Asesorías y Tutorías para la Investigación Científica en la Educación Puig-Salabarría S.C.
José María Pino Suárez 400-2 esq a Lerdo de Tejada. Toluca, Estado de México. 7223898475
RFC: ATI120618V12

Revista Dilemas Contemporáneos: Educación, Política y Valores.
http://www.dilemascontemporaneoseducacionpoliticayvalores.com/
Año: XII Número: 2 Artículo no.:37 Período: 1 de enero al 30 de abril del 2025

TÍTULO: Vulnerabilidad de los ciudadanos frente a amenazas cibernéticas.

AUTORES:

1. Máster. José Milton Jiménez Montenegro.
2. Est. Adanny Valentina Guerrero Naranjo.
3. Est. Daniela Lissbeth Tiñe Cando.

RESUMEN: La creciente incidencia de delitos cibernéticos en Ecuador ha representado una amenaza significativa para la seguridad de los ciudadanos; por tanto, este estudio se ha enfocado en analizar los desafíos y oportunidades en la protección de datos personales y la prevención del acoso cibernético frente a delitos como el spam y el phishing, al proponer estrategias para fortalecer la seguridad digital; para ello, se realizaron encuestas que revelaron el desconocimiento sobre la legislación vigente y la percepción de que las sanciones actuales son insuficientes. En conclusión, es prioritario fortalecer el marco legal y desarrollar campañas educativas que aumenten la conciencia pública sobre la seguridad digital, al acentuar la necesidad de una mayor protección frente a amenazas en el ciberespacio.

PALABRAS CLAVES: protección de datos, derechos digitales, delitos cibernéticos, marco legal.

TITLE: Citizen vulnerability to cyber threats.

AUTHORS:

1. Master. José Milton Jiménez Montenegro
2. Stud. Adanny Valentina Guerrero Naranjo
3. Stud. Daniela Lissbeth Tiñe Cando

ABSTRACT: The increasing incidence of cybercrime in Ecuador has represented a significant threat to the security of citizens. Therefore, this study has focused on analyzing the challenges and opportunities in the protection of personal data and the prevention of cyberbullying against crimes such as spam and phishing, by proposing strategies to strengthen digital security. To this end, surveys were carried out that revealed ignorance about current legislation and the perception that current sanctions are insufficient. In conclusion, it is a priority to strengthen the legal framework and develop educational campaigns that increase public awareness about digital security, by accentuating the need for greater protection against threats in cyberspace.

KEY WORDS: data protection, digital rights, cybercrime, legal framework.

INTRODUCCIÓN.

En la era digital, Ecuador enfrenta desafíos cada vez más complejos en materia de seguridad cibernética. Entre estos, el spam y el phishing delictivo han emergido como amenazas significativas que comprometen tanto la integridad de los datos personales como la seguridad en línea de sus ciudadanos (Flor-Unda et al., 2023).

Si bien el auge de las tecnologías de la información y la comunicación (TIC) ha impulsado avances sustanciales en conectividad y acceso a la información, también ha dado lugar a riesgos cibernéticos que requieren una atención urgente y estrategias específicas para su mitigación (Ayala-Chauvin et al., 2023) (Naqvi et al., 2023).

El incremento de estas amenazas resulta crucial debido a su creciente complejidad y al profundo impacto que tienen en individuos, organizaciones y la sociedad ecuatoriana en su conjunto (Ponce Tubay, 2024a). Lejos de ser una simple molestia, el spam se ha convertido en un vehículo eficaz para la propagación de malware (programas malignos) y fraudes. Mientras que el phishing supone un riesgo directo a la privacidad y a la seguridad financiera de los usuarios.

En cuanto a las estadísticas, datos recientes del Ministerio de Telecomunicaciones y de la Sociedad de la Información revelan, que en el año 2023, se registraron más de 40 millones de intentos de ciberataques en

Ecuador (Aleroud et al., 2020); de modo, que representa un alarmante incremento del 30% respecto al año anterior. Esta tendencia creciente amerita de medidas de protección existentes y de actualizar el marco jurídico para afrontar estas amenazas en constante evolución.

La situación se agrava al considerar el vínculo causal entre la sustracción de datos mediante técnicas de spam y phishing y su uso posterior en actos de acoso cibernético (Orunsolu et al., 2022). Este nexo plantea un desafío multidimensional para las autoridades y gobiernos de cada región. De forma que implica no solo la protección de los datos personales (Barahona-Martinez et al., 2024) (Andrade Armas et al., 2024), sino también la prevención y persecución de delitos derivados como el acoso, la extorsión y el fraude en línea (Coro & Barreto, 2024). Dada la complejidad de este fenómeno, se requiere un enfoque integral que abarque aspectos legales, tecnológicos y educativos.

Aunque la Constitución de Ecuador reconoce el derecho fundamental a la protección de datos personales, el marco legal actual presenta limitaciones significativas para su aplicación efectiva en el ciberespacio (Ponce Tubay, 2024b) (Ordóñez Córdova, 2024). La falta de una legislación específica y actualizada para enfrentar los delitos cibernéticos modernos deja a una gran parte de la población vulnerable ante amenazas que evolucionan rápidamente. Esta brecha legal no solo dificulta la persecución de los ciberdelincuentes, sino que también limita la implementación de medidas preventivas adecuadas.

En este entorno digital, el presente estudio tiene como objetivo analizar los desafíos y oportunidades en la protección de datos personales y la prevención del acoso cibernético en Ecuador, así como evaluar la efectividad del marco legal vigente frente a delitos como el spam y el phishing, con el fin de proponer estrategias que fortalezcan la seguridad digital y promuevan un entorno digital más seguro y confiable.

DESARROLLO.

Materiales y métodos.

Este estudio utilizó una metodología cuantitativa de tipo no experimental, con un diseño descriptivo y correlacional (Granikov et al., 2020). Esto permitió explorar la prevalencia y las características del spam y phishing delictivo, así como su relación con el acoso cibernético, sin manipular las variables de estudio. La

población objetivo estuvo conformada por residentes de Riobamba, Ecuador, de entre 18 y 35 años. La muestra incluyó a 29 participantes, seleccionados mediante un muestreo no probabilístico.

Para la recolección de datos, se aplicó una encuesta en línea a través de Google Forms, que contenía preguntas cerradas y abiertas. Este instrumento facilitó la obtención de datos cuantitativos sobre las experiencias de los participantes con el spam y phishing, y sus percepciones sobre la legislación y protección frente a estos delitos.

En cuanto a los métodos de investigación, el muestreo Bola de Nieve se eligió como estrategia principal debido a la sensibilidad del tema y la dificultad de identificar a las víctimas de ciberdelitos, así como permitir el acceso a una población difícil de alcanzar por otros medios (Zhang et al., 2023). Posteriormente, los datos cuantitativos obtenidos de las preguntas cerradas se analizaron mediante técnicas de estadística descriptiva, al calcular la frecuencias, porcentajes y medidas de tendencia central.

Para las preguntas abiertas, se utilizó el análisis de contenido, al permitir temas y patrones recurrentes en las respuestas de los participantes y brindar una comprensión de las experiencias y opiniones. Adicionalmente, se empleó un método comparativo, que contrastó los resultados obtenidos con la legislación vigente y las prácticas actuales en materia de ciberseguridad en Ecuador, con el fin de detectar brechas y áreas de mejora; por consiguiente, la combinación de estas metodologías permitió investigar el nexo causal entre la sustracción de datos y el acoso cibernético, al tiempo que se evaluó la efectividad de las medidas legales y de seguridad vigentes en Ecuador.

Resultados.

Los resultados de la Figura 1 muestran que el 51.7% de los encuestados han recibido correos electrónicos o mensajes de spam, al evidenciar una alta prevalencia de este problema en la muestra analizada. Esta cifra, aunque superior a la media global estimada, sugiere que los usuarios en Ecuador se encuentran expuestos a estas amenazas debido a una posible falta de filtros efectivos o menor conciencia sobre la seguridad digital.

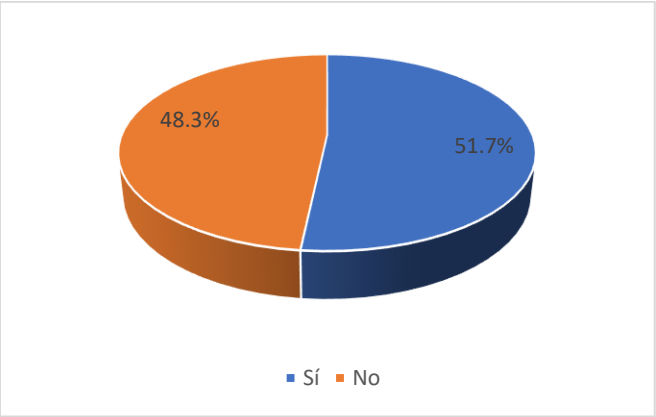

Figura 1: Prevalencia del spam en la muestra ecuatoriana. Fuente: Elaboración propia.

En la Figura 2, se observa que el 79.3% de los encuestados desconoce qué acciones legales pueden emprender si son víctimas de sustracción de datos personales. Este resultado refleja la falta de conocimiento sobre los mecanismos legales disponibles; de forma, que incrementa la vulnerabilidad frente a delitos cibernéticos como el phishing y el spam, en comparación con otros países con mayor madurez digital en términos de concientización pública sobre derechos digitales.

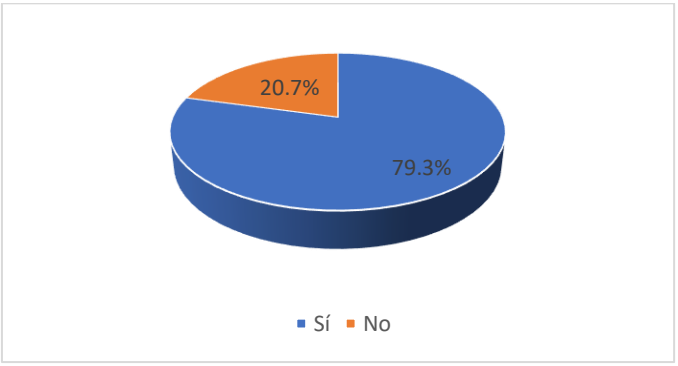

Figura 2: Desconocimiento sobre acciones legales frente a la sustracción de datos personales.

Fuente: Elaboración propia.

La Figura 3 revela que el 58.6% de los participantes no ha oído hablar de ninguna ley que proteja contra el acoso a través de mensajes de texto o llamadas. Este porcentaje de desconocimiento sobre las leyes de protección digital en Ecuador es preocupante y resalta la necesidad de educar a la población sobre los derechos y mecanismos de protección disponibles; de modo, que acentúan la falta de concienciación pública sobre los recursos legales existentes para combatir el acoso cibernético.

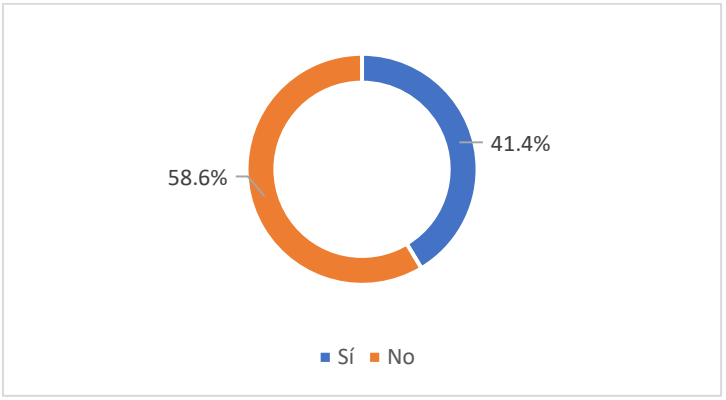

Figura 3: Falta de conocimiento sobre leyes contra el acoso digital en Ecuador.

Fuente: Elaboración propia.

Otro punto relevante se presenta en la Figura 4, donde el 79.3% de los encuestados considera que deberían existir jueces especializados en delitos por internet; de modo, que demuestra una fuerte demanda de especialización en el sistema judicial ecuatoriano para manejar de forma eficaz los delitos digitales. Este dato refleja la prioridad de reformar la estructura judicial actual para adaptarla mejor a los retos del entorno digital.

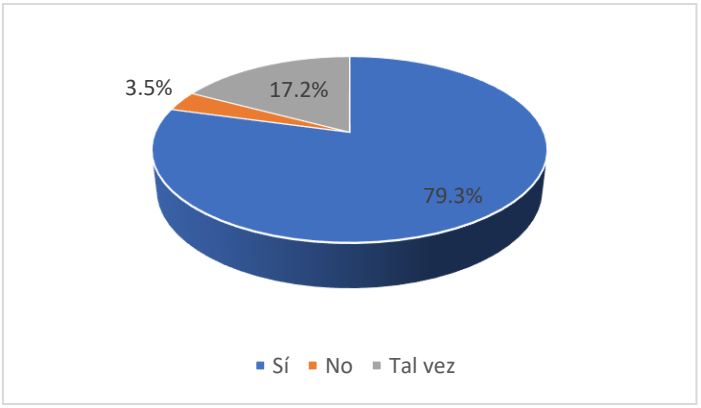

Figura 4: Opinión ciudadana sobre la necesidad de jueces especializados en delitos cibernéticos.

Fuente: Elaboración propia.

Según la Figura 5, el 51.7% de los encuestados considera que las penas actuales para los delitos de spam y phishing no son proporcionales al daño causado. Esta percepción pone de relieve la necesidad de revisar las sanciones legales en Ecuador para que sean más severas y disuasorias, alineándose con la gravedad del impacto que estos delitos tienen tanto a nivel personal como económico.

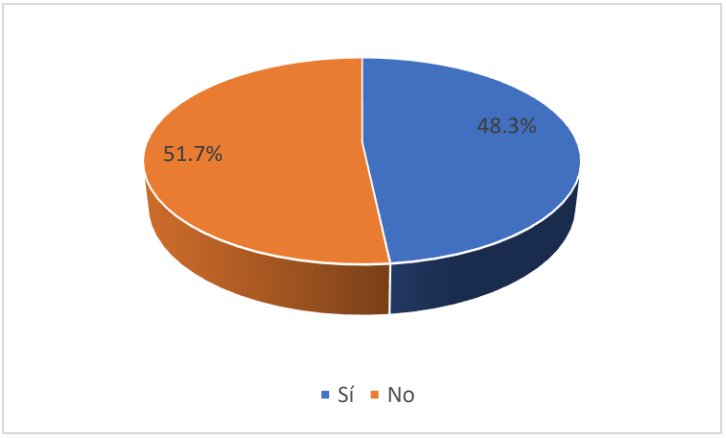

Figura 5: Percepción de la insuficiencia de las sanciones legales para delitos de spam y phishing.

Fuente: Elaboración propia.

La Figura 6 muestra que el 79.3% de los encuestados estaría de acuerdo con implementar medidas más estrictas de protección de datos; de tal manera, que señala una creciente preocupación entre los ciudadanos por la seguridad de su información personal y la demanda de medidas más contundentes por parte de las autoridades y organizaciones.

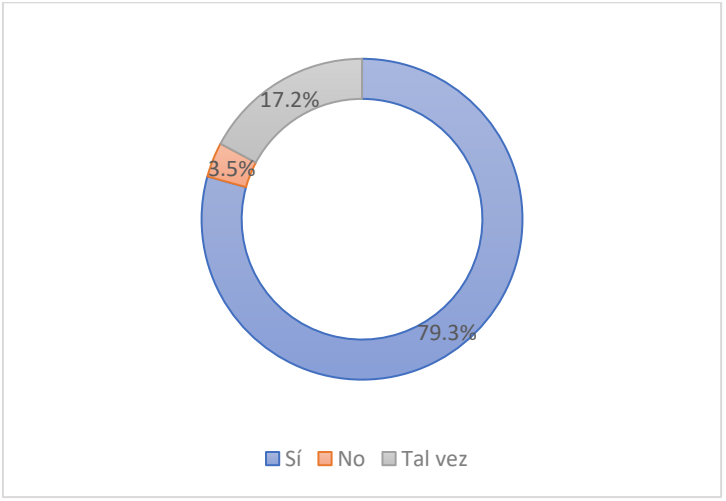

Figura 6: Implementación de medidas estrictas para la protección de datos personales.

Fuente: Elaboración propia.

La Figura 7 revela que el 96.6% de los encuestados cree que debería haber sanciones económicas para las empresas que no protegen adecuadamente los datos personales. Este resultado apunta la expectativa de que se apliquen sanciones efectivas a las empresas que no cumplan con las normativas de protección de datos;

de modo, que actuaría como un incentivo para mejorar las prácticas corporativas en materia de ciberseguridad.

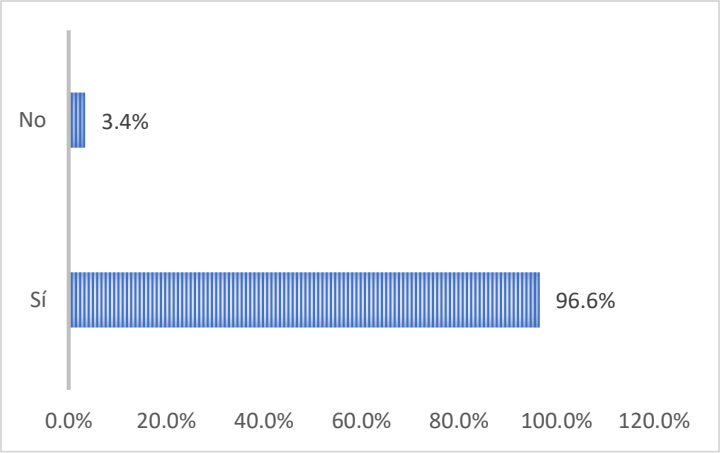

Figura 7: Aprobación de demandas para empresas que no protegen los datos personales.

Fuente: Elaboración propia.

En la Figura 8, se observa que el 62.1% de los participantes no tiene conocimiento sobre el derecho de Habeas Data. Esto refleja una carencia significativa de familiaridad con uno de los derechos clave en la protección de datos, al afectar la capacidad de los ciudadanos para defender sus derechos ante posibles violaciones.

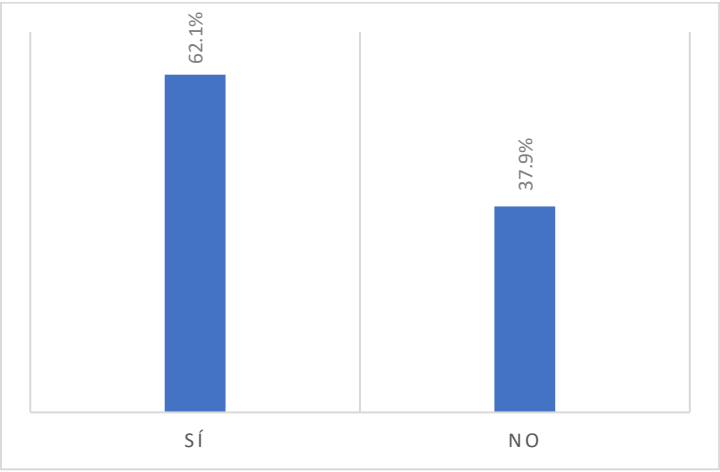

Figura 8: Falta de conocimiento sobre el derecho de Habeas Data en Ecuador. Fuente: Elaboración propia.

En cuanto a la Figura 9 muestra que el 86.2% de los encuestados cree que la evolución constante de las tácticas de los ciberdelincuentes complica la aplicación de la justicia, al poner de relieve los desafíos a los

que se enfrentan los sistemas judiciales en la era digital; además, la Figura 10 revela que el 93.1% de los encuestados considera que el spam puede dañar la reputación de una persona; de modo, que refuerza la prioridad de manejar el spam no solo desde una perspectiva de seguridad, sino también como un factor que afecta la imagen personal y profesional de los usuarios.

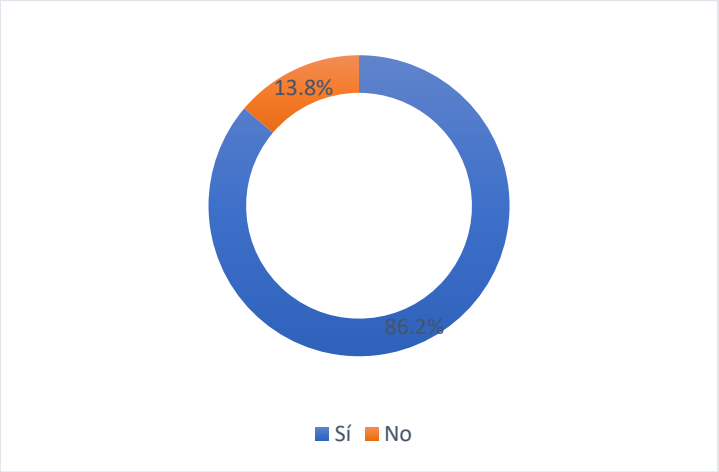

Figura 9: Dificultad de aplicar justicia ante la rápida evolución de las tácticas cibernéticas.

Fuente: Elaboración propia.

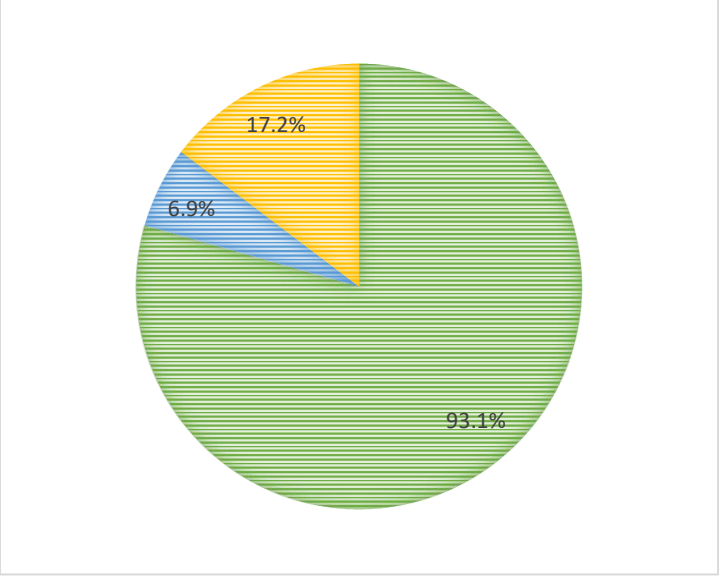

Figura 10: Percepción sobre el impacto del spam en la reputación personal.

Fuente: Elaboración propia.

En conjunto, los resultados de esta investigación muestran que Ecuador enfrenta grandes desafíos en la lucha contra los delitos cibernéticos; entre ellos, se destaca la prioridad de reformar tanto el marco legal como las políticas de concientización pública para mejorar la seguridad digital y la protección de los derechos de los ciudadanos en el entorno digital.

Conocimiento de la sociedad sobre el marco legal en Ecuador.

El nivel de conocimiento público sobre la legislación vigente en Ecuador relacionada con la protección de datos y los derechos digitales es considerablemente bajo, lo que genera preocupantes brechas en la conciencia ciudadana y expone a la población a riesgos crecientes en el entorno digital. De acuerdo con los resultados de estudios recientes, una gran mayoría de los ecuatorianos no tiene conocimiento claro sobre sus derechos en materia de protección de datos ni sobre las acciones legales que pueden emprender en casos de vulneraciones a su privacidad o acoso cibernético.

Uno de los factores clave que contribuyen a la falta de conocimiento es la limitada difusión de la legislación específica en torno a la protección de datos; por ejemplo, la Ley Orgánica de Protección de Datos Personales, aprobada en el año 2021, que aunque representa un avance significativo, no ha sido acompañada por campañas masivas de educación pública que expliquen su alcance. A esto se suma la falta de formación digital en general, al implicar a gran parte de la ciudadanía en la comprensión de las implicaciones de las normativas o cómo ejercer sus derechos.

Entre las principales brechas identificadas, destaca la falta de conciencia sobre la existencia de herramientas legales como el Habeas Data, que permite a los ciudadanos exigir la corrección o eliminación de datos personales incorrectos o mal utilizados. Este desconocimiento es grave, ya que limita el ejercicio de derechos fundamentales en la era digital. Adicionalmente, las encuestas indican que más de la mitad de la población no está informada sobre las leyes que protegen contra el spam, el phishing y el ciberacoso, lo que incrementa su vulnerabilidad ante estos delitos.

Los mecanismos de protección legal, aunque existentes, adolecen de una baja accesibilidad. Esto incluye la falta de jueces especializados en delitos cibernéticos y la percepción general de que las sanciones

impuestas no son proporcionales al daño causado. Esta debilidad estructural en el sistema judicial refuerza la percepción de que el entorno digital es un espacio de impunidad, lo que desalienta a las víctimas a denunciar y reclamar protección.

Propuestas de mejora dentro del marco legal ecuatoriano.

Para mejorar el marco legal ecuatoriano en la prevención y sanción de delitos cibernéticos, se deben implementar varias acciones estratégicas. En primer lugar, es esencial fortalecer la legislación específica que aborde el spam, el phishing y el acoso cibernético, basándose en modelos exitosos de otros países. Además, se debe crear juzgados especializados que permitan un manejo más eficiente de estos delitos, al capacitar a jueces en los aspectos técnicos y legales del cibercrimen; asimismo, es fundamental implementar campañas de educación y concienciación pública sobre seguridad digital, al integrar estos temas en los currículos escolares para formar a las nuevas generaciones.

Establecer mecanismos accesibles para la denuncia de delitos cibernéticos facilitaría que las víctimas reporten incidentes, lo que a su vez contribuiría a fomentar la confianza en el sistema legal. En este contexto, la colaboración internacional se vuelve crucial, ya que fortalecer acuerdos con otras naciones facilitaría la investigación y el enjuiciamiento de delitos que trascienden fronteras.

Es necesario revisar y actualizar las sanciones existentes para asegurarse de que sean disuasorias y proporcionales al daño causado; mientras que ofrecer incentivos a las empresas para que implementen medidas adecuadas de seguridad cibernética contribuiría a proteger la información de los usuarios. Finalmente, establecer mecanismos para la evaluación continua del marco legal aseguraría que la legislación se mantenga al día con las tendencias emergentes en el ámbito digital; de modo, que se cree así un entorno más seguro para los ciudadanos ecuatorianos frente a las amenazas cibernéticas.

Discusión.

Los resultados de este estudio resaltaron una desconexión notable entre la legislación vigente y la conciencia pública en Ecuador sobre la protección de datos y los derechos digitales.

La alta incidencia de spam y phishing observada en la población indicó una exposición considerable a riesgos cibernéticos, al respaldar la necesidad de adoptar un enfoque más riguroso en la regulación y el control de estas prácticas; además, el desconocimiento generalizado sobre las acciones legales que pueden emprender los ciudadanos reflejó una brecha crítica en la educación sobre derechos digitales.

Esta observación coincidió con investigaciones que documentaron que la falta de conocimiento sobre la legislación en ciberseguridad incrementa la vulnerabilidad ante el acoso cibernético y el fraude; asimismo, la percepción de que las sanciones actuales son insuficientes planteó preguntas sobre la efectividad del marco legal existente y su capacidad para disuadir actividades delictivas en línea.

La comparación con estudios realizados en otras jurisdicciones sugirió que una reforma legislativa es prioritaria para abordar esta disconformidad y aumentar la confianza de los ciudadanos en el sistema legal; en cambio, la demanda de jueces especializados en delitos cibernéticos destacó la necesidad de un enfoque más focalizado en el tratamiento de estas cuestiones legales emergentes. Esta inclinación hacia la especialización judicial ha sido respaldada por investigaciones que demuestran que sistemas judiciales capacitados en el ámbito digital tienden a ser más efectivos en la resolución de casos relacionados con cibercrimen.

La necesidad de actualizar el marco legal y de implementar estrategias educativas que fortalezcan la conciencia sobre la seguridad digital se presenta como una dirección crucial para el desarrollo de futuras políticas públicas; incluso, contribuye a crear un ecosistema digital más seguro y confiable en Ecuador, al fomentar el desarrollo socioeconómico en la era digital.

CONCLUSIONES.

La investigación ha evidenciado un alto nivel de desconocimiento entre los ciudadanos sobre la legislación vigente relacionada con la protección de datos y los derechos digitales en Ecuador. Este vacío de información ha incrementado la vulnerabilidad de la población ante amenazas cibernéticas, como el spam y el phishing. La falta de conciencia sobre los mecanismos legales disponibles para protegerse contra el

acoso cibernético resalta la necesidad urgente de campañas educativas que informen a los ciudadanos sobre sus derechos y las acciones que pueden emprender.

Las derivaciones del estudio han mostrado que la mayoría de los encuestados considera que las sanciones legales actuales para delitos cibernéticos son insuficientes. Este sentimiento ha resaltado una disconformidad generalizada con el marco legal existente, al sugerir que las medidas implementadas no logran disuadir eficazmente a los infractores; así, se propone la revisión y actualización de las normativas para asegurar que las penas sean proporcionales a la gravedad de los delitos, en línea con las mejores prácticas internacionales.

La alta demanda de jueces especializados en delitos cibernéticos ha quedado clara a partir de las respuestas de los encuestados. Esta observación sugiere la creación de tribunales o juzgados especializados en delitos informáticos para facilitar la resolución efectiva de casos y mejorar la confianza pública en la justicia en las dinámicas del ciberespacio.

REFERENCIAS BIBLIOGRÁFICAS.

1. Aleroud, A., Abu-Shanab, E., Al-Aiad, A., & Alshboul, Y. (2020). An examination of susceptibility to spear phishing cyber attacks in non-English speaking communities. Journal of Information Security and Applications, 55(December), 1-8. https://www.sciencedirect.com/science/article/pii/S2214212620307791
2. Andrade Armas, D., Toapanta Toapanta, M., Baño Hifong, M., & Gómez Díaz, E. (2024). Un enfoque de la inteligencia artificial para la protección de datos personales sustentado en la base legal : An artificial intelligence approach to personal data protection based on the legal basis. LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades, 5(4), 3808 – 3820. https://latam.redilat.org/index.php/lt/article/view/2530
3. Ayala-Chauvin, M., Avilés-Castillo, F., & Buele, J. (2023). Exploring the Landscape of Data Analysis: A Review of Its Application and Impact in Ecuador. Computers, 12(7), 146. https://www.mdpi.com/2073-431X/12/7/146

4. Barahona-Martinez, G. E., Barzola-Plúas, Y. G., & Peñafiel-Muñoz, L. V. (2024). El derecho a la protección de datos y el avance de las nuevas tecnologías en Ecuador: Implicaciones legales y éticas. Journal of Economic and Social Science Research, 4(3), 46-64. https://economicsocialresearch.com/index.php/home/article/view/113
5. Coro, J. E. O., & Barreto, W. E. R. (2024). El ciberacoso en Ecuador: Análisis comparado con la Legislación Española. Emergentes-Revista Científica, 4(3), 96-113. https://revistaemergentes.org/index.php/cts/article/view/204
6. Flor-Unda, O., Simbaña, F., Larriva-Novo, X., Acuña, Á., Tipán, R., & Acosta-Vargas, P. (2023). A Comprehensive Analysis of the Worst Cybersecurity Vulnerabilities in Latin America. Informatics, 10(3), 71. https://www.mdpi.com/2227-9709/10/3/71
7. Granikov, V., Hong, Q. N., Crist, E., & Pluye, P. (2020). Mixed methods research in library and information science: A methodological review. Library & Information Science Research, 42(1), 3-6. https://www.sciencedirect.com/science/article/abs/pii/S0740818819302294
8. Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S., & Porras, J. (2023). Mitigation strategies against the phishing attacks: A systematic literature review. Computers & Security, 132(September), 2-14. https://www.sciencedirect.com/science/article/pii/S0167404823002973
9. Ordóñez Córdova, L. A. (2024). El Marco Legal de los Delitos Cibernéticos en Ecuador. Reincisol., 3(5), 1447-1469. https://www.reincisol.com/ojs/index.php/reincisol/article/view/158
10. Orunsolu, A. A., Sodiya, A. S., & Akinwale, A. (2022). A predictive model for phishing detection. Journal of King Saud University-Computer and Information Sciences, 34(2), 232-247. https://www.sciencedirect.com/science/article/pii/S1319157819304902
11. Ponce Tubay, M. A. (2024a). Delitos informáticos: Caso Ecuador. Revista San Gregorio, 1(58), 119-123. https://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/article/view/2667
12. Ponce Tubay, M. A. (2024b). Desafíos y respuestas legales ante los delitos informáticos en Ecuador. Revista San Gregorio, 1(58), 111-118.

http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S2528-79072024000200111

13. Zhang, C., Tian, L., & Chu, H. (2023). Usage frequency and application variety of research methods in library and information science: Continuous investigation from 1991 to 2021. Information Processing and Management, 60(6), 4-8. https://www.sciencedirect.com/science/article/abs/pii/S0306457323002443

DATOS DE LOS AUTORES.

1. **José Milton Jiménez Montenegro.** Magister en Docencia Universitaria Mención Ciencias Jurídicas. Docente de la Universidad Regional Autónoma de Los Andes**,** Sede Riobamba, Ecuador**.** E-mail: ur.josejimenez@uniandes.edu.ec
2. **Adanny Valentina Guerrero Naranjo.** Estudiante de la Universidad Regional Autónoma de Los Andes, Sede Riobamba, Ecuador**.** E-mail: adannygn82@uniandes.edu.ec
3. **Daniela Lissbeth Tiñe Cando**. Estudiante de la Universidad Regional Autónoma de Los Andes, Sede Riobamba, Ecuador**.** E-mail: danielatc25@uniandes.edu.ec

RECIBIDO: 10 de septiembre del 2024. **APROBADO:** 6 de octubre del 2024.