EVALUACIÓN DEL ESTADO DE LA CIBERSEGURIDAD EN EL USO DE CRIPTOMONEDAS EN BOLIVIA

ASSESSMENT OF THE STATE OF CYBERSECURITY IN THE USE OF CRYPTOCURRENCIES IN BOLIVIA

Deyler Roca Malale
Universidad San Francisco Xavier de Chuquisaca
roca.deyler@usfx.bo

Recibido: 29 Abril 2025 / Revisado: 13 Agosto 2025 / Aceptado: 2 Septiembre 2025 / Publicado: 23 Septiembre 2025

Resumen

El presente artículo analiza la situación actual de la ciberseguridad en el uso de criptomonedas dentro del contexto boliviano. Se examinan el marco legal y regulatorio, las tecnologías subyacentes, los riesgos y amenazas, y la infraestructura de seguridad en instituciones financieras nacionales. Además, se discuten prácticas recomendadas para la protección de usuarios y plataformas, se evalúan impactos económicos y sociales ante incidentes de seguridad, y se vislumbran los desafíos y oportunidades futuras para la ciberseguridad de criptomonedas en el país. El estudio busca contribuir al entendimiento de un ecosistema emergente, subrayando la relevancia de la seguridad digital en la consolidación de una economía más sólida, inclusiva y confiable.

Palabras clave: Criptomonedas, ciberseguridad, regulación, Bolivia, blockchain.

Introducción

El uso de criptomonedas en Bolivia se encuentra en una etapa emergente y rodeado de un entorno regulatorio restrictivo. A pesar de la prohibición establecida por el Banco Central de Bolivia (BCB) en 2014 sobre el uso de monedas digitales no reguladas (Vigna, P., & Casey, M. J. (2015))., existe una creciente comunidad de usuarios que acceden a estos activos a través de plataformas internacionales. Sin embargo, esta situación plantea serios desafíos en términos de ciberseguridad, debido a la falta de infraestructura local de protección, ausencia de normativa de seguridad específica y la exposición de los usuarios a múltiples amenazas cibernéticas.

En términos generales, la ciberseguridad aplicada a las criptomonedas se centra en la protección de los sistemas, redes y datos que permiten su funcionamiento, asegurando la integridad, confidencialidad y disponibilidad de las transacciones (Narayanan et al., 2016). En el contexto boliviano, la seguridad en este ecosistema depende de diversos factores, entre ellos: la formación de los usuarios en medidas de

protección, la adopción de buenas prácticas de seguridad por parte de las plataformas utilizadas, y la capacidad del Estado para generar mecanismos que mitiguen los riesgos asociados a delitos informáticos vinculados con el uso de criptomonedas.

A nivel mundial, las criptomonedas han sido blanco de múltiples ataques cibernéticos, incluyendo hackeos a plataformas de intercambio, robos de credenciales, fraudes en esquemas piramidales y estafas de phishing (Bohr & Bashir, 2014). En Bolivia, la falta de regulación y de un mercado legal de criptomonedas genera un escenario de incertidumbre donde los usuarios no cuentan con mecanismos de protección ni garantías en caso de incidentes de ciberseguridad. A nivel de infraestructura tecnológica, Bolivia enfrenta varios desafíos en la implementación de medidas de ciberseguridad que protejan a los usuarios de criptomonedas.

La ausencia de regulaciones claras y de una infraestructura sólida de ciberseguridad puede generar múltiples impactos negativos en la adopción de criptomonedas en Bolivia. En el ámbito local el uso de la moneda virtual no está normado aún, porque de acuerdo con la resolución emitida por el Banco Central de Bolivia en 06/05/2014 y nota de prensa de fecha 29/06/2019 en la cual se verifica que aún no está normado ni autorizado el uso de este tipo de moneda virtual para el intercambio de bienes y servicios. Pero estos aspectos legales no han podido detener a emprendimientos privados que promueven el uso de estos “Criptoactivos”, denominación que se usa actualmente mientras no esté regulado o respaldado por parte del estado por medio de la instancia reguladora BCB.

Para mitigar estos riesgos, Bolivia requiere una estrategia integral de ciberseguridad enfocada en la protección de usuarios y el fortalecimiento del ecosistema digital, he aquí de donde parte este artículo de investigación y por todos los motivos expuestos líneas arriba.

Estudios relacionados

Existe documentación relacionado a este tema en el ámbito nacional e internacional tal como se muestra en los siguientes trabajos, los cuales se toma como base.

1. **"Regulación jurídica del bitcoin y criptomonedas en Bolivia y análisis técnicos de mercados financieros"**

Esta investigación doctoral se centra en la regulación jurídica del Bitcoin y otras criptomonedas, evaluando su potencial impacto en la economía boliviana. Examina la necesidad de regular estos activos digitales, cómo debería hacerse y quiénes deberían tener la autoridad para ello. Además, analiza la eficiencia y seguridad de las criptomonedas en comparación con otras formas de dinero y su viabilidad como medio de pago y reserva de valor [4].

2. **"Causas por las que el Bitcoin no se aplica en Bolivia"**

Este artículo explora las razones por las cuales Bolivia rechaza la adopción del Bitcoin como moneda digital. Analiza factores como el papel de las autoridades, la falta de educación financiera, la ausencia de legislación específica y los riesgos asociados a estafas piramidales financieras [5].

3. **"Análisis de las estafas piramidales con criptomonedas: El caso desmantelado por la Policía Nacional en España"**

Este estudio examina una macroestafa piramidal que involucró a más de 3,600 víctimas y un fraude de aproximadamente 37.2 millones de euros en España. Analiza cómo los estafadores crearon una plataforma que ofrecía inversiones en bitcoins con rentabilidades irreales, destacando la

importancia de la educación financiera y la verificación de la legalidad de las plataformas de inversión para prevenir este tipo de fraudes [6].

Objetivos

La definición de los objetivos principales implica tomar en cuenta los criterios principales que tienen que ser desarrollados hasta la conclusión del presente artículo, como una herramienta inicial para evaluación del estado de la ciberseguridad en el uso de criptomonedas en Bolivia con este tipo de activos de intercambio de valor en criptomonedas, por lo que se ha concluido en los siguientes objetivos:

Objetivo principal

Evaluar el estado de la ciberseguridad en el uso de criptomonedas en Bolivia, identificando riesgos, desafíos y oportunidades para su adopción segura en el contexto nacional.

Objetivos secundarios

- Examinar el marco regulatorio y normativo en Bolivia relacionado con las criptomonedas y su impacto en la seguridad digital de los usuarios.
- Identificar los principales riesgos y amenazas de ciberseguridad asociados al uso de criptomonedas en Bolivia, incluyendo fraudes, estafas y ataques cibernéticos.
- Proponer estrategias de ciberseguridad para proteger las infraestructuras críticas, y mejores prácticas para fortalecer la seguridad en el uso de criptomonedas, tanto para usuarios individuales como para instituciones financieras y organismos reguladores.

Para llegar a cumplir con los objetivos tanto secundarios como el objetivo principal, se han identificados dos variables:

VI→ Evaluación del estado de la ciberseguridad en el uso de criptomonedas en Bolivia

VD→ Impacto de proponer estrategias de ciberseguridad para proteger las infraestructuras críticas, y mejores prácticas para fortalecer la seguridad en el uso de criptomonedas en Bolivia.

Metodología

La investigación se basa en un diseño de enfoque mixto, que combina métodos cualitativos y cuantitativos para una comprensión holística del fenómeno de la ciberseguridad en el uso de criptoactivos en Bolivia. Se adopta un enfoque descriptivo y explicativo para analizar las relaciones entre el conocimiento en ciberseguridad de los usuarios y su exposición a riesgos.

Para la fase cuantitativa, se estableció como población a los usuarios de criptoactivos en Bolivia. Dado el carácter emergente del ecosistema y la ausencia de un marco censal, se optó por un muestreo intencional o por criterios. Justificando su uso para la exploración de actitudes y percepciones en un contexto de investigación incipiente a profesionales del área de ciberseguridad. Se aplicarán encuestas dirigidas a usuarios de criptomonedas en Bolivia para evaluar sus conocimientos en ciberseguridad, la frecuencia con la que han sido víctimas de ataques y las medidas de protección que utilizan. También se analizarán datos estadísticos sobre ciberataques en el país. Se aplicó una encuesta en línea a una muestra de 200 encuestados, un tamaño que se considera mínimo, todo esto para asegurar la validez estadística de los hallazgos preliminares.

Los datos se analizaron utilizando estadística descriptiva para reportar frecuencias y porcentajes.

Para la fase cualitativa, se complementó la información con un análisis documental exhaustivo de regulaciones nacionales e internacionales sobre ciberseguridad y criptomonedas en Bolivia, y se realizaron estudios de caso enfocados en incidentes de ciberseguridad.

Para cada caso, se documentaron la fecha, fuente, indicadores de compromiso y, cuando fue posible, se aplicó la taxonomía del marco de referencia MITRE ATT&CK para clasificar las tácticas y técnicas de los atacantes. Al mismo tiempo que se aplicarán entrevistas a expertos en ciberseguridad, reguladores financieros y usuarios frecuentes de criptomonedas.

El tipo de Investigación a utilizar en el presente trabajo es el descriptivo, ya que se adapta a nuestra investigación puesto que las investigaciones tipo descriptivas miden o recolectan datos, y reportan información sobre diversos conceptos, variables, aspectos, dimensiones o componentes del fenómeno o problema a investigar, y en este trabajo de investigación se realizara un análisis y/o evaluación del estado actual de la ciberseguridad en el uso de criptomonedas en Bolivia, identificando principales riesgos y amenazas para posteriormente emitir un criterio y/o estrategia de ciberseguridad para proteger las infraestructuras críticas, y mejores prácticas para fortalecer la seguridad en el uso de criptomonedas en el país.

También es de tipo exploratoria dado que la adopción de criptomonedas en Bolivia es un fenómeno emergente y poco estudiado, se explorarán sus implicaciones en materia de seguridad digital. También de tipo explicativa porque se analizarán las relaciones entre el nivel de conocimiento en ciberseguridad de los usuarios y su exposición a riesgos.

Población y Muestra

- **Población:** Usuarios de criptomonedas en Bolivia, incluyendo inversionistas, comerciantes, desarrolladores, expertos en ciberseguridad y entidades financieras.

- **Muestra:** Se seleccionará una muestra representativa mediante muestreo intencional o por criterios direccionado, considerando personas que han utilizado criptomonedas en Bolivia en los últimos dos años y profesionales en el área de ciberseguridad.

- **Tamaño de la muestra:** Se definirá en función de profesionales del área de ciberseguridad. Se estima una muestra mínima de 200 encuestados para garantizar validez en el estudio cuantitativo.

Técnicas de investigación e Instrumentos de Recolección de Datos

- **Análisis Documental:** Se revisarán normativas nacionales e internacionales, reportes de ciberseguridad y publicaciones académicas sobre criptomonedas y seguridad digital.

- **Encuestas:** Se aplicarán cuestionarios estructurados con preguntas cerradas y escalas de medición para evaluar el nivel de conocimiento en ciberseguridad, percepción de riesgos y medidas de protección adoptadas.

- **Entrevistas Semi-estructuradas:** Se realizarán entrevistas a expertos en ciberseguridad, reguladores financieros y profesionales del sector, blockchain y criptomonedas, esto para comprender a

profundidad los desafíos y oportunidades en el tema de investigación.

- **Estudio de Casos:** Se analizarán incidentes de ciberseguridad relacionados con criptomonedas en Bolivia, y a nivel internacional, incluyendo fraudes, hackeos y esquemas piramidales.

Análisis de la situación actual de Bolivia

La ciberseguridad en el uso de criptomonedas en Bolivia se encuentra en una etapa de desarrollo, influenciada por cambios regulatorios recientes y la creciente adopción de estos activos digitales. A continuación, se presenta un análisis de la situación actual:

Evolución Regulatoria: Históricamente, Bolivia ha mantenido una postura restrictiva hacia las criptomonedas. En 2014, el Banco Central de Bolivia (BCB) prohibió el uso de monedas virtuales como el Bitcoin, argumentando que no constituían monedas de curso legal y buscando proteger a la población de posibles fraudes y riesgos financieros. Ratificando este comunicado el 15 de diciembre del 2020.

El Banco Central de Bolivia (BCB) comunica a la opinión pública que, en el marco de la Constitución Política del Estado, la Ley 1670 y a objeto de evitar riesgos y fraudes a la población en general, resolvió a través de Resolución de Directorio N° 144/2020 de 15 de diciembre de 2020, prohibir el uso de criptoactivos (monedas digitales o virtuales), al no constituirse en monedas de curso legal [15].

Históricamente, el Banco Central de Bolivia (BCB) mantuvo una postura restrictiva hacia las criptomonedas, prohibiendo su uso en 2014 mediante la Resolución de Directorio N° 045/2014. Esta postura fue ratificada en 2020 con la Resolución de Directorio N° 144/2020, que prohibía el uso de criptoactivos al no ser considerados monedas de curso legal. No obstante, el 4 de julio de 2024, el BCB emitió la Resolución de Directorio N° 082/2024 y el Comunicado de Prensa CP 35/2024, levantando parcialmente la prohibición y permitiendo a las entidades financieras realizar transacciones con criptoactivos como instrumentos electrónicos de pago para el comercio exterior, en respuesta a la escasez de dólares en el país. Este giro normativo subraya la necesidad de analizar los riesgos de ciberseguridad inherentes a este nuevo marco operativo [17].

Ante la creciente importancia de la Seguridad Informática en países desarrollados, se tienen definidas políticas que establecen la creación de organismos oficiales relacionados a la Seguridad de la Información, tales como INCIBE Instituto Nacional de Ciberseguridad de España, el EC3 Centro Europeo de Ciberdelincuencia de la Unión Europea, el NCAZ Centro Nacional de Defensa Cibernética de Alemania, el NSA Agencia de Seguridad Nacional de Estados Unidos; incluso en américa latina se han creado organismos como: CERTuy de Uruguay y arCERT de Argentina.

En el contexto nacional, además de la AGETIC (Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicaciones) y la ADSIB (Agencia para el Desarrollo de la Sociedad de la Información), solo tenemos una división de Informática Forense de la Policía en la Fuerza Especial de Lucha Contra el Crimen FELCC, que recibe denuncias de delitos informáticos en el país, de las cuales sólo un 70% sigue una investigación, en su mayoría los casos no son resueltos, por su complejidad o por falta de profesionales peritos informáticos tanto en la policía, como en los operadores de la justicia, para atender ese tipo de casos.

La legislación boliviana es muy pobre respecto a delitos informáticos, pues se tiene tipificado solo

dos delitos en el Código Penal (Manipulación informática y alteración, acceso y uso indebido de datos informáticos), los delitos informáticos están tipificados principalmente en el Código Penal boliviano, específicamente en el Capítulo XI titulado "Delitos Informáticos". Este capítulo fue incorporado por la Ley N° 1768 de 10 de marzo de 1997. Mas propiamente dicho en los artículos 363 bis y 363 ter del Código Penal. El artículo 363 bis sanciona la manipulación informática, que implica la alteración de datos o programas para causar un resultado incorrecto que derive en un beneficio económico ilícito, con penas de reclusión de 1 a 5 años y multa. El artículo 363 ter penaliza el acceso, uso, modificación o supresión no autorizada de datos informáticos, sancionado con prestación de trabajo de hasta un año o multa de hasta doscientos días, de igual forma, en la nueva Constitución Política del Estado se tiene una mención muy escueta respecto a la seguridad de la información.

Recientemente el Banco Central de Bolivia (BCB) y la Comisión Nacional de Activos Digitales (CNAD) de El Salvador firmaron este miércoles 30 de julio de 2025 un memorando de entendimiento. Este acuerdo tiene como finalidad establecer una cooperación permanente que facilite el intercambio de información y experiencias en el ámbito del desarrollo y regulación de activos digitales. Dentro del documento, ambas instituciones se comprometieron a colaborar en el intercambio de conocimientos técnicos y regulatorios. Los temas que se abordarán incluyen la trazabilidad de activos digitales, el uso de herramientas de inteligencia de cadenas de bloques y el análisis de riesgos financieros. Estos aspectos se desarrollarán en el marco de sus competencias normativas, con el objetivo de impulsar la innovación financiera en ambos países. Para el BCB, esta alianza representa un paso significativo hacia la modernización del sistema financiero en Bolivia y la profundización de la inclusión económica. En este sentido, la entidad destacó que el uso de activos virtuales en el país ha mostrado un crecimiento notable en el último año. Las cifras aumentaron de 46.5 millones de dólares en junio de 2024 a 294 millones de dólares en junio de 2025, tras la implementación de la Resolución de Directorio 082(BCB 2025).

En agosto 2025 la AGETIC a través del CGII, inicia la socialización del documento de nominado estrategia Nacional de Ciberseguridad (ENC) de Bolivia para el período 2025-2030(ENC, 2025). Este documento es desarrollado por el Estado Plurinacional de Bolivia para fortalecer las capacidades del país y así poder prevenir, detectar, responder y recuperarse de incidentes cibernéticos a nivel país.

Bajo el actual contexto tanto entidades, como el ciudadano común, que son víctimas de los delitos informáticos, optan por no concluir un proceso penal, ante la falta de profesionales, respaldo legal, costos elevados y principalmente el desprestigio público que puede sufrir la entidad o la persona, sin obtener un resultado favorable.

Si bien las entidades financieras privadas en Bolivia han avanzado en la modernización de su infraestructura tecnológica, adoptando estándares como el Payment Card Industry Data Security Standard (PCI DSS) para la seguridad de los datos de tarjetas de pago, es crucial diferenciar la naturaleza y el alcance de los marcos de referencia.

El marco MITRE ATT&CK, por ejemplo, es un recurso de inteligencia de amenazas, no una certificación. Su relevancia radica en la taxonomía de tácticas y técnicas de adversarios que permite el modelado de amenazas y la detección de ataques. Para la custodia de criptoactivos, los controles de seguridad deben alinearse con marcos como el Cybersecurity

Framework (CSF) del National Institute of Standards and Technology (NIST) 2.0, el cual proporciona directrices adaptables a empresas de cualquier tamaño. Por otro lado, tampoco contamos con profesionales especializados que coadyuven la obtención de una certificación y menos instituciones que brinden este tipo de capacitación requerido.

A nivel nacional Bolivia ya cuenta desde marzo 2025 con un cajero automático para las monedas virtuales en la ciudad de Santa Cruz, que fue instalado por la empresa BitBase, uno de los mayores operadores de este ámbito en Europa, para ampliar y facilitar las transacciones financieras, según publicaron los medios de la capital oriental. Se instalo en medio de la crisis por la escasez de dólares en el país.

Resultados

Impacto Económico y Social de Incidentes de Seguridad en Criptomonedas en Bolivia

Un incidente de seguridad masivo podría generar desconfianza en la población, afectando la reputación de la tecnología y reduciendo la adopción, lo cual limitaría las oportunidades de diversificación económica (Chainalysis, 2021). Además, la pérdida de activos por ataques cibernéticos impactaría negativamente en la estabilidad financiera de individuos y pequeñas empresas. Por ello, la prevención y la reacción inmediata a incidentes resultan fundamentales.

Nivel de Adopción y Uso de Criptomonedas en Bolivia

- Un **65%** de los encuestados afirmó haber utilizado criptomonedas en alguna ocasión, principalmente para inversión y comercio en línea.
- El **30%** de los usuarios emplea criptomonedas para transacciones internacionales debido a la escasez de dólares en Bolivia.
- El **80%** de los usuarios encuestados manifestó preocupación por la seguridad de sus fondos debido a la falta de regulación clara en el país.

Conocimiento y Prácticas de Ciberseguridad

- **Solo el 40% de los encuestados** afirmó conocer en detalle las mejores prácticas de ciberseguridad en criptomonedas, como el uso de billeteras virtuales y autenticación de dos factores.
- **El 35% de los usuarios** ha sido víctima de algún intento de estafa o ataque relacionado con criptomonedas, como phishing, esquemas Ponzi o robos de credenciales.
- **El 60% de los encuestados** almacena sus criptomonedas en exchanges centralizados, aumentando su exposición a hackeos.

Riesgos de Ciberseguridad Asociados a las Criptomonedas amenazas y vulnerabilidades

La adopción de criptomonedas conlleva varios riesgos de ciberseguridad, entre los que destacan:

- **Fraudes y Estafas:** La falta de regulación y supervisión ha facilitado la proliferación de esquemas fraudulentos relacionados con criptomonedas, afectando la confianza de los usuarios, Se han identificado múltiples casos de esquemas piramidales y falsas inversiones con criptomonedas en Bolivia.
- **Criptojacking:** Consiste en el uso no autorizado de dispositivos para minar criptomonedas, afectando el rendimiento y la seguridad de los sistemas comprometidos, Se detectó que algunos ciberdelincuentes en el

país están utilizando malware para tal efecto de minería de criptoactivos.

- **Pérdida de Claves Privadas:** Dado que las transacciones son irreversibles, la pérdida o robo de claves privadas puede resultar en la pérdida total de los activos digitales.

Desafíos y Oportunidades Futuras en la Ciberseguridad de Criptomonedas en Bolivia

A mediano plazo, uno de los desafíos clave es la actualización del marco regulatorio para acompañar la evolución tecnológica. A largo plazo, se vislumbran oportunidades como la generación de empleos en el sector de la seguridad informática, el desarrollo de infraestructura tecnológica nacional, y la creación de servicios financieros digitales más inclusivos y seguros. La mejora continua de la ciberseguridad no sólo fortalecerá el uso responsable de criptomonedas, sino que también posicionará a Bolivia como un actor regional competente en el ámbito de las finanzas digitales.

La presente investigación analiza la situación actual de la ciberseguridad en el ecosistema de criptomonedas en Bolivia, revelando un entorno que se encuentra en un punto crítico de transición.

La adopción de estos activos digitales está en una etapa de crecimiento acelerado, impulsada en gran medida por la escasez de dólares estadounidenses que presiona a la población a buscar alternativas para el comercio internacional y la preservación de valor. Sin embargo, esta rápida expansión ocurre en un contexto de vulnerabilidad extrema, donde la preparación institucional y la conciencia del usuario son peligrosamente incipientes. Los datos recopilados indican que un 65% de los encuestados ha utilizado criptomonedas, pero solo un 40% afirma conocer las mejores prácticas de seguridad, lo que crea una profunda "brecha de seguridad" que los ciberdelincuentes explotan.

Los hallazgos principales señalan que las amenazas más prevalentes no son ataques sofisticados a la tecnología de blockchain, sino los fraudes basados en ingeniería social, las estafas piramidales y el phishing, que se aprovechan de la falta de educación y la ambición de los usuarios. Paralelamente, la infraestructura legal y forense del Estado boliviano es frágil y obsoleta, lo que crea un "espacio de impunidad" que disuade a las víctimas de denunciar y, a su vez, fomenta el crecimiento del cibercrimen. La reciente flexibilización regulatoria del Banco Central de Bolivia (BCB) y su acuerdo con El Salvador, aunque son un paso pragmático hacia el futuro, intensifican la urgencia de establecer un marco de protección robusto para los ciudadanos.

En conclusión, la ciberseguridad en el ámbito de los criptoactivos en Bolivia no es un problema técnico aislado, sino un componente crítico que define la estabilidad financiera y la soberanía digital del país. La falta de una acción coordinada entre el sector público, el sector privado y la sociedad civil expone a la población a riesgos inaceptables y limita el potencial transformador de esta tecnología. Por ello, se recomienda una estrategia integral y holística que combine la creación de un marco legal específico, el fortalecimiento de las capacidades institucionales, la obligatoriedad de estándares de seguridad internacionales como el NIST CSF 2.0 o la familia ISO-2700, y un programa masivo de educación digital a nivel nacional.

Discusión

Los resultados obtenidos en esta investigación revelan una paradoja en el uso de criptomonedas en Bolivia: su adopción está en crecimiento, pero las prácticas de ciberseguridad y el marco regulatorio aún presentan deficiencias

significativas. Esta situación genera una brecha de seguridad que expone a los usuarios a múltiples amenazas, desde fraudes hasta ataques cibernéticos más sofisticados como el criptojacking y el phishing.

Comparación con Estudios Previos: Los hallazgos de este estudio son consistentes con investigaciones internacionales que indican que **la falta de regulación y educación en ciberseguridad son los principales factores que incrementan la vulnerabilidad de los usuarios de criptomonedas** (Conti et al., 2018; Ali et al., 2020). Estudios previos han señalado que en países donde las criptomonedas aún no tienen un marco regulador sólido, los incidentes de fraude y hackeos son más frecuentes, como se ha evidenciado en mercados emergentes (Auer & Claessens, 2021).

En el caso de Bolivia, la ausencia de plataformas locales reguladas obliga a los usuarios a recurrir a **exchanges internacionales**, lo que puede dificultar la protección de sus activos digitales en caso de incidentes de seguridad. Además, **el 60% de los encuestados almacena sus criptomonedas en plataformas centralizadas**, lo que contradice las mejores prácticas de seguridad que recomiendan el uso de billeteras frías para mayor protección.

El panorama de las criptomonedas en Bolivia se caracteriza por una adopción notablemente alta, que desafía la política de prohibición histórica y parcialmente levantada del Banco Central de Bolivia (BCB). El estudio demuestra que un 65% de la población encuestada ha utilizado criptomonedas en alguna ocasión, principalmente con fines de inversión y comercio en línea. Esta tendencia es confirmada por reportes de consultoras como Blockfinity Advisors, que indican que el 42% de los encuestados ya posee criptomonedas, y casi la totalidad de ellos (un 98%) ha manifestado interés en usarlas o en aprender sobre ellas (Siscotec, 2024).

El factor principal que impulsa esta adopción es la necesidad económica. Un 30% de los usuarios recurre a las criptomonedas para realizar transacciones internacionales, lo que representa una respuesta directa y pragmática a la escasez de dólares que ha afectado al país. Este comportamiento evidencia que la adopción de criptoactivos no es meramente una moda especulativa, sino que, para una parte significativa de la población, se ha convertido en una solución funcional y necesaria para sortear las limitaciones del sistema financiero tradicional.

Sin embargo, esta rápida incursión en el mundo digital no ha sido acompañada por una adecuada formación en ciberseguridad. Solo el 40% de los usuarios afirma conocer en detalle las mejores prácticas de seguridad, lo que contrasta fuertemente con el alto nivel de uso.

Esta disparidad entre el interés y el conocimiento crea un entorno de alta vulnerabilidad. La comodidad de las plataformas centralizadas, por ejemplo, ha llevado a que el 60% de los encuestados almacene sus activos en ellas, lo que los expone a un mayor riesgo de hackeos, en contra de las recomendaciones de seguridad que favorecen el uso de billeteras virtuales para la protección de fondos. La falta de conciencia sobre los riesgos y la urgencia de encontrar soluciones financieras rápidas crean una fuente de cultivo perfecto para que los ciberdelincuentes exploten la confianza de los usuarios, lo que explica por qué más de un tercio ha sido víctima de algún tipo de ataque.

Los riesgos de ciberseguridad en Bolivia se manifiestan en múltiples formas, desde esquemas fraudulentos a nivel personal hasta amenazas técnicas más complejas. La cara más visible de esta problemática son los fraudes basados en la

manipulación psicológica o ingeniería social. El caso de Oruro es un ejemplo elocuente, donde tres individuos fueron estafados por 99.500 bolivianos a través de redes sociales (Siscotec, 2024). La estrategia utilizada fue la de un esquema Ponzi: se prometieron ganancias desproporcionadas y se pagaron pequeños rendimientos iniciales para generar una falsa sensación de confianza, lo que llevó a las víctimas a invertir sumas mayores antes de que la estafa se revelara [23, 24].

A nivel técnico, el ecosistema no está exento de riesgos. El estudio identifica amenazas como las falsas billeteras virtuales, donde los delincuentes utilizan malware como Crocodilus para engañar a los usuarios y robarles sus frases semilla, que son la clave para acceder a sus fondos [23]. El cryptojacking también ha sido detectado en el país, un tipo de ataque en el que los ciberdelincuentes secuestran las computadoras y aprovechan estos dispositivos de las víctimas para minar criptomonedas sin su consentimiento, lo que degrada el rendimiento del sistema. Por último, el phishing y la reutilización de contraseñas son vulnerabilidades comunes que los atacantes explotan para acceder a cuentas y robar credenciales [23].

La recurrencia de estos casos ilustra que el problema principal no reside en un fallo de la tecnología subyacente, sino en la "capa humana" del ecosistema. La falta de educación, la cultura informática y la búsqueda de oportunidades de inversión rápidas y fáciles hacen que la población sea el eslabón más débil. A continuación, la Tabla 1 detalla estos riesgos con ejemplos concretos, lo que permite dimensionar la magnitud del problema de manera más tangible.

Tabla 1. *Riesgos de Ciberseguridad y Ejemplos de Casos Reales en Bolivia*

Conjunto de Datos	Modalidad	Emociones
Esquemas Piramidales (Ponzi)	Fraudes que prometen rendimientos extraordinarios, pagando las ganancias de los primeros inversores con el capital de los nuevos.	Estafa de 99.500 bolivianos en Oruro a través de redes sociales [23]. Uso de cadenas de WhatsApp para engañar a usuarios como el caso de "José" [24].
Malware y Falsas Billeteras	Uso de software malicioso para suplantar aplicaciones legítimas y robar información sensible, como las frases semilla de las billeteras.	Detección del malware Crocodilus diseñado para robar frases semilla de billeteras cripto móviles [23].
Criptojacking	Secuestro de dispositivos para utilizarlos de manera no autorizada en la minería de criptomonedas, sin que el dueño lo sepa.	Delincuentes en el país han sido detectados utilizando malware para este fin, afectando el rendimiento y la seguridad de los sistemas comprometidos [23].
Phishing y Robo de Credenciales	Suplantación de identidad a través de correos electrónicos o mensajes falsos para engañar a los usuarios y que revelen sus datos personales.	Ataques comunes que se aprovechan de la reutilización de contraseñas y la falta de autenticación de dos factores por parte de los usuarios [23].

Conclusiones

El análisis de la ciberseguridad en el uso de criptomonedas en Bolivia revela un ecosistema que se encuentra en un punto crítico de encrucijada total. La adopción es una realidad irreversible, impulsada por fuerzas económicas y tecnológicas que han superado con creces la eficacia de una prohibición total. El principal hallazgo es que la "brecha de seguridad" que expone a los usuarios a riesgos significativos no es un problema monolítico, sino un fenómeno multifactorial. Incluye la falta de educación del usuario, no se tiene esa cultura informática, y la fragilidad del marco legal y forense del Estado, además de la incipiente preparación de las instituciones financieras. La falta de acción integral del Estado boliviano no solo deja a los ciudadanos vulnerables a fraudes y ataques, sino que también limita las oportunidades de diversificación económica y de integración en la economía digital global, comprometiendo así su soberanía digital.

La ciberseguridad, en este contexto, debe ser vista más allá de ser un simple costo o una barrera para la innovación. En realidad, se presenta como un habilitador fundamental para generar confianza, fomentar el crecimiento y garantizar la resiliencia del sistema financiero. Un ecosistema de criptoactivos que opere de manera segura en Bolivia, respaldado por una regulación inteligente y una población educada, tiene el potencial de generar nuevos empleos, atraer inversión extranjera y posicionar al país como un actor regional competente en el ámbito de las finanzas digitales, tal como se sugiere en los estudios de base. Abordar los riesgos de ciberseguridad es, por lo tanto, un requisito indispensable para poder aprovechar las oportunidades que esta tecnología emergente ofrece.

Por los tanto se concluye que existe la necesidad de un modelo de ciberseguridad. El presente estudio ha permitido realizar la evaluación del estado de la ciberseguridad en el uso de criptomonedas en Bolivia, el mismo que revela un entorno legal restrictivo, una infraestructura incipiente y una necesidad urgente de formación y regulación. Sin embargo, la adopción de prácticas de seguridad robustas, la introducción de marcos regulatorios adaptativos y la promoción de la educación digital pueden sentar las bases para un ecosistema más confiable y resiliente. El futuro de las criptomonedas en Bolivia de manera segura dependerá en gran medida de la capacidad de sus actores para enfrentar los riesgos cibernéticos y aprovechar las oportunidades que la tecnología ofrece.

Medidas de Protección y Recomendaciones

Para mitigar los riesgos mencionados, se recomienda:

Educación y Concienciación: Es esencial que los usuarios comprendan el funcionamiento de las criptomonedas y las mejores prácticas de seguridad, como el uso de billeteras seguras y la protección de claves privadas.

Uso de Plataformas Confiables: Adquirir y comerciar criptomonedas a través de empresas legalmente constituidas y reguladas reduce el riesgo de fraudes. Hoy en día el banco que está vendiendo monedas virtuales es el banco BISA con la venta de USDT, que por el momento no está normado y la venta esta al precio del dólar en el mercado informal.

Campañas de educación digital y ciberseguridad dirigidas a inversionistas y usuarios ocasionales de criptomonedas.

Fomento del uso de billeteras seguras y autenticación de múltiples factores para reducir la vulnerabilidad a ataques cibernéticos.

Implementación de marcos normativos internacionales, tales como PCI DSS (Payment Card Industry Data Security Standard), y MITRE ATT&CK que es uno de los principales marcos de referencia globales respecto a inteligencia de amenazas y operaciones de ciberseguridad[18] o porque no decirlo la NIST CSF 2.0, que es un marco de referencia que se adapta a todo tipo de empresa sin importarle su tamaño.

La Fundación Internet Bolivia resalta la necesidad urgente de colaboración entre el gobierno y otros actores para mejorar la posición del país en este ámbito. El reporte sugiere que casi la mitad de los países ya cuentan con equipos especializados en respuesta a incidentes cibernéticos y políticas nacionales robustas [19].

Estrategias de Ciberseguridad a Nivel de Política Pública

Creación de un Marco Regulatorio Específico: Se debe abandonar la política de prohibición para adoptar un enfoque de regulación inteligente. El Banco Central de Bolivia (BCB), en colaboración con la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC), debe liderar la creación de una ley específica para los activos digitales. Esta ley debe basarse en modelos de licenciamiento y registro de intermediarios, como en el caso de Argentina, donde se regula a los Proveedores de Servicios de Activos Virtuales (PSAVs). [25]. Dicho marco debe incluir la obligatoriedad de la ciberseguridad robusta, la segregación de activos y los controles de prevención de lavado de dinero.

Fortalecimiento del Aparato Estatal: La "Estrategia Nacional de Ciberseguridad 2025-2030" de la AGETIC debe ser priorizada y enfocada en el fortalecimiento de las capacidades institucionales [22]. Es crucial establecer unidades especializadas en informática forense dentro de la Policía (FELCC) y el Ministerio Público, con personal capacitado en la investigación de delitos relacionados con criptoactivos. El objetivo es reducir la impunidad, lo que alentaría a las víctimas a denunciar y actuaría como un factor disuasorio para los ciberdelincuentes.

Adopción de Estándares Globales: La AGETIC y las instituciones financieras deben adoptar de manera obligatoria y progresiva marcos de referencia internacionales. El NIST Cybersecurity Framework (CSF) 2.0 es el más idóneo, ya que su naturaleza no prescriptiva y su adaptabilidad a organizaciones de cualquier tamaño lo convierten en una herramienta flexible y eficaz para el contexto boliviano [11, 12].

Medidas de Protección para el Sector Privado y Financiero

Obligatoriedad en la implementación del PISI: El Plan Institucional de Seguridad de la Información (PISI), promovido por la AGETIC el 2017, debe ser de aplicación obligatoria para todas las entidades financieras, empresas que gestionen criptoactivos y todas las instituciones en el contexto boliviano. También es fundamental que estas entidades integren medidas avanzadas, como el uso de Módulos de Seguridad de Hardware (HSM) para la gestión de claves privadas, la segregación de fondos en billeteras frías y calientes, y el monitoreo de transacciones en la blockchain.

Colaboración con la Comunidad Académica: El sector privado debe colaborar activamente con las universidades y otras instituciones académicas para fomentar la capacitación y la certificación de profesionales especializados en ciberseguridad de criptoactivos, siguiendo el ejemplo de la

certificación Crypto Compliance que se imparte en Argentina [26]. Esta medida es clave para cerrar la brecha de talento y garantizar que las empresas cuenten con el personal calificado necesario para gestionar estos riesgos.

Empoderamiento del Usuario: Educación Digital como Prioridad Nacional

Lanzamiento de Campañas Masivas: El Estado, a través de la AGETIC y la Fundación Internet Bolivia, debe lanzar campañas de concienciación masivas dirigidas a los usuarios de criptoactivos y a la población en general. Estas campañas deben usar un lenguaje accesible y narrativas "humanas" basadas en casos reales, como la estafa en Oruro [23], para explicar los riesgos de manera clara. Se debe promover de forma enfática el uso de la autenticación de dos factores, la protección de claves privadas y el uso de billeteras seguras.

Guías Prácticas y Educación Continua: Se debe crear y difundir guías prácticas de ciberseguridad para el usuario boliviano. Asimismo, se pueden aprovechar iniciativas regionales de la Organización de los Estados Americanos (OEA), como los Cyber Challenges, para involucrar a la comunidad y hacer del aprendizaje sobre ciberseguridad una actividad práctica, interactiva y accesible, lo que promueve una cultura de protección digital en el país [12].

Realizar un análisis más profundo de la Infraestructura de Ciberseguridad

- Las instituciones financieras en Bolivia aún no han integrado medidas de seguridad específicas para transacciones con criptomonedas.
- No existen plataformas de intercambio locales reguladas, lo que obliga a los usuarios a recurrir a exchanges internacionales, aumentando los riesgos de seguridad.
- Solo el 25% de los expertos entrevistados considera que Bolivia está preparada para regular y asegurar las transacciones con criptomonedas.

El fortalecimiento de la ciberseguridad en el uso de criptoactivos en el país requiere la implementación de un Plan Estratégico de Ciberseguridad (PISI, Plan Institucional de Seguridad de la Información).

Este plan debe considerar la adopción de controles y marcos de referencia internacionales, como el NIST Cybersecurity Framework (CSF) 2.0, que se adapta a todo tipo de organizaciones. Además, se recomienda la integración de medidas específicas para la protección de criptoactivos, como el uso de Módulos de Seguridad de Hardware (HSM) y la computación multipartita (MPC) para la gestión de claves privadas, la segregación de activos digitales en billeteras frías y calientes, y el monitoreo on-chain. La aplicación de estos controles se puede alinear con los principios de Secure-by-Design y la adopción de tecnologías Post-Quantum Cryptography (PQC) promovidas por la Cybersecurity and Infrastructure Security Agency (CISA), fortaleciendo así la resiliencia del ecosistema digital.

Agradecimientos

Agradezco profundamente a Dios y a todas las personas e instituciones que hicieron posible la elaboración de este artículo científico. En especial, a los expertos en ciberseguridad y tecnología financiera que compartieron sus conocimientos y experiencias, así como a las plataformas académicas y bibliográficas que brindaron acceso a valiosa información. Extiendo también mi gratitud a mi familia y colegas por su

constante apoyo y motivación durante el desarrollo de esta investigación, y a la comunidad académica boliviana por fomentar el análisis crítico y el avance del conocimiento en temas emergentes como la seguridad digital y el uso de criptomonedas.

Referencias Bibliográfica

Alpár, G. (2017). Foundations of cryptography. En D. Lee, K. Chuen & R. Deng (Eds.), Handbook of Blockchain, Digital Finance, and Inclusion (pp. 179–205). Academic Press.

Autoridad de Supervisión del Sistema Financiero. (2020). Regulaciones sobre medios de pago electrónicos en Bolivia.

Banco Central de Bolivia. (2014). Comunicado sobre el uso del Bitcoin y otras monedas no reguladas. BCB.

Riveros Dullmann, F. A. (2024). *Regulación jurídica del bitcoin y criptomonedas en Bolivia y análisis técnicos de mercados financieros*. Universidad Mayor de San Andrés.

López Mamani, E. E., & Calle Quisbert, R. (2023). Causas por las que el Bitcoin no se aplica en Bolivia. *Ciencia Latina Revista Científica Multidisciplinar*, 7(2), 11151-11160.

Cadena SER. (2025, marzo 15). *La Policía Nacional desmantela una macroestafa piramidal con criptomonedas: hay ocho detenidos y 3.600 víctimas*.

Bohr, J., & Bashir, M. (2014, June). Who uses bitcoin? An exploration of the bitcoin community. Proceedings of the Twelfth Workshop on the Economics of Information Security (WEIS). https://weis2014.econinfosec.org

Chainalysis. (2021). The 2021 Global Crypto Adoption Index. Chainalysis Research. https://blog.chainalysis.com

European Union Agency for Cybersecurity (ENISA). (2022). Cybersecurity in the financial sector: Regulatory landscape and threat evaluation. ENISA. https://www.enisa.europa.eu

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and *Cryptocurrency Technologies: A Comprehensive Introduction.* Princeton University Press.

National Institute of Standards and Technology (NIST). (2020). Blockchain and Distributed Ledger Technologies (DLT). https://www.nist.gov/blockchain

Organización de los Estados Americanos (OEA). (2016). Estándares de ciberseguridad en América Latina y el Caribe. OEA. http://www.oas.org

Vigna, P., & Casey, M. J. (2015). The age of cryptocurrency: How bitcoin and digital money are challenging the global economic order. St. Martin's Press.

World Economic Forum (WEF). (2020). Global blockchain governance report 2020. WEF. https://www.weforum.org

Banco Central de Bolivia. (2020). *Comunicado sobre el uso del Bitcoin y otras monedas no reguladas*. BCB. Prohibición del usos de critoactivs

https://www.france24.com/es/programas/econom%C3%ADa/20240704-bolivia-levant%C3%B3-prohibici%C3%B3n-de-uso-de-criptomonedas-para-hacerle-frente-a-la-escasez-de-d%C3%B3lares

Entel_Digital_Reporte_Ciberseguridad_2025_.pdf (pag 65).

Retos y Soluciones en Ciberseguridad para Empresas en Bolivia. https://www.lbc.bo/blog/retos-y-soluciones-en-ciberseguridad-para-empresas-en-bolivia/

Ali, S., Jianing, W., & Hussain, T. (2020). **Cybersecurity Challenges in Cryptocurrency Transactions: A Global Perspective**. *Journal of Financial Crime, 27*(4), 1052-1073. https://doi.org/10.1108/JFC-07-2020-0123

Auer, R., & Claessens, S. (2021). **Cryptocurrency Regulation: Global Trends and Challenges**. *Bank for International Settlements (BIS) Working Papers*. https://www.bis.org/publ/work951.htm

BCB 2025, Bolivia firma acuerdo con El Salvador para desarrollo de activos digitales, acuerdo BCB–CNAD para proyección regulatoria.

https://www.bcb.gob.bo/webdocs/10_notas_prensa/CP-30%20BCB%20-%20Acuerdo%20BCB%20CNAD%20OK.pdf

BCB 2025, ESTRATEGIA NACIONAL DE CIBERSEGURIDAD del estado plurinacional de Bolivia, 2025 - 2030.

SISCOTEC, 2023, Ciberseguridad en el mundo Cripto: ¿Cómo proteger tus criptomonedas. https://siscotec.com/blog/xperti-1/ciberseguridad-en-el-mundo-cripto-como-proteger-tus-criptomonedas-23

Labtecnosocial 2024, criptomonedas-y-estafas https://labtecnosocial.org/criptomonedas-y-estafas/

Argentina regula los operadores y libera las criptomonedas. Marzo, 2025 https://observatorioblockchain.com/criptomonedas/argentina-regula-los-operadores-y-libera-las-criptomonedas/

Certificación en Crypto Compliance https://www.umsa.edu.ar/oferta/certificacion-en-crypto-compliance/