CIENCIAMATRIA
Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología
Año XI. Vol. XI. N°3. Edición Especial III. 2025
Hecho el depósito de ley: pp201602FA4721
ISSN-L: 2542-3029; ISSN: 2610-802X
Instituto de Investigación y Estudios Avanzados Koinonía. (IIEAK). Santa Ana de Coro. Venezuela

DOI 10.35381/cm.v11i3.1950

La ciberseguridad frente a los delitos informáticos en las entidades financieras

Cybersecurity against cybercrime in financial institutions

Nathaly Kasandra Moncayo-Morlas
nathalymm31@uniandes.edu.ec
Universidad Regional Autónoma de Los Andes, Quevedo, Los Ríos
Ecuador
https://orcid.org/0000-0002-5297-2894

Adriana Mercedes Salazar-Obando
dq.adrianamso11@uniandes.edu.ec
Universidad Regional Autónoma de Los Andes, Quevedo, Los Ríos
Ecuador
https://orcid.org/0000-0001-5817-5223

Dionisio Ponce-Ruiz
uq.dionisioponce@uniandes.edu.ec
Universidad Regional Autónoma de Los Andes, Quevedo, Los Ríos
Ecuador
https://orcid.org/0000-0002-5712-4376

Deinier Ros-Álvarez
uq.deinierra09@uniandes.edu.ec
Universidad Regional Autónoma de Los Andes, Quevedo, Los Ríos
Ecuador
https://orcid.org/0000-0002-1531-3355

Recibido: 20 de agosto 2025
Revisado: 10 de octubre 2025
Aprobado: 15 de noviembre 2025
Publicado: 01 de diciembre 2025

CIENCIAMATRIA
Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología
Año XI. Vol. XI. N°3. Edición Especial III. 2025
Hecho el depósito de ley: pp201602FA4721
ISSN-L: 2542-3029; ISSN: 2610-802X
Instituto de Investigación y Estudios Avanzados Koinonía. (IIEAK). Santa Ana de Coro. Venezuela

RESUMEN

El objetivo general de la investigación fue analizar la ciberseguridad frente a los delitos informáticos en las entidades financieras. La investigación utilizó el método cuantitativo el cual produce datos descriptivos, que se originan por la recolección de datos. Se apoyó en la revisión documental-bibliográfica. Además, se aplicó el método inductivo-deductivo, y analítico-sintético. Se aplicó demás un cuestionario a usuarios, encargados de la seguridad informática de las entidades bancarias, además de los agentes de la policía nacional. Se concluye que, las inversiones en ciberseguridad, producen confianza en los clientes, lo cual es un elemento fundamental para la sostenibilidad de las entidades financieras. La puesta en marcha de programas para capacitar a los trabajadores, la supervisión en tiempo real y la autenticación multifactor son tácticas primordiales para reducir los peligros.

Descriptores: Delito informático; cibercrimen; ley. (Tesauro UNESCO)

ABSTRACT

The overall objective of the research was to analyze cybersecurity against cybercrime in financial institutions. The research used the quantitative method, which produces descriptive data originating from data collection. It was supported by a documentary-bibliographic review. In addition, the inductive-deductive and analytical-synthetic methods were applied. A questionnaire was also administered to users, those responsible for IT security at banking institutions, and national police officers. It was concluded that investments in cybersecurity build customer trust, which is a fundamental element for the sustainability of financial institutions. The implementation of employee training programs, real-time monitoring, and multi-factor authentication are key tactics for reducing risks.

Descriptors: Computer crime; cybercrime; law. (UNESCO Thesaurus)

INTRODUCCIÓN

Las instituciones bancarias tienen la capacidad de optimizar y supervisar las acciones financieras que sus clientes llevan a cabo diariamente: el cumplimiento de regulaciones y normativas, la gestión del efectivo, la atención de reclamaciones y consultas, así como el procesamiento de transacciones tanto en sucursales bancarias como por vías electrónicas. Por lo tanto, a medida que avanza la tecnología, entidades financieras como los bancos y las cooperativas han incorporado herramientas digitales, como la banca web o móvil, para facilitar a sus usuarios las operaciones realizadas en el banco o cooperativa. Teniendo la posibilidad de hacerlo desde casa, en la actualidad los usuarios suelen rechazar las aplicaciones móviles debido a su preocupación por el malestar social que enfrentan. Por ello, este estudio se enfoca en analizar delitos informáticos como fraudes electrónicos y ciberataques que golpean tanto a entidades bancarias como a clientes, además de la seguridad que brindan los servicios financieros ofrecidos en las instituciones financieras del Cantón Quevedo.

En Ecuador, el acceso no autorizado a los sistemas, el fraude cibernético y el robo de identidad están regulados por la Ley de Comercio Electrónico (2002), la Ley de Protección de Datos Personales (2021) y el Código Orgánico Integral Penal (2014). No obstante, la mayor dificultad está en poner en práctica estas políticas a nivel local de manera efectiva. Por ende, es crucial analizar el rendimiento en términos de ciberseguridad de las entidades financieras del Cantón Quevedo para detectar debilidades en la seguridad.

La ciberseguridad se ha convertido en un ámbito fundamental para proteger la información digital, particularmente en el sector financiero, donde los delitos informáticos han aumentado como consecuencia de la digitalización de los servicios. Los delitos como el malware, el phishing y las intrusiones en redes suponen una amenaza para la confidencialidad, integridad y disponibilidad de los datos, lo que perjudica a los usuarios y a las instituciones.

Los delitos cibernéticos, desde el campo legal, son una realidad nueva que reta a las leyes tradicionales. A pesar de que en Ecuador se han incluido disposiciones sobre delitos cibernéticos (artículos 232-233) en el Código Orgánico Integral Penal (COIP), siguen existiendo vacíos legales en lo que respecta a la prevención de la ciberseguridad en las instituciones financieras.

A través de marcos jurídicos integrales y colaboración internacional, entidades como la OEA (2023) fomentan el fortalecimiento de la ciberseguridad. Esta investigación tiene como objetivo sugerir tácticas jurídicas y tecnológicas que fortalezcan la protección digital en Ecuador, con el fin de asegurar la seguridad de los servicios financieros digitales y promover la confianza de los usuarios en las plataformas tecnológicas.

En tal sentido, los usuarios deben ser conscientes de que su consentimiento es fundamental y debe ser explicado de forma clara por la entidad solicitante, y que poseen derechos de eliminación u oposición al tratamiento de sus datos. La cesión no consentida es la principal vía de vulneración de estos derechos. (Torres-Ocampo et. al.,2023).

Por otro lado, se define a los ciberdelitos como conductas complejas que utilizan la tecnología para transgredir bienes jurídicos como la propiedad, la economía y la privacidad. Una característica clave es su transnacionalidad, que permite al delincuente cometer el acto desde cualquier lugar sin presencia física. (Posso-López et al.,2023).

En tal sentido, la ciberseguridad ha adquirido una importancia particular en las instituciones financieras debido al aumento de la digitalización de los servicios y del número de delitos informáticos. Es un deber tanto legal como ético proteger la información delicada de los usuarios, lo cual tiene un impacto directo en la estabilidad del sistema financiero (Gonzáles, 2023). Además, iniciativas como la Estrategia Nacional de Ciberseguridad del Ecuador fue implementada en 2022 por el Ministerio de Telecomunicaciones y de la Sociedad de la Información.

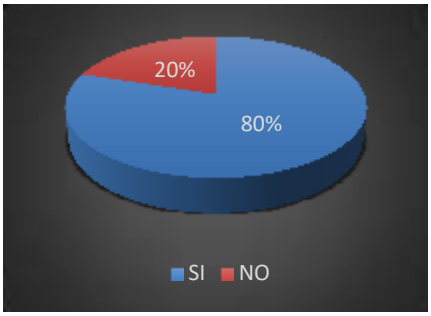
Se plantea como objetivo general de la investigación analizar la ciberseguridad frente a los delitos informáticos en las entidades financieras.

MÉTODO

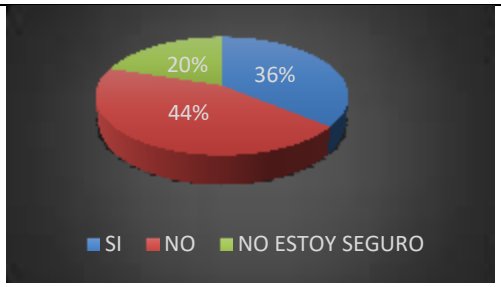
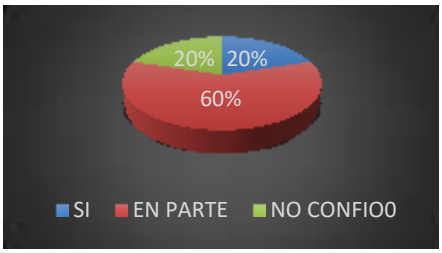
La investigación utiliza el método cuantitativo el cual produce datos descriptivos, que se originan por la recolección de datos. Apoyado en la revisión documental-bibliográfica. Además, se aplica el método inductivo-deductivo, el cual sugiere que para encontrar una verdad se deben buscar los hechos y no basarse en meras especulaciones, además de partir de afirmaciones generales para llegar a específicas (Dávila, 2006). Se plantea además el método analítico-sintético por medio del cual, se descompone un todo en partes extrayendo cualidades, componentes, relaciones y más para posteriormente unir las partes analizadas y con ello descubrir características y relaciones entre los elementos (Rodríguez y Pérez, 2017). Se aplica demás un cuestionario a usuarios, encargados de la seguridad informática de las entidades bancarias, además de los agentes de la policía nacional.

RESULTADOS

Se presentan a continuación los resultados obtenidos.

¿Ha escuchado hablar sobre el término ciberseguridad en el contexto de servicios financieros?	¿Considera que las entidades financieras en Quevedo implementan medidas suficientes de ciberseguridad en sus sistemas financieros?
	

CIENCIAMATRIA
Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología
Año XI. Vol. XI. N°3. Edición Especial III. 2025
Hecho el depósito de ley: pp201602FA4721
ISSN-L: 2542-3029; ISSN: 2610-802X
Instituto de Investigación y Estudios Avanzados Koinonía. (IIEAK). Santa Ana de Coro. Venezuela

El 80% de los encuestados afirma haber escuchado sobre la ciberseguridad en el ámbito financiero, lo que indica un alto nivel de familiaridad con el término. Sin embargo, el 20% que no lo conoce evidencia la necesidad de mayor difusión y educación sobre este tema.	 El 44% de los encuestados considera que las medidas de ciberseguridad no son suficientes, mientras que solo el 36% cree que sí lo son. Un 20% no está seguro, lo que refleja la percepción de inseguridad entre los usuarios de los servicios financieros digitales.
¿Confía en las medidas de seguridad que ofrecen las entidades financieras en Quevedo?  El 60% de los encuestados confía solo "en parte" en las medidas de seguridad bancaria, mientras que el 20% no confía en absoluto. Esto sugiere que las entidades financieras	¿Considera que las aplicaciones móviles de los bancos son seguras?  Si bien el 44% de los encuestados cree que las aplicaciones bancarias son seguras, un 36% considera que no lo son y un 20% no está seguro, lo que refleja una falta de confianza generalizada en estas plataformas.

deben reforzar su seguridad y mejorar la comunicación sobre las medidas de protección que implementan.	

Elaboración: Los autores.

Estudiar las conclusiones de la encuesta sobre ciberseguridad en instituciones financieras del cantón Quevedo facilita el reconocimiento de inquietudes y tendencias particulares entre los habitantes en relación con los delitos informáticos. En primer lugar, se observa que una gran parte de los encuestados ha oído hablar del concepto de ciberseguridad. Esto indica que la conciencia sobre la relevancia de la protección digital está aumentando en la sociedad. Sin embargo, los resultados también reflejan que un porcentaje considerable de los encuestados se siente poco informado sobre los riesgos de los delitos financieros en plataformas digitales.

La confianza en las medidas de seguridad de las instituciones financieras es otro elemento que causa inquietud. El sondeo revela que gran parte de los usuarios tiene confianza parcial en las medidas de seguridad bancarias, lo cual sugiere que el escepticismo sobre la eficacia de las tácticas puestas en marcha sigue existiendo.

Además, la ausencia de colaboración entre los bancos y las autoridades puede obstaculizar la lucha contra los delitos cibernéticos, según los datos. Un enfoque cooperativo entre las entidades gubernamentales y el sector financiero es necesario para abordar los delitos cibernéticos. La percepción de vulnerabilidad en las transacciones digitales es otro punto importante. Los encuestados manifestaron que, aunque las aplicaciones de los bancos ofrecen medidas de seguridad, todavía temen ser víctimas de fraude.

El análisis de la encuesta revela que, a pesar de que está aumentando la inquietud por

la ciberseguridad en el sector financiero de Quevedo, todavía se presentan retos en cuanto a educación digital, confianza institucional y cooperación entre entidades bancarias y autoridades. Para reducir los riesgos, se aconseja optimizar la comunicación con los clientes, implementar tecnologías de vanguardia para detectar fraudes y fortalecer las regulaciones.

DISCUSIÓN

Los resultados de este estudio demuestran que la ciberseguridad en el sector financiero del cantón Quevedo se enfrenta a retos importantes en lo que respecta a la protección de datos y la prevención de crímenes informáticos. A pesar de que se ha determinado que la mayor parte de los usuarios está al tanto acerca de lo importante que es la ciberseguridad, esto no implica necesariamente que practiquen acciones seguras, lo cual indica que la educación y sensibilización sobre cómo utilizar correctamente las herramientas digitales continúan siendo deficientes. Este hallazgo está de acuerdo con investigaciones anteriores que indican la importancia de fortalecer la cultura de seguridad digital en las entidades financieras y en la sociedad en su conjunto.

La percepción de los encuestados en relación con la insuficiencia de las medidas de seguridad aplicadas por las entidades bancarias locales es un elemento alarmante. La percepción de ser vulnerables frente a potenciales ataques cibernéticos y la falta de confianza en los sistemas de protección evidencian una brecha entre las políticas de seguridad institucional y la experiencia que viven realmente los clientes. La confianza de los usuarios puede crecer y la cantidad de fraudes financieros puede disminuir si se ponen en práctica protocolos avanzados, como la cifrado de datos y la autenticación multifactor. Otro descubrimiento importante es la ausencia de información precisa acerca de los peligros que representan los delitos informáticos en las plataformas digitales. Los datos de la encuesta indican que una gran cantidad de usuarios no conocen las maneras más habituales de fraude y el modo de protegerse frente a ellas.

En este contexto, es evidente que las instituciones financieras deben no solamente fortalecer sus sistemas de seguridad, sino también elaborar estrategias educativas para empoderar a los usuarios en la utilización segura de sus plataformas digitales. Esto ha sido evidenciado por estudios internacionales. El análisis también demostró que una porción importante de la población ha sido blanco de estafas financieras en línea, lo cual confirma el peligro en aumento que suponen los delitos informáticos en la industria bancaria. Específicamente en contextos con regulaciones débiles o donde la respuesta institucional no es efectiva, este problema es especialmente serio. En este contexto, los hallazgos obtenidos coinciden con estudios anteriores que indican que una capacidad de respuesta institucional insuficiente y la ausencia de un marco normativo robusto pueden aumentar la frecuencia de esta clase de crímenes.

La poca aplicación de mecanismos de seguridad eficaces, como la autenticación de doble factor, es uno de los factores más importantes que contribuyen a la vulnerabilidad del usuario. Aunque se trata de una de las tácticas más aconsejadas para proteger cuentas bancarias, la información indica que un porcentaje elevado de los clientes no la emplea o no sabe que existe. Esto demuestra la necesidad de promover más el uso de las herramientas de ciberseguridad existentes, así como de fomentar su empleo a través de campañas informativas y capacitaciones.

Por otra parte, la falta de satisfacción de los clientes con las políticas que sus bancos tienen contra el fraude es un factor que aumenta la desconfianza en el sistema financiero. La impresión de que las instituciones bancarias no reaccionan apropiadamente frente a casos de fraude puede tener un efecto perjudicial en la adopción de servicios digitales y en la estabilidad del sector financiero. En esta línea, es esencial que los bancos mejoren sus protocolos para atender al cliente y ofrezcan soluciones más rápidas y efectivas ante incidentes relacionados con la ciberseguridad.

El análisis además determinó que la escasa cooperación entre los bancos y las autoridades judiciales en el seguimiento de delitos informáticos representa una barrera

principal para luchar contra el fraude financiero. La falta de coordinación entre instituciones obstaculiza el reconocimiento y castigo de los ciberdelincuentes, lo que fomenta la impunidad y la repetición de estos delitos. Para mejorar esta circunstancia, se deben implementar mecanismos de colaboración más eficientes entre los entes de justicia y seguridad y el sector financiero.

CONCLUSIONES

Las inversiones en ciberseguridad, producen confianza en los clientes, lo cual es un elemento fundamental para la sostenibilidad de las entidades financieras. La puesta en marcha de programas para capacitar a los trabajadores, la supervisión en tiempo real y la autenticación multifactor son tácticas primordiales para reducir los peligros.

Respecto a las herramientas de seguridad, se notó que gran cantidad de usuarios no hacen uso de la autenticación de dos factores en sus transacciones digitales o ni siquiera saben que existe. Esto supone una vulnerabilidad seria, pues la verificación de dos pasos es uno de los métodos más eficaces para impedir el acceso no autorizado y las estafas en línea.

FINANCIAMIENTO

No monetario.

AGRADECIMIENTO

A la Universidad Regional Autónoma de Los Andes, en el desarrollo de la investigación.

REFERENCIAS CONSULTADAS

Asamblea Nacional (2014). Código Orgánico Integral Penal. Registro Oficial Nº 180. https://url2.cl/53c6h

Asamblea Nacional de la República del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales. Quinto Suplemento Nº 459 - Registro Oficial. Recuperado de:

https://n9.cl/mv7ow

Congreso Nacional. (2002). Ley de Comercio Electrónico, Firmas y Mensajes de Datos. Ley 67. Registro Oficial Suplemento 557 de 17-abr-2002. Estado: Vigente. https://n9.cl/l1srj

Dávila Newman, G. (2006). El razonamiento inductivo y deductivo dentro del proceso investigativo en ciencias experimentales y sociales. Laurus*, 12*(Ext),180-205. https://n9.cl/nx847

González, L. (2023). La protección de la información sensible de los usuarios es una obligación legal y ética que impacta directamente en la estabilidad del sistema financiero. *Seguridad Digital*, 9(1), 102–110.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2022). Estrategia Nacional de Ciberseguridad del Ecuador. https://n9.cl/1v5mo

OEA. (2023). Programa de Ciberseguridad. https://n9.cl/dhv5tq

Posso-López, D. F., Granja-Zurita, D. F., & Estupiñan-Ricardo, J. (2023). Delitos informáticos transnacionales y su incidencia en la impunidad. IUSTITIA SOCIALIS, 8(1), 1518–1525. https://doi.org/10.35381/racji.v8i1.3328

Rodríguez Jiménez, A., y Pérez Jacinto, A. O. (2017). Métodos científicos de indagación y de construcción del conocimiento. *Revista Ean*, (82),175–195. https://doi.org/10.21158/01208160.n82.2017.1647

Torres-Ocampo, T. A., Ros Álvarez, D., & Ojeda-Sotomayor, P. M. (2023). Vulneración del derecho a la protección de datos e intimidad por cesión de información personal. *IUSTITIA SOCIALIS, 8*(1), 184–193. https://doi.org/10.35381/racji.v8i1.2505