27(4): 415-418, 2024

SCIÉNDO

Influencia de los Delitos Cibernéticos Económicos en Perú

Influence of Economic Cybercrime in Peru

Víctor Hugo Che León Antinori[1,*]

1 Universidad Nacional de Trujillo, Av. Juan Pablo II s/n, Trujillo, Perú.

*Autor correspondiente: **vhcheleonan@unitru.edu.pe** (V. H. Che León Antinori).

Fecha de recepción: 08 09 2024. Fecha de aceptación: 21 10 2024.

RESUMEN

El presente artículo tuvo como objetivo analizar la influencia de los delitos cibernéticos económicos en el Perú durante el año 2024, abordó las modalidades más comunes, su impacto económico y las deficiencias en el marco legal. Los delitos cibernéticos económicos, como el phishing, el robo de identidad, los ataques a plataformas de pago y las estafas en comercio electrónico, han crecido de manera significativa en los últimos años, generando pérdidas económicas sustanciales y afectando la confianza de los usuarios en las plataformas digitales. La metodología que se adoptó fue de carácter cualitativo, con un enfoque exploratorio y descriptivo. Para la recolección de datos se empleó entrevistas semiestructuradas con abogados penalistas, fiscales y expertos en ciberseguridad, junto con el análisis de casos judiciales relevantes y la revisión documental de informes oficiales. Los resultados mostraron un incremento del 26% en los delitos cibernéticos económicos en comparación con el año 2023. Entre las conclusiones del estudio, se destacó la urgente necesidad de actualizar el marco legal peruano para adaptarse a las nuevas modalidades delictivas que surgen con el avance tecnológico. Este análisis buscó aportar una visión crítica sobre la incidencia de los delitos cibernéticos económicos en el Perú.

Palabras claves: Delitos cibernéticos; Economía digital; Seguridad Informática.

ABSTRACT

This article aimed to analyze the influence of economic cybercrimes in Peru during the year 2024, addressing the most common modalities, their economic impact, and deficiencies in the legal framework. Economic cybercrimes, such as phishing, identity theft, attacks on payment platforms, and e-commerce scams, have grown significantly in recent years, generating substantial economic losses and affecting user confidence in digital platforms. The methodology adopted was qualitative, with an exploratory and descriptive approach. For data collection, semi-structured interviews with criminal lawyers, prosecutors, and cybersecurity experts were used, along with the analysis of relevant court cases and the documentary review of official reports. The results showed a 26% increase in economic cybercrimes compared to the year 2023. Among the conclusions of the study, the urgent need to update the Peruvian legal framework to adapt to the new criminal modalities that arise with technological advances was highlighted. This analysis sought to provide a critical view on the incidence of economic cybercrimes in Peru.

Keywords: Cyber-crimes; Digital economy; Informatic security.

INTRODUCCIÓN

En los últimos años, el Perú ha experimentado un notable incremento en la incidencia de delitos cibernéticos económicos, en concordancia con el crecimiento exponencial del comercio electrónico y la digitalización de los servicios financieros. Estos delitos, que abarcan desde el fraude electrónico hasta el robo de identidad y los ataques a plataformas de pago, han generado impactos significativos en la economía y la seguridad jurídica del país (Zárate, 2023).

Los delitos cibernéticos económicos no solo afectan a las grandes corporaciones, sino también a pequeños comerciantes y usuarios individuales. El Instituto Nacional de Estadística e Informática (INEI) (2024) reporta que en el primer trimestre del año 2024 se registraron más de 30,000 casos de fraude electrónico, lo que representa un aumento del 25% en comparación con el mismo periodo del año anterior. Este crecimiento se ha visto impulsado por el incremento del uso de aplicaciones de pago móvil y plataformas digitales de comercio que, aunque ofrecen conveniencia, también han mostrado vulnerabilidades que los ciberdelincuentes han sabido explotar.

Castro (2022), señala que el marco jurídico peruano, si bien ha experimentado avances en los últimos años, aún presenta importantes lagunas que dificultan la persecución eficaz de los delitos cibernéticos. En su análisis de la legislación vigente, destaca que uno de los principales problemas radica en la falta de capacitación técnica de los operadores de justicia, lo que limita la capacidad del sistema judicial para adaptarse a la complejidad de los crímenes digitales. Esto es especialmente preocupante dado el carácter transnacional de muchos de estos delitos, que requiere no solo una actualización legislativa constante, sino también una mayor cooperación internacional.

En cuanto a las modalidades delictivas más comunes en el Perú, el Banco Central de Reserva del Perú (BCRP) (2024) ha identificado al phishing como una de las principales amenazas para los usuarios de servicios financieros. El phishing, que consiste en el envío de correos electrónicos fraudulentos para obtener información personal y bancaria, representa más del 40% de los ataques reportados en 2024. Este tipo de delitos afecta principalmente a usuarios particulares y pequeñas empresas, que carecen de los recursos necesarios para implementar medidas de protección avanzadas.

La evolución de los delitos cibernéticos en el país está íntimamente relacionada con la creciente dependencia de las tecnologías digitales para la realización de transacciones financieras. La falta de conciencia y educación sobre ciberseguridad entre la población peruana ha facilitado el aumento de estas actividades delictivas, ya que muchas víctimas no están familiarizadas con las técnicas básicas de protección de datos (Rodríguez, 2023).

El estudio de los delitos cibernéticos no solo es crucial para proteger a las víctimas, sino también para fortalecer la confianza en las plataformas digitales, que son esenciales para el desarrollo económico del país, mediante respuestas coordinadas entre diferentes sectores (Villanueva, 2023).

La presente investigación tiene como objetivo analizar cualitativamente la influencia de los delitos cibernéticos económicos en el Perú durante el año 2024.

METODOLOGÍA

Se abordó el diseño fenomenológico, que describe la esencia de las experiencias por los individuos en relación a los delitos cibernéticos económicos. Este diseño obtiene comprensión holística por parte de los expertos en ciberseguridad en el Perú. Se recolecto datos por medio de análisis de documentos oficiales, reportes y estudios relacionados delitos cibernéticos económicos en el Perú. Se empleó el análisis temático en este artículo cualitativo. Se analizó cualitativamente las tendencias de los delitos cibernéticos económicos en el Perú, así también se evaluó la efectividad de las respuestas legales y jurídicas en la persecución de estos delitos. Se realizó una revisión de los informes publicados por el Instituto Nacional de Estadística e Informática (INEI), el Ministerio del Interior (MININTER), y la Policía Nacional del Perú (PNP).

RESULTADOS Y DISCUSIÓN

La figura 1, muestra la distribución de las modalidades de delitos cibernéticos en el Perú 2024. El phishing y el fraude electrónico representan la mayor proporción, con un 45%, seguido por el robo de identidad con un 22%, lo ataques a plataformas de pago con un 18%, las estafas en comercio electrónico con un 15%. Estos datos reflejan la prevalencia de los distintos tipos de cibercrímenes en el país y su incidencia en la economía digital.

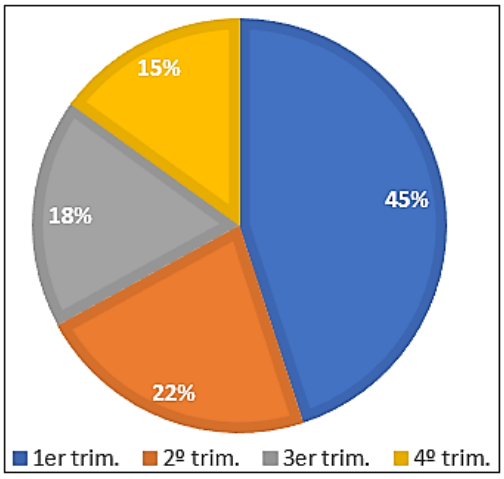

Figura 1. Incremento de Delitos Cibernéticos Económicos en el Perú (2019-2024). Fuente: Producción propia con datos de INEI (2024).

Se analizo el incremento, y se obtuvo que el aumento constante en los delitos cibernéticos económicos en Perú es evidente en los últimos cinco años. Según el Institudo Nacional de Estadística e Informática (INEI) (2024), se estima que en 2024 se registrarán más de 26,500 casos de este tipo de delitos, lo que representa un incremento del 26% respecto al año anterior (pág. 35). Este aumento se atribuye al incremento en el uso de tecnologías digitales, especialmente en el ámbito del comercio y los servicios financieros en línea pág. 35).

El abogado penalista López Silva (2023) indica que este crecimiento refleja la "falta de medidas de ciberseguridad adecuadas tanto a nivel corporativo como en el uso personal, lo que ha facilitado que los ciberdelincuentes exploten las vulnerabilidades tecnológicas" (pág. 112).

Núñez Robinson (2023) destaca que el Estado peruano, al adherirse al Convenio de Budapest, ha mostrado un esfuerzo importante por adaptar su legislación a los estandares internacionales. Esto ha permitido establecer procedimientos que mejoran la cooperación internacional en investigaciones sobre delitos cibernéticos, algo esencial debido a la naturaleza efectiva de estas herramientas aún es limitada en Perú, lo que se refleja en la cantidad de archivamientos fiscales y las mínimas sentencias condenatorias obtenidos en estos casos (pág. 18).

Bernal Gallardo y Menacho Ortega (2021)han realizado investigaciones sobre la implementación de fiscalias y juzgados especializados en ciberdelincuencia en Perú. Señalan que se ha avanzado en la normativa y en la creacion de unidades especializadoas, el sistema de justicia peruano todavía enfrenta grandes desafíos logísticos y tecnológicos, lo que genera desconrfianza en la población para denunciar delitos cibernéticcos, y limita la capacidad del Estado para sancionar efectivamente a los delincuentes.

Iura Lex Abogados y Asociados (2024) resaltó que los delitos como el phishing, vishing, y smishing estan en aumento, que ha afectado tanto a individuos como a empresas. La Ley N°. 30096 prevé penas de hasta 10 años para los delitos, demostró el compromiso del Estado para combatirlos. Las medidas actuales son insuficientes frente a la rápida evolución de las tecnologías delictivas, sobre todo en delitos económicos que involucran el robo de capitales mediante software malicioso.

Tabla 1
Distribución de Modalidades de Delitos Cibernéticos Económicos en el Perú (2024)

Modalidad	Porcentaje %
Phishing y fraude electrónico	45%
Robo de identidad	22%
Ataques a plataformas de pago	18%
Estafas en comercio electrónico	15%

Fuente: Policía Nacional del Perú (PNP), 2024.

En la tabla 1, se analizó las modalidades, como se puede observar, la modalidad de phishing y fraude electrónico es la más prevalente, representando el 45% de los casos reportados en 2024. Esta técnica consiste en el envío de correos electrónicos o mensajes fraudulentos para obtener información sensible de las víctimas, como contraseñas o datos bancarios. Estos resultados coinciden con García (2023), quien manifesto que debido a su alta efectividad y la falta de educación digital en la población el phishing es la técnica más usada por los ciberdelincuentes.

El robo de identidad, que ocupa el 22%, sigue siendo una modalidad crítica, afectando la integridad de los usuarios de plataformas de pago y comercio en línea.

En Perú, las modalidades de delitos cibernéticos económicos han experimentado un notable incremento en los últimos años, especialmente en 2024, a medida que las tecnológias van en aumento y son usadas para gestiones ilícitas. El Estado peruano ha sufrido varias modalidades de delitos cibernéticos que impactan tanto en instituciones privadas y públicas.

IUS 360 (2024) la modalidad por Fraude Informático o cibernético, tipificado en el artículo 8 de la Ley N°. 30096, ha implicado la manipulación ilégitima de sistemas informáticos para causar perjuicio económico a terceros. Hoy en el 2024, el fraude informático ha afectado signifcativamente a diversas entidades financieras y organismos gubernamentales mediante técnicas como el phishing y vishing, donde los delincuentes cibernéticos suplantan a instituciones bancarias o del Estado para obtener información confidencial de los usuarios.

IUS 360 (2024), la Clonación de Tarjetas y Suplantación de Identidad, son otras modalidades que golpeó duramente al país que ha sidod la clonación de tarjetas de crédito y débito, así tambien la suplantación de identidad. Estos delitos han crecido debido al acceso no autorizado a las bases de datos como la RENIEC, que permitió que los delincuentes manipularan la información personal y financiera de los ciudadanos.

Tabla 2
Pérdidas Económicas estimadas por Delitos Cibernéticos en el Perú (2019-2024)

Año	Pérdidas estimadas (millones de soles)
2019	15
2020	18
2021	24
2022	29
2023	35
2024	40 (estimado)

Fuente: Banco Central de Reserva del Perú (BCRP), 2024.

En la tabla 2, se analizó el impacto económico de los delitos cibernéticos, este ha crecido significativamente en el Perú, con pérdidas estimadas en 400 millones de soles para 2024, según el Banco Central de Reserva del Perú (BCRP) (2024). Estas pérdidas afectan tanto a empresas privadas como a instituciones públicas, poniendo en riesgo la confianza en las transacciones digitales. Este resultado es respaldado por Paredes (2023), quien señala que los delitos cibernéticos son una amenaza constante para la economía peruana por falta de inversión en ciberseguridad y las deficiencias en el marco legal.

Las pérdidas son atribuidas principalmente a ataques de Ransomware, fraudes financieros y suplantación de identidad, afectando tanto a instituciones públicas y privadas.

Ardiles (2024) el Registro Nacional de la Identificación y Estado Civil (RENIEC), informó que desde el año 202 bloqueó un total de 923 casos de suplantación de identidad en las inscripciones del DNI. Esto fue posible luego de un trabajo realizado con la nueva versión del Sistema Automatizado de Identificación Biométrica (ABIS) y de los peritos grafotécnicos del Reniec, que se encargaron de identifica, autenticar y validar la información presentada.

El Comercio (2024) en su publicación, evidencia que hubo condenas dos años y seis meses de prisión suspendida por el delito contra la fe pública en la modalidad de suplantación de identidad.

CONCLUSIONES

Una de las principales conclusiones del artículo es la urgente necesidad de actualizar y fortalecer el marco legal en materia de ciberseguridad en el Perú.

La legislación actual no es suficiente para enfrentar la magnitud y sofisticación de los delitos cibernéticos económicos en 2024.

El artículo advierte que la falta de concientización sobre ciberseguridad es un factor clave en la vulnerabilidad de las empresas y los individuos frente a los delitos cibernéticos económicos.

Los delitos cibernéticos económicos en Perú han experimentado un crecimiento preocupante en 2024, afectando tanto a empresas como a individuos, y generando importantes pérdidas económicas.

Aunque se han dado pasos para reforzar la legislación, todavía existen importantes vacíos legales y técnicos que limitan la efectividad de las medidas implementadas.

Las PYMES, en particular, deben ser un foco de estas campañas dado su papel crucial en la economía peruana y su alta susceptibilidad a los ciberataques.

Es esencial que el gobierno peruano fortalezca la infraestructura de ciberseguridad del país.

Hay dificultad para rastrear a los autores, delincuentes utilizan herramientas que les permiten anonimizar sus actividades en línea, como redes privadas virtuales (VPN).

Finalmente, se concluye que el sector privado, especialmente las instituciones financieras, debe asumir una mayor responsabilidad en la protección contra los delitos cibernéticos económicos. Esto incluye la inversión en tecnologías avanzadas de ciberseguridad, así como la colaboración con el gobierno para desarrollar estándares y protocolos de seguridad más sólidos.

REFERENCIAS BIBLIOGRÁFICAS

Ardiles, A. (19 de marzo de 2024). Reniec detectó y bloqueó 923 casos de suplantación de identidad desde 2020: así utilizan información de personas fallecidas. El Comercio, págs. 1-3.

Banco Central de Reserva del Perú (BCRP). (2024). Informe anual sobre el impacto económico de los delitos cibernéticos en Perú. Banco Central de Reserva del Perú (BCRP), 58.

Bernal Gallardo, J., y Menacho Ortega, B. (2021). Las fiscalías y los juzgados especializados en ciberdelincuencia y su implementación en el sistema de justicia del Perú 2020. UPN Repository, 45-47.

Castro Ruiz, J. (2022). Cibercrimen y legislación penal en Perú. Lima: Ediciones Jurídicas del Perú.

DIVINDAT. (03 de 2016). División de Investigación de Delitos de Alta Tecnología. Obtenido de https://www.seguroseninternet.org/es/divindat.html

El Comercio. (11 de abril de 2024). Facebook: Poder Judicial condena a mujer por crear perfil falso en redes sociales. El Comerciio, págs. 1-5.

García Sánchez, R. (2023). El impacto del phishing en la ciberseguridad peruana. Lima: Universidad de Lima.

García, P. (2021). Desafíos Legales en la persecución de delitos cibernéticos en el Perú. Revista de Derecho Penal y Criminología, 102-119.

Institudo Nacional de Estadística e Informática (INEI). (2024). Informe anual de delitos cibernéticos en el Perú: Impacto económico y social. 2-11.

Iura Lex Abogados y Asociados. (2024). La ciberdelincuencia en el Perú. Iura Lex - Abogados y Asociados, 37-38.

IUS 360. (2024). Los delitos cibernéticos en el Perú: Análisis de las modalidades delictivas más relevantes. IUS 360, 75-78.

López Silva, M. (2023). Cibercriminalidad económica: Retos legales en Perú. Lima: Editorial PUCP.

Mendoza, J., y Torres, F. (2023). La respuesta institucional frente a la cibercriminalidad en Perú. Revista Peruana de Derecho Penal, 89-104.

Núñez Robinson, R. (2023). Los delitos cibernéticos en el Perú y el Convenio de Budapest. IUS 360 - Uandina Repository, 18.

Paredes Velásquez, C. (2023). Cibercrimen y economía: Consecuencias jurídicas y económicas en Perú. Arequipa: Universidad Nacional de San Agustín.

Policía Nacional del Perú (PNP). (2024). Informe de la División de Cibercrimen sobre delitos económicos cibernéticos en el Perú. 12.

Rodríguez Silva, M. (2023). La evolución del cibercrimen en Perú: Un análisis jurídico. Arequipa: Universidad de San Agustín.

Valdivia, J., y Zárate, P. (2023). Ciberseguridad y delitos cibernéticos en Perú: Retos y soluciones. Lima: Editorial PUCP.

Villanueva Quispe, D. (2023). La respuesta penal frente a la cibercriminalidad: Un enfoque latinoamericano. Lima: Universidad de Lima.