2020, Benavides llevó a cabo un experimento para sensibilizar sobre los ataques de ingeniería social. Este experimento consistió en un ataque simulado que utilizaba tácticas comunes de ingeniería social para recopilar datos sensibles de los usuarios, como direcciones IP y sistemas operativos, mediante un blog ficticio. También se realizó un escaneo de puertos en servidores web y SSH de las víctimas. Los resultados fueron reveladores: solo el 2% de los participantes detectó el verdadero propósito del blog, lo que indica un bajo nivel de conciencia sobre el phishing y la ingeniería social. Este estudio subraya la vulnerabilidad de la información sensible y la importancia de fortalecer la educación en ciberseguridad.

En una línea similar, Campoverde (2022) demostró la eficacia de la combinación de Kali Linux con técnicas de ingeniería social para simular ataques de phishing y evaluar la seguridad de la información en el Gad Municipal de la provincia de Santa Elena. Los ataques controlados revelaron una notable vulnerabilidad entre los empleados, muchos de los cuales cayeron presa de estos engaños. Además, se usó MetaExploit para exponer brechas de seguridad en los sistemas informáticos, resaltando la urgencia de adoptar medidas de protección más robustas. Estas pruebas permitieron evaluar la preparación de los usuarios y la seguridad de sus equipos, proporcionando la base para desarrollar estrategias de seguridad más efectivas en el Gad Municipal, fortaleciendo así la confianza de sus clientes.

La Policía Nacional del Ecuador (2017) enfatiza la importancia de adoptar prácticas efectivas de seguridad en línea para combatir la ciberdelincuencia. Sus recomendaciones clave incluyen marcar como favoritos los sitios web confiables, evitar hacer clic en enlaces sospechosos y no dejarse intimidar por tácticas de miedo empleadas por ciberdelincuentes. Además, resaltan la importancia de compartir conocimientos de seguridad cibernética y utilizar soluciones de seguridad eficaces, así como aprovechar las funciones de seguridad en sitios web populares como Facebook.

En una línea complementaria, Guevara y Flores (2023) proponen medidas específicas contra los ataques de ingeniería social. Recomiendan crear con anticipación correos electrónicos para simulacros de ataque, aprovechando la confiabilidad percibida de los correos validados. Sugieren también limitar la operación de servidores fraudulentos a un máximo de cuatro días y realizar campañas de cambio continuo de contraseñas, además de evitar el uso repetido de contraseñas en distintas aplicaciones y redes sociales. Estas recomendaciones apuntan hacia una estrategia proactiva para incrementar la concienciación y fortalecer la seguridad cibernética.

CONCLUSIONES

La revisión de los diversos estudios y reportes sobre la ciberseguridad en Ecuador revela un panorama complejo y en constante evolución. Los ataques de ingeniería social, en particular, han mostrado un aumento alarmante, evidenciado por el incremento significativo de ciberdelitos reportados por la Policía Nacional del Ecuador. Estos ataques, que van desde el phishing hasta el smishing, demuestran una vulnerabilidad notable en la población, a pesar de los esfuerzos gubernamentales para mejorar la seguridad digital.

Experimentos como los realizados por Benavides y Campoverde destacan la facilidad con la que se pueden comprometer datos personales y la importancia de la concienciación y educación en ciberseguridad. Además, se observa una disparidad entre las medidas de seguridad implementadas por el sector estatal y el privado, siendo este último más proactivo en la adopción de protocolos avanzados de seguridad.

El gobierno ecuatoriano ha reconocido estos desafíos y ha respondido con la implementación de políticas y estrategias integrales, incluyendo la Estrategia Nacional de Ciberseguridad y la Ley Orgánica

de Protección de Datos Personales. Además, se ha fomentado la educación y la prevención, especialmente entre los más jóvenes, para construir una cultura de seguridad digital más robusta.

En conclusión, aunque Ecuador ha realizado avances significativos en la lucha contra la ciberdelincuencia, los estudios indican que aún queda mucho por hacer para asegurar una protección efectiva contra los ciberataques. La necesidad de una mayor concienciación, educación y cooperación entre todos los sectores es crucial para enfrentar con éxito los desafíos de la seguridad cibernética en un mundo digital cada vez más interconectado.

REFERENCIAS BIBLIOGRAFICAS

Alcázar, J. P. (2021). Ecuador Estado Digital Enero 2021.

Alzas Hernandez, J. (2023). Estudio de fraudes basados en la técnica de Ingeniería Social. Obtenido de https://openaccess.uoc.edu/handle/10609/148147

Benavides, E., Fuertes, W., & Sánchez, S. (2020). *Un experimento para crear conciencia en las personas acerca de los ataques de Ingeniería Social.* Universidad de las Fuerzas Armadas-ESPE, Ecuador. Retrieved from https://www.redalyc.org/journal/5826/582661898003/

Campoverde, L. (2022). *Implementación de técnicas en ingeniería social en un gobierno autónomo descentralizado de la provincia de Santa Elena.*

Cedeño, R., Vásquez, P., & Maldonado, I. (2023). Impacto de las Tecnologías de la Información y la Comunicación (TIC) en el Rendimiento Académico: Una Revisión Sistemática de la Literatura. *Ciencia Latina Revista Científica Multidisciplinar, 7*(4). https://doi.org/https://doi.org/10.37811/cl_rcm.v7i4.7732

Competencia. (2022). *Existe la Ingeniería Social en el Ecuador?* Obtenido de https://www.competencia.com.ec/corporativo/existe-la-ingenieria-social-en-el-ecuador/

Díaz, J. (2021). Ingeniería social, un ejemplo práctico. . *Revista Odigos, 2*(3).

Escobar, A. (2022). Anólisis de ciberataques sobre el uso de redes sociales en relación a la protección de datos personales en Ecuador. . *Dominio de las Ciencias, 8*(1).

Guevara, D., & Flores, S. (2023). Análisis de vulnerabilidades en el uso de las redes sociales en ciber ataques de ingeniería social para fortalecer la seguridad de la información en la Facultad de Ciencias Humanas y de la Educación, de la Universidad Técnica de Ambato. Obtenido de https://repositorio.uta.edu.ec/handle/123456789/38382

Gutierrez, F. (2020). *Ciberseguridad e ingeniería social de la mano del ciberdelincuente.* Obtenido de http://repository.unipiloto.edu.co/handle/20.500.12277/7660

Hernández, R. (2014). *Metodología de la investigación.* McGRAW-HILL.

Mendoza, J. (2020). *Concientización en Ciberseguridad a través de Ataques de Ingeniería Social.* . INF-FCPN-PGI Revista PGI, 62-64. Obtenido de https://ojs.umsa.bo/ojs/index.php/inf_fcpn_pgi/article/view/109

Ministerio de Telecomunicaciones. (2020). Política pública sobre internet seguro para niñas, niños y adolescentes.

Notimundo. (2022). Delitos Informaticos en Ecuador.

OEA. (2020). *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe*. Obtenido de https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

Onofa, M. (2022). Ataques cibernéticos amenazan seguridad en Ecuador. *Dialogo Americas.*

Ordóñez, L. (2017). La protección de datos personales en los estados que conforman la Comunidad Andina. . *Revista de Derecho.*

Peña, D. (2023). Diseño de una campaña de ataques de ingeniería social. *Magister en Ciberseguridad.* PUCE. Obtenido de https://repositorio.puce.edu.ec/items/4f084144-df9f-4bd2-9263-b8c17a048a1c

Policía Nacional del Ecuador. (2017). *Ingeniería Social, sus repercusiones y recomendaciones*. Obtenido de https://www.policia.gob.ec/ingenieria-social-sus-repercusiones-y-recomendaciones/?amp=1

POLICÍA NACIONAL DEL ECUADOR. (2023). *Boletín Informativo de Ciberseguridad : LAS ESTAFAS CIBERNÉTICAS EN LA ACTUALIDAD.* Obtenido de

https://www.policia.gob.ec/wp-content/uploads/downloads/2020/11/Boletin-Estafas-Ciberneticas.pdf

Sancho, C., Cuenca, J., & Ortega, J. (2023). Ingeniería social y sus consecuencias en la población académica tecnológica de la provincia de El Oro. *MQRInvestigar, 7*(4).

Sancho, C., Cuenca, J., & Ortega, J. (2023). Ingeniería social y sus consecuencias en la población académica tecnológica de la provincia de El Oro. .

SR Radio. (2023). *LOS CIBERATAQUES CON INGENIERÍA SOCIAL MARCARÁN EL 2024*. Obtenido de https://srradio.com.ec/los-ciberataques-con-ingenieria-social-marcaran-el-2024/

Toala, Y. (2021). *Delitos informáticos frecuentes en el Ecuador: casos de estudio* . Obtenido de https://dspace.ups.edu.ec/handle/123456789/20942

Villalba, A. (2017). Reflexiones jurídicas sobre la protección de datos y el derecho a la intimidad en la autodeterminación informativa. *Revista de Derecho.* Obtenido de https://dominiodelasciencias.com/ojs/index.php/es/article/view/2622/html

Zúñiga, P., Cedeño, R., & Palacios, I. (2023). Metodología de la investigación científica: guía práctica. *Ciencia Latina Revista Científica Multidisciplinar, 7*(4). Retrieved from https://doi.org/10.37811/cl_rcm.v7i4.7658