ÉLITE **ÉLITE 2024** VOL 6. NUM 2. ISSN: 2600-5875
DOI: https://doi.org/10.69603/itsqmet.vol6.n2.2024.88

# Análisis de la efectividad de phishing automático

## *Analysis of the effectiveness of automatic phishing*

**Juan Pazmiño-Quiñonez[1], Marcela Saavedra-De la Cueva[1] y Luis Yulan-Mendoza[1]**

1 Instituto Tecnológico Superior Quito Metropolitano. Carán N3-195 y Calle B (Nueva Tola 2) Quito, Ecuador.

jupazmino@itsqmet.edu.ec, lsaavedra@itsqmet.edu.ec, lyulan@itsqmet.edu.ec

**Resumen:** El artículo examina la creciente amenaza del phishing automatizado, una técnica de ingeniería social que ha evolucionado con la automatización, complicando la protección de los sistemas informáticos tanto en Ecuador como a nivel global. El objetivo es analizar la efectividad de esta técnica y su impacto en la seguridad de la información. La metodología utilizada incluye una revisión sistemática de la literatura sobre phishing automatizado, destacando cómo la automatización ha incrementado la sofisticación y el alcance de estos ataques. Los resultados muestran que los ataques automatizados, facilitados por inteligencia artificial y machine learning, han superado en frecuencia a los ataques tradicionales a nivel global. En Ecuador, aunque menos comunes, los ataques automatizados han tenido un impacto notable, especialmente en sectores con medidas de seguridad limitadas. Las conclusiones resaltan la necesidad de adoptar controles de seguridad robustos, como la autenticación multifactor y la capacitación continua en ciberseguridad, además de seguir estándares internacionales como ISO/IEC 27001 para mitigar los riesgos del phishing automatizado. Se recomienda también realizar charlas de concientización para fortalecer la seguridad ante estas amenazas.

**Palabras clave:** Seguridad Informática, Phishing automatizado, Ciberseguridad, Ingeniería Social.

***Abstract**: The article examines the growing threat of automated phishing, a social engineering technique that has evolved with automation, complicating the protection of computer systems both in Ecuador and globally. The objective is to analyze the effectiveness of this technique and its impact on information security. The methodology used includes a systematic review of the literature on automated phishing, highlighting how automation has increased the sophistication and scope of these attacks. The results show that automated attacks, facilitated by artificial intelligence and machine learning, have surpassed traditional attacks in frequency globally. In Ecuador, although less common, automated attacks have had a notable impact, especially in sectors with limited security measures. The findings highlight the need to adopt robust security controls, such as multi-factor authentication and ongoing cybersecurity training, in addition to following international standards such as ISO/IEC 27001 to mitigate the risks of automated phishing. Awareness talks are also recommended to strengthen security against these threats.*

***Keywords:*** Computer Security, Automated Phishing, Cybersecurity, Social Engineering.

**ÉLITE 2024, VOL. (6). NÚM. (2)**
ISSN: 2600-5875
Recibido: 05/09/2024
Revisado: 14/09/2024
Aceptado: 17/09/2024
Publicado: 27/09/2024

## INTRODUCCIÓN

El uso de la tecnología bajo la operación del internet a tenido en los últimos años un crecimiento considerable tanto en hogares como organizaciones, lo cual presenta un aumento en la necesidad y obligación de proteger los sistemas informáticos y la información que estos gestionan, siendo la vía principal para cometer ciberataques o cibercrímenes. (Guaña Moya, y otros, 2022)

Entre estos delitos informáticos se encuentra la ingeniería social la cual se lo define como aquel método que utilizan los agentes de ataques para influir o efecto engañar a las personas para obtener información sensible en base a la manipulación psicológica, cabe mencionar que este método se basa en el uso de un conjunto de técnicas psicológicas con la única finalidad de conseguir que los usuario revelen voluntariamente datos sensibles como credenciales de acceso, información financiera o información sensible ya sea personal o corporativa para poder eludir los controles y políticas de seguridad de las organizaciones. (Hernandez, 2023)

Las estadísticas brindadas por la empresa Cybint, indica que las vulnerabilidades conscientes por los agentes de ataque suman un total de 95%, las cuales son generadas por errores humanos, en consecuencia, a esta cifra en términos globales las organizaciones ya sean Pymes o multinacionales son víctimas de este método de ataque siendo este un total de 700 veces en el transcurso del año. (Cybint, 2023)

En base a este panorama una de las técnicas de ataque más comunes de ingeniería social es el phishing, esta técnica tiene la finalidad de que un agente de ataque se hace pasar por un intermediario o remitente lícito buscando engañar a los usuarios con la intención de lograr introducir malware en la infraestructura de red informática de las organizaciones. (Asadullah & Satwinder, 2023)

Recientemente, el phishing se ha vuelto más sofisticado debido a la automatización de los procesos, lo que permite a los atacantes ampliar el alcance de sus ataques. El phishing automatizado utiliza scripts de software y algoritmos para enviar mensajes falsos en masa con el fin de aumentar las probabilidades de éxito del fraude. Esto hace que los ataques sean más rápidos, eficaces y difíciles de detectar, lo que supone una grave amenaza para la seguridad de usuarios y organizaciones, en base a esta preocupante novedad de ciberseguridad, Pilas López ex presidenta de Microsoft España indica que las actividades de los ciberdelincuentes se han vuelto más sofisticadas y sobre todo han aumentado los ataques que tienen como objetivo principal el afectar activos de alto valor pertenecientes a entidades tanto gubernamentales como de infraestructura críticas. (Actuarios, 2021)

## METODOLOGÍA

La metodología implementada para la presente investigación es de carácter descriptivo en la revisión sistemática de la literatura referente al análisis de la efectividad de phishing automático.

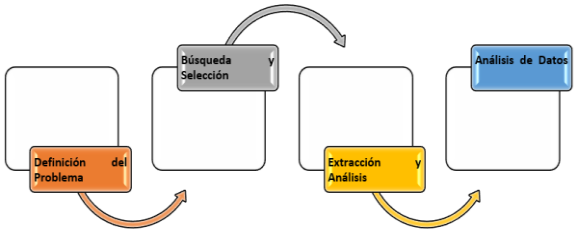


**Figura 1**. Representación e implementación de las fases de la metodología. Autoría propia.

**Fase I – Definición del problema:** La contrariedad principal a considerar es la creciente amenaza que presenta el phishing automatizado el cual resalta entre las diferentes técnicas de ingeniería social que con el pasar de los últimos

**ÉLITE 2024** VOL 6. NUM 2. ISSN: 2600-5875
DOI: https://doi.org/10.69603/itsqmet.vol6.n2.2024.88

ha presentado un cambio relevante en sus métodos eficaces de ataque, cabe mencionar que phishing automatizado, impulsado por la sistematización automática de instrucciones por lo tanto brinda a los agente de ataques el poder implementar múltiples acciones de e-mail maliciosos dando como resultado el aumentando, eficacia y trascendencia de los ataques en las redes informáticas.

Cabe especificar que el phishing es una amenaza informática global el cual se ve plasmada en los reportes de seguridad, siendo datos muy alarmantes que determinan una creciente impresionante tanto en la periodicidad y sofisticación de los ataques de phishing. Consiguiente a este tema en términos globales, la automatización de los ataques ya sea impulsada por machine learning o deep learning sin duda alguna a prestado la sencillez en la operación y ejecución a grados altos de afectaciones en la seguridad de la información siendo las principales víctimas los usuarios ya sean persona u organizaciones. En cambio, sí pones el enfoque en Ecuador, la situación sigue siendo igual, es decir, el inconveniente se sitúa diferente a los ojos o perspectiva de otros países de América latina, debido que se centra más en detalles de errores humanos tales como la falta de razón y saber ante estos tipos de ataques de ingeniería social los cuales puede declinar negativamente el o los escenarios de la confiabilidad, disponibilidad e integridad de los datos, situando en un impacto alto el riesgo de estas incidencia comprometiendo seriamente a entidades tanto privadas como públicas o gubernamentales.

**Fase III – Extracción y análisis:** Es crucial comprender el impacto que abarca la automatización en mejorar la eficacia de los ataques de phishing en las redes informáticas y a la par tener clara la idea de como aplicar controles o políticas de seguridad que faciliten el proceso de mitigar o reducir el riesgo.

Por lo cual es evidente tener claro el enfoque significativo y preocupante de la evolución que a establecido la automatización del phishing en base al uso de software, bot o script que permiten enviar masivamente tráfico de datos maliciosos de forma masiva, con la finalidad de que la probabilidad de ocurrencia sea más alta y que la amenaza tenga más éxito en su cometido, por lo cual en los últimos años uno de los ataques automatizado que más se han establecidos en el mundo de la ciberseguridad es el phishing kits, este tipo de amenaza permite a los agentes de ataques mejorar sus técnicas de suplantación de identidad, recopilación de correos personales o inclusive hasta el tener la capacidad de modificar páginas web falsas. (Guaña Moya, y otros, 2022)

En términos generales los ataques a nivel global, también son temas de interés, un claro ejemplo de como la automatización está tomando relevancia en la eficacia y sofisticación del phishing en este campo, el reconocido ataque Business Email Compromise “BEC”, este tipo de phishing automatizado en los últimos años se ha convertido en los más usuales, aquel método representa niveles económicos cruciales y de impacto de riesgo bajo para los agentes de ataque, pero con importantes ganancias, cada vez los agentes de ataque manejan equipos o en efecto herramientas de alta tecnología los cuales facilitan la forma de perpetrar sus actividades fraudulentas dirigidas hacia las organizaciones. Cabe recalcar que en estos últimos años organizaciones en Estados Unidos, han reportado perdidas elevadas de dinero las cuales abarcan en un total de 2.400 millones de dólares, dando a entender que este reporte muestra un dato alarmante de que tan comprometido, y nocivo que es este tipo de phishing automático para todo el negocio ya sea a nivel de Pymes como multinacionales. (Interpol, 2023)

En Ecuador, aunque los incidentes de phishing son menos frecuentes, se han registrado ataques a instituciones

financieras en los que la automatización ha jugado un papel clave. Esta tecnología ha hecho que los ataques sean más rápidos y difíciles de detectar, utilizando técnicas como la rotación de IP y la personalización dinámica del correo electrónico, lo que ha aumentado su efectividad, especialmente contra pequeñas y medianas empresas con defensas cibernéticas limitadas.

En respuesta, las organizaciones han implementado inteligencia artificial y aprendizaje automático para detectar patrones anómalos y han fortalecido la capacitación de los empleados y las políticas de autenticación multifactor "MFA". Sin embargo, el impacto del phishing automatizado varía según la región y la industria; Si bien en los países desarrollados se ha avanzado en la adaptación a estas amenazas, en Ecuador persisten desafíos importantes, especialmente en sectores como finanzas, salud y educación, donde la digitalización ha aumentado la vulnerabilidad. (Garzón, Navas, Illicachi, Espinoza, & Estrella, 2024)

**Fase IV – Análisis de datos:** El análisis de datos en esta investigación se enfoca en sintetizar los hallazgos obtenidos a lo largo de las fases anteriores, con un enfoque crítico en la evaluación de la efectividad de las técnicas de phishing automatizado y su impacto tanto a nivel global como en Ecuador.

A partir de los datos recopilados, se identifican patrones y tendencias que ilustran la creciente sofisticación y frecuencia de estos ataques, especialmente en sectores vulnerables como finanzas, salud y educación.

## RESULTADOS Y DISCUSIÓN

### 3.1. Estadísticas de ataques por phishing automatizado en Ecuador.

En la figura 2, se proyecta el ciclo de ataque de phishing automatizado a una víctima, se determina el proceso inicial con el agente de ataque, quien envía un mensaje con tráfico malicioso a la víctima mediante un correo electrónico, al hacer clic en el enlace proporcionado, la víctima es redirigida a una página web de phishing diseñada para imitar una página legítima, en esta página falsa, la víctima ingresa sus credenciales, que son capturadas por el agente de ataque, en base a esta información, el agente accede a la página web legítima usando las credenciales obtenidas, completando así el ataque.

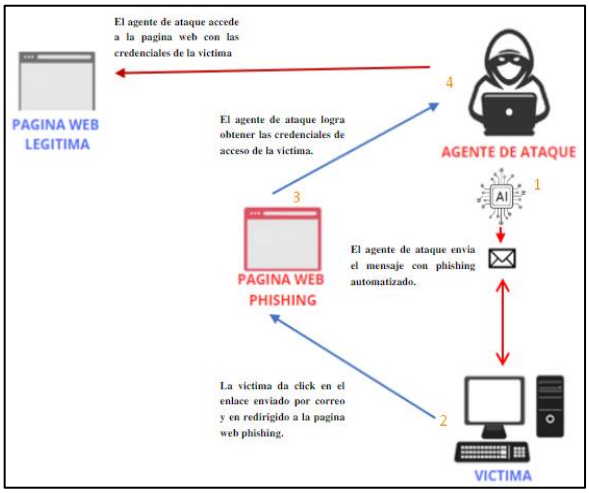


***Figura 2.*** *Proceso de ataque phishing automatizado. Fuente: Autoría propia.*

En base a este modelo de ataque, se estima el reporte preocupante de una creciente del 90% de las contravenciones en la seguridad de la información la cual está directamente afín con los ataques por phishing automatizado, en definitiva, en estos últimos años se ha convertido en una de las principales procedencias de robo de credenciales de acceso a datos o información confidencial o datos financieros lo cual lo convierte en peligro constante tanto para una o varias personas u organización.

Y es aquí donde se ve reflejado el aumento de conocimiento en este tipo de técnicas cada vez más complejas en el robo de información y a la par el desarrollo contante de la tecnología, más la creciente desentendencia

de plataformas digitales y uso del internet lo definen como aquella amenaza de alto riesgo. (Interpol, 2023)

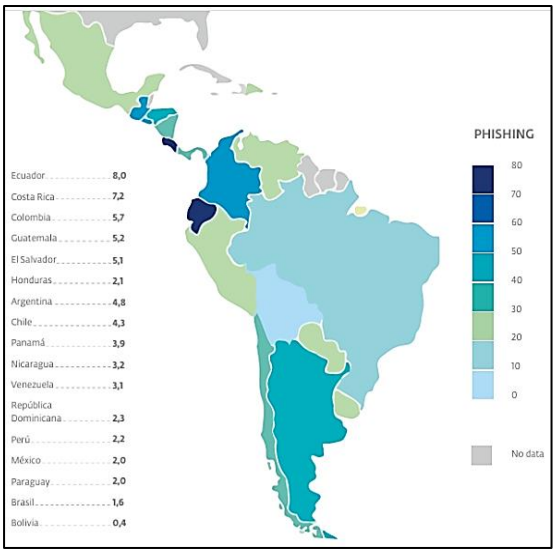


**Figura 3.** Países de América latina con mayor cantidad de detecciones de phishing 2022. Fuente: (ESET, 2023)

En la figura 3, se observa el reporte detallado por ESET, en el cual se indican las incidencias de ataques por phishing en la región, se tiene un crecimiento considerable del 69%, es decir, que la mayoría de las Pymes y multinacionales en América Latina fueron víctimas de incidencias u ocurrencias de ataques durante este último año, en base a estas estadísticas se centra a Ecuador como uno de los países más atacados por este método de ingeniería social con un 8%. (ESET, 2023)

Por lo tanto, es evidente que Ecuador afronta una ardua ola de ataques sofisticados, es decir, phishing automatizados, pero, ¿por qué se dan estos datos preocupantes en Ecuador?, es por lo que la mayoría de sistemas de protección de información tradicionales no son funcionalmente tan efectivos contra este método de ingeniería social. (ODD, 2023)

**Tabla 1.** Análisis del reporte de ataque phishing en el 2023 por las provincias importantes de Ecuador. Fuente: Fiscalía General del Estado.

| # | Provincia | Total, de ataques phishing |
|---|---|---|
| **1** | Pichincha | 1256 |
| **2** | Guayas | 1513 |
| **3** | Azuay | 185 |

### 3.2. Estadísticas de ataques por phishing automatizado a nivel global.

El análisis de las estadísticas globales sobre ataques de phishing automatizado revela un crecimiento alarmante en los últimos años, impulsado por la sofisticación de las herramientas empleadas y la expansión de los vectores de ataque, aproximadamente el 36% de las contravenciones de información reportados a nivel global abarcaron técnicas de phishing, de las cuales una proporción significativa se llevó a cabo de manera automatizada, en base a estos valores la tendencia está correlacionada con el aumento del uso de tecnologías como el Machine Learning y la inteligencia artificial en la creación de operaciones masivas de phishing, que permiten la personalización intensiva de correos electrónicos y mensajes engañosos a gran escala, logrando así evadir con mayor eficacia los sistemas de detección convencionales. (APWG, 2024)

ÉLITE **ÉLITE 2024** VOL 6. NUM 2. ISSN: 2600-5875
DOI: https://doi.org/10.69603/itsqmet.vol6.n2.2024.88

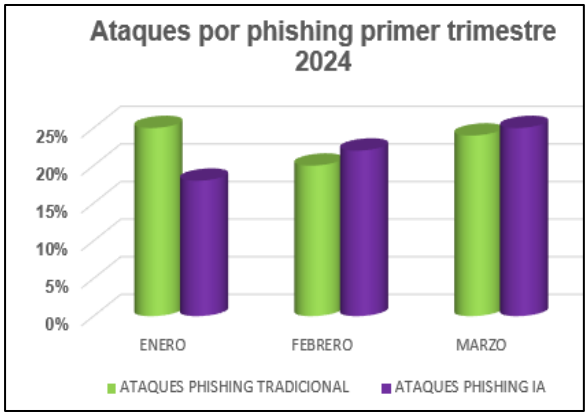


**Figura 4.** Reporte de ataques por phishing a nivel global. Fuente: Autoría propia.

Como se puede apreciar en la figura 4, en enero de 2024, los ataques de phishing tradicional alcanzan su punto más alto con un 25%, mientras que los ataques asistidos por IA representan un porcentaje menor, cercano al 15%, consiguiente aquello en febrero, aunque los ataques tradicionales experimentan una ligera disminución, los ataques de phishing potenciados por IA aumentan, casi igualando en número a los tradicionales. Finalmente, en marzo de 2024, los ataques de phishing asistidos por IA superan a los tradicionales, alcanzando el 25%, lo que indica un cambio notable en la dinámica de amenazas cibernéticas. Este gráfico subraya la creciente amenaza que representan los ataques de phishing asistidos por IA. A medida que la tecnología avanza, los ciberdelincuentes adoptan herramientas de inteligencia artificial para mejorar la efectividad de sus ataques, haciéndolos más difíciles de detectar y combatir.

Este porcentaje se ve referenciado en los objetivos que tiene los agentes de ataque, es decir, que su principal punto de ataque es el poder obtener información relevante que les permita tener tanto credenciales de acceso como información crítica de las organizaciones o en efecto de los usuarios bajo las operaciones industriales por lo tanto se tiene como resultado alarmante que la mayoría de ataques se ingeniería social y en especial phishing automatizado se da en las redes sociales con un total del 37,6%. (APWG, 2024)

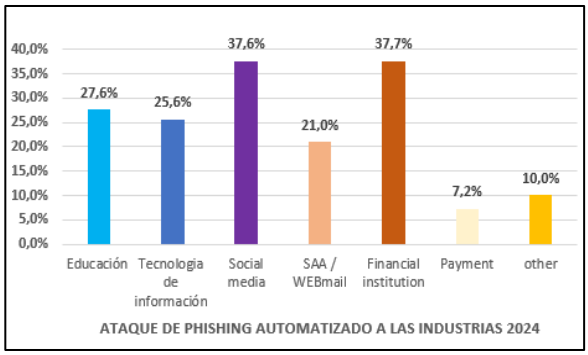


**Figura 5**. Reporte de ataques de phishing automatizado a las industrias. Fuente: Autoría propia.

Con este panorama se puede determinar el gran riesgo que presenta este tipo de ataque automatizado en las industrias según su tipo de servicio, el reporte global del primer trimestre por APWG, determinó que los agentes de ataque en la mayoría de sus lanzamientos de phishing automatizado van redirigidos a dominios de cuentas de correo web gratuito como se puede apreciar en la figura 6, la cual revela un esquema claro en los ataques de phishing automatizado, con una fuerte concentración en los servicios de correo electrónico más populares, como Google y Microsoft, y más que nada este enfoque investigativo en plataformas populares demuestra una pauta de ataque eficiente que se centra en maximizar el éxito de las campañas automatizadas de phishing.

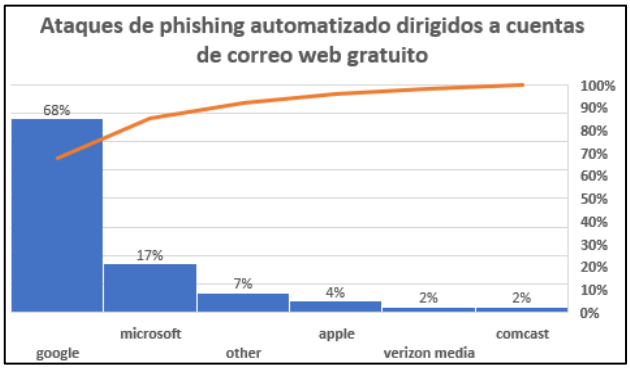


**Figura 6.** Ataques de phishing automatizado dirigidos a cuentas de correo web gratuito

**CONCLUSIONES.**

En el contexto de la creciente digitalización y la expansión del uso de internet, se ha evidenciado un notable incremento en la necesidad de salvaguardar los activos de información, debido al aumento de ciberataques y cibercrímenes y especialmente la ingeniería social, y más específicamente el phishing automatizado, se ha destacado como una amenaza considerable.

El análisis revela que el phishing automatizado no solo ha sofisticado los métodos de ataque, sino que también ha amplificado su impacto, tanto a nivel global como en Ecuador. Las estadísticas globales indican un crecimiento alarmante en los ataques de phishing, destacando la efectividad de la automatización mediante el uso de inteligencia artificial y machine learning para personalizar mensajes engañosos y evadir sistemas de detección

Por tanto, es imperativo que las organizaciones y usuarios se adapten a esta evolución en las técnicas de phishing. Las medidas recomendadas incluyen la implementación de controles de seguridad robustos, como la autenticación multifactor y la capacitación continua en ciberseguridad, para contrarrestar los ataques automatizados, cabe mencionar que de igual manera que se implementen controles de seguridad es importante adoptar medidas de seguridad o estándares internacionales que permitan mitigar o reducir este tipo de ataque de ingeniería social como la norma ISO/IEC 27001.

Además, es crucial que las organizaciones programen charlas por medio de los encargados de la seguridad de la información para concientizar a los usuarios sobre buenas prácticas ante el uso de plataformas digitales o internet.

**CONTRIBUCIONES DE LOS AUTORES:**

Para el desarrollo de esta investigación se tuvo la contribución de varios autores a lo largo de todo el proceso para estructurar dicho artículo.

La contribución de cada uno de los autores relevantes en este artículo se la describe a continuación:

Para la conceptualización y metodología, contribuyeron, Juan Pazmiño-Quiñonez y Marcela Saavedra-De la Cueva; para la parte de análisis formal, investigación y recursos, Juan Pazmiño-Quiñonez, Marcela Saavedra-De la Cueva y Luis Yulan-Mendoza; curación de datos, Juan Pazmiño-Quiñonez, Marcela Saavedra-De la Cueva y Luis Yulan-Mendoza; escritura-preparación del borrador original, Juan Pazmiño-Quiñonez; redacción-revisión y edición, Juan Pazmiño-Quiñonez; visualización, supervisión, administración de proyectos, Juan Pazmiño-Quiñonez.

**FINANCIAMIENTO:**

Cabe mencionar que esta investigación no tuvo financiamiento externo.

**REFERENCIAS.**

- Actuarios. (2021). Ciberriesgos. Acuarios, 10-11.
- APWG. (2024). Unificando la respuesta global al cibercrimen.
- Asadullah, S., & Satwinder, S. (2023). Una revisión sistemática de la literatura sobre técnicas de detección de sitios web de phishing. ELSEVIER, 590-611.
- Cybint, S. (2023). Cybint Solutions. Obtenido de Cybint Solutions: https://www.cybintsolutions.com/
- ESET. (2023). Report Security, Latinoamérica 2023. Bratislava: ESET.
- Garzón, C., Navas, C., Illicachi, A., Espinoza, R., & Estrella, G. (2024). ANALYSIS OF SOCIAL ENGINEERING ATTACKS IN ECUADOR. Ciencia Latina, 4354-4367.

**ÉLITE 2024** VOL 6. NUM 2. ISSN: 2600-5875
DOI: https://doi.org/10.69603/itsqmet.vol6.n2.2024.88


- Guaña Moya, J., Chiluisa Chiluisa, M., Jaramillo Flores, P., Naranjo Villota, D., Mora Zambrano, E., & Larrea Torres, L. (2022). Ataques de phishing y cómo prevenirlos. IEEE, 6.
- Hernandez, J. (2023). Estudio de fraudes basados en la técnica de Ingeniería Social. Cataluña: UOC.
- Interpol. (2023). Informe Sobre la Evaluación de las Ciberamenzas en Africa. Lyon: Interpol.
- ODD. (2023). Nueva ola de ataques de phishing en Ecuador. ODD, 1-7.