Ciencia & tecnología DIGITAL

Volumen 1
Número 1 (2025)

ISSN
Impreso: 0000-0000
Virtual: 0000-0000

FCyT

sis | INGENIERÍA DE SISTEMAS

tel | INGENIERÍA EN TELECOMUNICACIONES

dad | INGENIERÍA EN DISEÑO Y ANIMACIÓN DIGITAL

cic | INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN

tic | INGENIERÍA EN TECNOLOGÍA DE LA INFORMACIÓN Y SEGURIDAD

Ciencia & tecnología DIGITAL

Publicada por

Facultad de Ciencias y Tecnología - USFX

Periodicidad

Semestral

Volumen y Número

Volumen 1, Número 1

Fecha de publicación

Octubre 2025

ISSN (Impreso)

0000 - 0000

ISSN (Virtual)

0000 - 0000

Sede editorial

Facultad de Ciencias y Tecnología
Calle Regimiento Campos 180
Sucre, Bolivia

Comité Editorial

Comité Arbitral

La Revista Ciencia y Tecnología Digital es una publicación académica multidisciplinaria de acceso abierto, orientada a la difusión de artículos originales y de revisión en los campos de la ingeniería y las ciencias computacionales. Su propósito es convertirse en un espacio de referencia para la articulación del conocimiento teórico y práctico, promoviendo la innovación y la generación de soluciones a los desafíos contemporáneos mediante el uso intensivo de las tecnologías digitales.

La Revista Ciencia y Tecnología Digital es una iniciativa académica impulsada por la Dirección de las carreras de Ingeniería de Sistemas, Ingeniería en Ciencias de la Computación, Tecnologías de Información y Seguridad, Diseño y Animación Digital, e Ingeniería en Telecomunicaciones, comprometida con el fortalecimiento de la investigación científica y la innovación tecnológica en el ámbito académico y profesional.

Contenidos

EVALUACIÓN DE LA EXPERIENCIA DE USUARIO ANTE INTERFACES WEB DE SOFTWARE DE GESTIÓN A TRAVÉS DEL ANÁLISIS DE EMOCIONES: ESTADO DEL ARTE DE MÉTODOS BASADOS EN INTELIGENCIA ARTIFICIAL

EVALUATING USER EXPERIENCE IN WEB INTERFACES FOR MANAGEMENT SOFTWARE USING EMOTION ANALYSIS: STATE OF THE ART OF ARTIFICIAL INTELLIGENCE-BASED METHODS

Gustavo Poquechoque Foronda
Universidad San Francisco Xavier
poquechoque.gustavo@usfx.bo

Carlos Walter Pacheco Lora
Universidad San Francisco Xavier
pacheco.carlos@usfx.bo

Recibido: 29 Abril 2025 / Revisado: 3 Agosto 2025 / Aceptado: 11 Agosto 2025 / Publicado: 23 Septiembre 2025

Resumen

Debido a la importancia de la experiencia de usuario (UX) como factor crítico en el éxito de productos y servicios digitales, que acentúa la necesidad de incorporar dimensiones emocionales en su evaluación, considerando que hasta ahora la medición de emociones en UX se ha basado en métodos como entrevistas y cuestionarios, que presentan limitaciones en términos de subjetividad y en la captura de emociones subconscientes. En este contexto, la inteligencia artificial (IA) se perfila como una herramienta prometedora para realizar evaluaciones más objetivas mediante el reconocimiento automático de emociones.

Se ha presentado una revisión sistemática de la literatura de los últimos siete años, en la que se exploran métodos basados en IA, donde se destacan desde algoritmos clásicos de machine learning hasta modelos avanzados de aprendizaje profundo. Además, se discute la relevancia de enfoques híbridos que integran múltiples fuentes de datos para obtener una evaluación integral del estado emocional del usuario, se examina los principales conjuntos de datos utilizados en la detección de emociones, paralelamente se identifican y discuten los desafíos éticos y técnicos actuales.

Conclusivamente el estudio evidencia que la aplicación de la IA en la evaluación de UX no solo amplía el horizonte metodológico al incorporar análisis emocionales de manera automatizada, sino que también proporciona una visión holística y detallada de la experiencia del usuario, lo que es fundamental para desarrollar interfaces más intuitivas, personalizadas y satisfactorias, que auguran un futuro donde la evaluación emocional en UX sea más precisa y adaptativa, abriendo nuevas oportunidades de innovación en el campo.

Palabras claves: Inteligencia Artificial, Evaluación de la Experiencia de Usuario, Análisis de Emociones, Aprendizaje Profundo.

Abstract

Given the importance of user experience (UX) as a critical factor in the success of digital products and services, which underscores the need to incorporate emotional dimensions into its evaluation, and considering that until now, the measurement of emotions in UX has relied on methods such as interviews and questionnaires, which present limitations in terms of subjectivity and in capturing subconscious emotions, artificial intelligence (AI) emerges as a promising tool for conducting more objective assessments through automatic emotion recognition.

This paper presents a systematic review of the literature from the last seven years, exploring AI-based methods, ranging from classic machine learning algorithms to advanced deep learning models. Furthermore, it discusses the relevance of hybrid approaches that integrate multiple data sources to obtain a comprehensive assessment of the user's emotional state, examines the main datasets used in emotion detection, and identifies and discusses current ethical and technical challenges.

In conclusion, the study demonstrates that the application of AI in UX evaluation not only expands the methodological horizon by incorporating automated emotional analysis, but also provides a holistic and detailed view of the user experience, which is essential for developing more intuitive, personalized, and satisfying interfaces. This suggests a future where emotional evaluation in UX is more precise and adaptive, opening new opportunities for innovation in the field.

Keywords: Artificial Intelligence, User Experience Evaluation, Emotion Analysis, Deep Learning.

Introducción

La experiencia de usuario (UX) se ha convertido en un diferenciador clave para el éxito de productos y servicios digitales, abarcando aspectos que van más allá de la funcionalidad y usabilidad, tradicionalmente la evaluación de las emociones en UX se ha basado en métodos cualitativos, como entrevistas y cuestionarios, aunque útiles, estos enfoques presentan limitaciones relacionadas con la subjetividad y la capacidad del usuario para expresar con precisión sus sentimientos, además que pueden no capturar emociones subconscientes que afectan el comportamiento del usuario (Hernandez Perez, 2022). En años recientes la inteligencia artificial (IA) ha emergido como una herramienta prometedora para evaluar y mejorar la UX de forma más objetiva y continua (Galindo Monfil et al., 2025), en particular la integración de IA para el reconocimiento automático de emociones permite a las máquinas comprender y responder a las emociones humanas, lo que puede mejorar significativamente la interacción y satisfacción del usuario en diversos contextos (Liu, 2024).

La computación afectiva como disciplina que combina la informática y la psicología, ha desarrollado múltiples métodos de análisis emocional asistidos por IA para inferir el estado emocional del usuario, como el reconocimiento facial, el análisis de voz, el procesamiento de lenguaje natural (PLN) aplicado a textos y la sensorización fisiológica, que consiste en medir indicadores corporales como la frecuencia cardíaca, la conductancia de la piel o la actividad cerebral (EEG) para detectar cambios afectivos involuntarios (Liu, 2024), junto al apoyo de técnicas de machine learning y deep learning ha permitido alcanzar una alta precisión en entornos controlados al reconocer estados emocionales del usuario (Khare et al., 2024a) (Liu, 2024), buscando evaluaciones UX más sensibles y continuas, que puedan lograr métricas operativas

de satisfacción en ámbitos como salud, entretenimiento, educación, entre otros (Razzaq et al., 2023) (Pereira et al., 2024).

La aplicación de IA para la evaluación emocional en UX enfrenta desafíos importantes, uno de ellos son los sesgos algorítmicos, debido a que los modelos de reconocimiento emocional pueden reflejar prejuicios presentes en sus datos de entrenamiento, mostrando diferentes niveles de precisión según la demografía del usuario (como, variaciones por género, edad o cultura) (Verhoef & Fosch-Villaronga, 2023); evidenciando sesgos de género y raza, entre otros, lo cual plantea preocupaciones de equidad en su uso (Plisiecki et al., 2025), el manejo de datos emocionales sensibles también se vincula a aspectos relativos a la privacidad, la recopilación y análisis de expresiones faciales, voces o señales fisiológicas de los usuarios deben realizarse respetando marcos éticos y legales, asegurando que no se vulnere la confidencialidad ni la autonomía del individuo (Liu, 2024).

La literatura reciente presenta una fragmentación disciplinaria; el mapeo sistemático en español de Galindo Monfil et al. muestra un aumento sostenido de estudios sobre emociones y satisfacción del usuario, pero también evidencia que ambas variables se evalúan, en la mayoría de los casos, de forma independiente y con instrumentos heterogéneos (Galindo Monfil et al., 2025). Por su parte, revisiones internacionales centradas en visión por computador destacan la proliferación de propuestas basadas en deep learning, pero subrayan la escasez de análisis comparativos que integren modalidades múltiples y métricas de UX (Pereira et al., 2024). Esta dispersión dificulta a investigadores y profesionales identificar tendencias sólidas, líneas de investigación y prácticas consolidadas, lo que refuerza la necesidad de una revisión de los métodos y sus contextos de aplicación.

Se plantea relevar y ofrecer una visión sintética y crítica de los avances sobre el uso de IA para evaluar la UX a partir del análisis de emociones como alternativa a los cuestionarios tradicionales para la identificación de emociones a partir de distintos recursos, caracterizando los métodos de análisis emocional especificando sus enfoques algorítmicos y métricas, comparando su precisión y aplicabilidad, nivel de efectividad y confianza de resultados logrados en los diferentes trabajos y ámbitos de aplicación, para su posible aplicación en procesos de UX, identificando vacíos y desafíos en relación a con sus sesgos, privacidad de datos, interpretabilidad y estandarización de procedimientos; que pueda servir como una guía para investigadores y profesionales en proyectos de UX impulsados por IA.

Metodología

El artículo adopta una Revisión Sistemática de la Literatura (RSL) como enfoque, adecuado para sintetizar con rigor la evidencia, definiendo los siguientes pasos:

- Identificación de fuentes y búsquedas, cadena principal("user experience evaluation" AND "emotion* analys*" AND AI) y variantes en: IEEE Xplore, ACM Digital Library, Scopus, arXiv. Filtros: 2017 2025, idioma inglés OR español, tipo article / conference paper.

- Definición de preguntas de investigación: Establecer preguntas claras que guían la revisión, como: ¿Qué técnicas de IA se han utilizado para analizar emociones en UX? ¿Cuáles son las ventajas y limitaciones de estos métodos?

- Criterios de inclusión y exclusión: Determinar los criterios para seleccionar estudios relevantes, considerando aspectos como el

período de publicación, idioma, tipo de estudio y pertinencia al tema central.

- Búsqueda de literatura: Realizar búsquedas exhaustivas en bases de datos académicos reconocidos (por ejemplo, IEEE Xplore, ACM Digital Library, Scopus) utilizando palabras clave relacionadas, como "experiencia de usuario", "análisis de emociones" e "inteligencia artificial".

- Selección de estudios: Aplicar los criterios de inclusión y exclusión para filtrar los estudios obtenidos, asegurando la relevancia y calidad de las fuentes seleccionadas.

- Extracción y análisis de datos: Recopilar información clave de los estudios seleccionados, como métodos de IA utilizados, métricas de evaluación, contextos de aplicación y hallazgos principales.

- Síntesis de resultados: Analizar y sintetizar los datos extraídos para identificar tendencias, brechas en la investigación y oportunidades para futuros estudios en el campo.

Se oriento el trabajo a partir del establecimiento de las siguientes preguntas: ¿Qué modelos y tecnologías de IA se han utilizado para identificar emociones humanas en diferentes ámbitos y circunstancias similares a las requeridas en los ámbitos de UX? ¿Cuáles son las exigencias o requerimientos técnicos y tecnológicos, las ventajas y limitaciones de estos modelos o tecnologías?

El criterio de inclusión y exclusión de los trabajos revisados consideró: el período de publicación, idioma, tipo de estudio y pertinencia con relación al propósito principal.

Se realizaron búsquedas exhaustivas en las bases de datos de las revistas científicas Arxiv, IEEE Xplore, ACM Digital Library, Scopus entre otros.

El proceso de extracción y análisis de datos, permitió recopilar información clave de los estudios seleccionados, en relación a modelos y tecnologías de IA, principalmente Deeplearning, métricas de evaluación, contextos de aplicación y hallazgos principales.

La síntesis de resultados, considero el análisis y síntesis de los datos extraidos, que permitió identificar las tendencias, las limitaciones y desafíos de los trabajos que establecen el estado del arte.

La revisión sistemática de la literatura facilito la identificación, evaluación y síntesis de investigaciones relevantes, proporcionando una visión integral del estado actual del conocimiento en un área específica:

- Identificar tendencias y avances, junto a la detección de las técnicas de IA más utilizadas en el análisis de emociones aplicadas a la UX.

- Evaluar la eficacia y limitaciones, analizando la efectividad de estos métodos y las posibles áreas de mejora.

- Detectar vacíos en la investigación, señalando áreas que requieren mayor atención o desarrollo futuro.

Resultados

Deep learning aplicado al análisis de emociones a partir de recursos multimodades

Los métodos de IA aplicados al análisis de emociones en UX abarcan desde algoritmos de aprendizaje automático tradicional hasta modelos avanzados de aprendizaje profundo, pero se ha

dado preferencia a técnicas basadas en redes neuronales debido a su alta capacidad (Khare et al., 2024b).

Los modelos de IA aplicados pueden ser clasificados en los siguientes grupos:

- **Clasificadores de machine learning clásicos**: Algoritmos como Support Vector Machines (SVM), k-NN, árboles de decisión, bosques aleatorios o regresión logística se utilizaron ampliamente para clasificar estados emocionales a partir de características extraídas de datos de usuario, por ejemplo, un SVM entrenado sobre rasgos faciales o fisiológicos puede distinguir entre "frustrado" vs "no frustrado". Estos métodos requieren definir manualmente las características relevantes (p.ej., frecuencia cardíaca promedio, número de clics, palabras positivas/negativas en un comentario).

- **Redes neuronales profundas**: Modelos como las redes neuronales convolucionales (CNN)**,** las redes recurrentes (RNN) y arquitecturas híbridas han ganado protagonismo (Khare et al., 2024b), las CNN son comunes para analizar imágenes y video (p. ej., expresiones faciales), mientras que las RNN o LSTM se usan en secuencias temporales como voz, texto o señales fisiológicas, por ejemplo, las CNN han sido exitosas para reconocer expresiones faciales básicas a partir de cámaras web, y las LSTM para capturar la evolución temporal de señales EEG o el tono de voz.

- **Modelos de IA modernos**: En años recientes se incorporaron técnicas de vanguardia como redes generativas adversarias (GAN) para síntesis de expresiones, modelos de atención y especialmente transformers en el ámbito de PLN. Los modelos transformer (e.g. BERT, GPT) han revolucionado el análisis de sentimientos en texto, permitiendo detectar emociones con mayor precisión al tener en cuenta el contexto semántico, por ejemplo, BERT y sus variantes pueden clasificar la emoción expresada en reseñas de usuarios o comentarios de redes sociales con resultados superiores al 90% de exactitud en conjuntos de prueba. Asimismo, en visión por computadora se exploran Transformers (Vision Transformers) para reconocimiento facial emocional, estos modelos profundos suelen superar a los algoritmos tradicionales cuando se dispone de grandes cantidades de datos de entrenamiento (Ghatoray & Li, 2025).

- **Enfoques híbridos y de fusión**: Dado que las emociones pueden manifestarse en múltiples canales, se emplean métodos que combinan información de diversas fuentes (análisis multimodal), por ejemplo, sistemas que integran simultáneamente análisis facial vía CNN, tono de voz vía modelos de audio, y análisis de texto de lo que el usuario dice (transcripción) vía modelos de PLN (Ghatoray & Li, 2025), la fusión puede hacerse a nivel de características (uniendo vectores de atributos de cada modalidad) o a nivel de decisión (combinando las salidas de clasificadores independientes), un enfoque de investigación reciente propone asignar pesos dinámicos a cada modalidad según su fiabilidad, usando funciones de mezcla generalizadas, para mejorar la discriminación entre emociones (Khare et al., 2024b).

Los métodos de IA más utilizados abarcan desde técnicas supervisadas clásicas (regresión, SVM, árboles) hasta modelos profundos especializados en modalidades particulares (visión, audio, texto, fisiología), la tendencia clara desde 2018 es el predominio de aprendizaje profundo multimodal, aprovechando arquitecturas neuronales avanzadas para lograr un reconocimiento más robusto de las emociones del usuario (Khare

et al., 2024b) (Ghatoray & Li, 2025). Estos métodos permiten automatizar la detección de estados afectivos relevantes durante pruebas de UX, como detectar frustración, confusión, sorpresa o satisfacción de forma objetiva, algo difícil de lograr solo con métodos tradicionales de encuestas.

Enfoques más efectivos para la medición de emociones en interacción humano-computadora

El estado del arte establece que los enfoques multimodales son los más efectivos para medir emociones en entornos de interacción humano-computadora (HCI), ninguna señal por sí sola capta toda la complejidad emocional; por ello, combinar múltiples fuentes (expresiones faciales, voz, lenguaje verbal, fisiología, comportamientos de interacción) tiende a mejorar la precisión y robustez del análisis (Ghatoray & Li, 2025) (Razzaq et al., 2023).

Los enfoques más empleados son:

Análisis multimodal integrado: Consiste en registrar varias modalidades del usuario en paralelo durante la interacción con el sistema, por ejemplo, usar la cámara para analizar microexpresiones faciales, el micrófono para el tono de voz y el contenido verbal (vía speech-to-text), y posiblemente sensores como eye-tracking o pulseras para ritmo cardíaco. La fusión de estas señales proporciona una "vista completa" de la experiencia emocional del usuario (Ghatoray & Li, 2025).

Estudios recientes demuestran que este enfoque es superior a analizar un solo canal. Razzaq et al., 2023 reportan que un modelo híbrido con fusión de audio, video y texto alcanzó un ~98% de precisión promedio al clasificar emociones básicas (alegría, tristeza, enojo, neutral), superando por margen considerable a modelos unimodales (Razzaq et al., 2023); esto muestra cómo la combinación de modalidades logra capturar matices emocionales que podrían pasar inadvertidos con un solo tipo de dato.

Medición de respuestas fisiológicas: Las señales fisiológicas (frecuencia cardíaca, actividad electrodermal, respiración, EEG cerebral, dilatación pupilar) son valiosas porque reflejan directamente la activación emocional del sistema nervioso y son difíciles de controlar conscientemente (Khare et al., 2024b), en interacción humano-computadora, el uso de dispositivos como bandas GSR (respuesta galvánica de la piel), wearables (smartwatches con PPG para ritmo cardiaco) o EEG portátiles puede aportar indicadores objetivos de estrés, excitación o carga cognitiva. De hecho, las señales fisiológicas se consideran fuente ampliamente utilizada para identificar emociones debido a que son involuntarias y menos susceptibles a disimulo, por ejemplo, un aumento en la conductancia de la piel y la frecuencia cardiaca durante una tarea puede indicar frustración o ansiedad del usuario, complementando la lectura de su expresión facial, que si bien requieren sensores adicionales, estos datos enriquecen la evaluación emocional, especialmente para emociones internas que no siempre se manifiestan externamente (Khare et al., 2024b).

Evaluación de expresiones faciales y voz: Las expresiones faciales han sido un enfoque clásico y efectivo para detectar emociones en HCI, gracias a avances en visión por computadora, mediante cámaras web comunes permiten capturar las microexpresiones faciales del usuario; algoritmos de reconocimiento facial (Por ejemplo redes neuronales entrenadas en conjuntos de datos como FER-2013 o AffectNet) infieren emociones discretas como alegría, sorpresa, enojo o disgusto con buena precisión en tiempo real (Ghatoray & Li, 2025). Este enfoque es muy útil

para emociones de valencia claramente positiva o negativa (sonrisa = satisfacción), de modo similar, la voz del usuario (tono, ritmo, volumen) se analiza mediante técnicas de procesamiento de audio para detectar estrés o estados afectivos (voz temblorosa, tono agudo en enojo, pausas largas en confusión). La ventaja de estas señales "físicas" (cara y voz) es que se pueden captar de forma no intrusiva durante la interacción y los usuarios suelen aceptarlas mejor que los sensores corporales, Por tanto; combinadas, la expresión facial y la entonación de voz ofrecen un indicador confiable de la reacción emocional momentánea del usuario ante la interfaz.

Instrumentos subjetivos complementarios: Aunque el presente trabajo está centrado en la IA, es importante mencionar que en evaluación UX a menudo se complementan las mediciones objetivas con autoinformes del usuario (escalas de emoción percibida, encuestas post-tarea como SAM, PANAS, etc.), ya que estudios recientes muestran que el método más utilizado históricamente para medir emociones en HCI ha sido el cuestionario auto-reportado (Galindo Monfil et al., 2025), por su sencillez, sin embargo, estos dependen de la memoria del usuario y pueden interrumpir la tarea; siendo que los enfoques de IA buscan mejorar la efectividad midiendo emociones en tiempo real sin interrumpir al usuario, en la práctica, una estrategia efectiva es la combinación de ambos enfoques, tanto los registros fisiológicos/observacionales durante la interacción, complementados con breves encuestas subjetivas, permite correlacionar las señales medidas con la experiencia auto-reportada para obtener una evaluación más completa de la UX.

En general, los enfoques más efectivos integran múltiples modalidades y métodos, aprovechando la fortaleza de cada uno, la literatura destaca que los sistemas multimodales superan consistentemente a los unimodales en tasa de acierto y capacidad para reconocer distintas categorías emocionales (Razzaq et al., 2023). Asimismo, combinar medidas objetivas (Expresiones observadas) con las percepciones declaradas por el usuario mejora la validez de la evaluación. Por último, la contextualización es crucial: un enfoque efectivo incorpora información del contexto de la interacción (Qué tarea realiza el usuario, qué estímulos presenta la interfaz) al interpretar las señales emocionales, esto ayuda a distinguir, por ejemplo, si un ceño fruncido indica frustración con el sistema o simplemente concentración. En síntesis, el enfoque multimodal contextual donde varias fuentes de datos se analizan conjuntamente en contexto se considera el paradigma más efectivo actualmente para medir emociones en HCI y UX.

Evolución reciente de la aplicación de ia en el análisis de emociones para ux (2018–2025)

En los últimos siete años ha ocurrido una evolución significativa en cómo se aplica la IA para evaluar emociones en la experiencia de usuario, hacia 2018, muchas investigaciones de UX seguían midiendo emociones principalmente mediante métodos tradicionales (encuestas de satisfacción emocional al final de la sesión, observación manual de gestos), las primeras aplicaciones de IA en este ámbito se centraban en aspectos aislados, por ejemplo, usar reconocimiento facial o análisis de sentimientos de comentarios por separado y a menudo en entornos controlados de laboratorio. Sin embargo, conforme las técnicas de aprendizaje profundo demostraron su eficacia en reconocimiento de emociones en general (imagen, voz, texto), su adopción dentro del campo de UX aumentó rápidamente .

2018-2020, en este periodo inicial se publicaron trabajos pioneros que integraban IA en evaluaciones de UX, comenzaron a explorarse asistentes de voz (ej. Alexa, Siri) evaluados por su capacidad de generar satisfacción emocional, usando cuestionarios de emoción percibida junto con análisis del tono de voz del usuario (Galindo Monfil et al., 2025)

También surgieron estudios sobre el uso de electroencefalografía (EEG) y aprendizaje automático para detectar estados emocionales (como carga cognitiva o interés) durante el uso de sistemas educativos o videojuegos (Fernández-Ordóñez et al., 2019), no obstante, muchas de estas primeras incursiones trataban emociones y satisfacción por separado y de forma experimental. Galindo et al. (2025) hallaron en un mapeo sistemático que hasta 2024 la mayoría de trabajos evaluaban las emociones del usuario y su satisfacción de manera independiente, y que pocas investigaciones integraban ambos aspectos en una evaluación unificada (Galindo Monfil et al., 2025)

2020-2022, estos años vieron un despegue en la cantidad de investigaciones que aplican IA para UX analytics, varias tendencias confluyeron para acelerar la evolución: La madurez de frameworks de deep learning de código abierto (TensorFlow, PyTorch) facilitó a equipos de UX incorporar modelos pre-entrenados de emoción (Con modelos de reconocimiento facial ya entrenados en AffectNet) en sus estudios (Ghatoray & Li, 2025). La pandemia de COVID-19 (2020-2021) impulsó la evaluación remota de UX, generando necesidad de métodos no intrusivos para captar la experiencia del usuario a distancia, esto derivó en trabajos que utilizan la cámara web y micrófono del usuario final para evaluar sus emociones mientras interactúa con un software desde casa, dado que la observación presencial no era posible. Y finalmente aparecieron datasets más grandes y variados de emociones que permitieron entrenar modelos más generalizables, por ejemplo, en PLN, Google liberó en 2021 GoEmotions (Un amplio conjunto de datos de textos con 27 categorías emocionales), lo cual potenció el desarrollo de análisis de sentimientos más sutiles en reseñas y comentarios de usuarios.

Durante este período, se empieza a apreciar una transición de enfoques unimodales a enfoques multimodales en UX, un estudio de 2021 integró eye-tracking y seguimiento de clics del ratón para inferir la carga emocional durante la navegación web, encontrando correlaciones entre ciertos patrones (movimientos oculares erráticos, clics repetitivos) y frustración del usuario (Ghatoray & Li, 2025). En general, 2020-22 marcó el paso de la teoría a la práctica, con más herramientas accesibles y varios estudios de caso demostrando que la IA podía añadir valor real al proceso de evaluación de experiencia de usuario.

2023-2025, en los años más recientes, la aplicación de IA en análisis emocional para UX ha alcanzado un nuevo nivel de sofisticación y adopción, y se observa un énfasis en la automatización completa del proceso de obtención de insights de UX: por ejemplo, Ghatoray & Li (2025) desarrollan un sistema que analiza automáticamente videos de sesiones de prueba de usuarios, extrayendo emociones faciales, transcribiendo el discurso del usuario a texto (Usando el modelo avanzado Whisper) y luego analizando la carga afectiva del texto con un modelo de emociones entrenado, para finalmente fusionar todos estos datos y generar insights accionables (Ghatoray & Li, 2025)

Otra evolución es la dinámica multimodal adaptativa, en lugar de combinar señales con pesos fijos, se investiga cómo ajustar la contribución de cada modalidad según la situación y la calidad de los datos, Satti et al. (2023) introducen funciones de mezcla generalizadas para asignar pesos dinámicos a

cada modalidad (video, audio, texto) dependiendo de su fiabilidad momento a momento (Por ejemplo, si el usuario deja de hablar, el sistema aumenta el peso de la expresión facial) (Razzaq et al., 2023).

En cuanto a la aceptación industrial, hacia 2025 comienzan a aparecer herramientas comerciales o prototipos avanzados que incorporan IA afectiva en el ciclo de diseño, como UXapp (Cordeiro et al., 2024) propone una plataforma que evalúa productos digitales mediante reconocimiento de emociones del usuario captadas por cámara, generando reportes para los diseñadores (referencia en (Ghatoray & Li, 2025).

En suma, la evolución 2018–2025 se caracteriza por: Un mayor volumen de investigación, un incremento sostenido de publicaciones que abordan emociones en UX (Galindo Monfil et al., 2025). Progreso tecnológico de métodos simples hacia deep learning multimodal, posibilitando una detección más precisa y en tiempo real. La integración práctica de experimentos aislados hacia herramientas integrales que automatizan la obtención de insights emocionales. Y el reconocimiento del valor de la emoción en UX, pasando de considerarse un "dato complementario" a un componente central para evaluar y optimizar diseños. No obstante, muchos estudios recientes advierten que la aplicación de IA en este campo aún enfrenta retos y está en consolidación, requiriendo validaciones adicionales antes de generalizarse plenamente en entornos industriales y comerciales

Conjuntos de datos utilizados en la evaluación de emociones en ux mediante ia

La disponibilidad de conjuntos de datos etiquetados de emociones ha sido un factor crucial para entrenar y evaluar los modelos de IA en este campo. A continuación, se resumen los principales datasets empleados en los últimos años, para el reconocimiento de emociones aplicable a UX, tanto multimodales como específicos por tipo de señal, estos conjuntos de datos proveen insumos para entrenar algoritmos que luego se aplican en contextos de UX, o bien sirven como benchmarks para comparar métodos.

- **DEAP (Database for Emotion Analysis using Physiological signals)**: Un dataset clásico (Koelstra et al. 2012) ampliamente reutilizado hasta la actualidad, que contiene señales fisiológicas de 32 sujetos (EEG, electrooculograma, GSR, ritmo cardiaco, respiración) mientras ven videos musicales emotivos, con etiquetas de emoción en dimensiones valencia/arousal, es relevante para UX porque proporciona datos biométricos bajo estímulos audiovisuales controlados, útiles para entrenar modelos que luego podrían aplicarse a reacciones de usuario ante interfaces multimedia.

- **FER-2013**: Conjunto de ~35k imágenes de rostros en escala de grises categorizadas en 7 emociones básicas, introducido en una competencia de Kaggle 2013, si bien más pequeño y con datos menos "en el mundo real" que AffectNet, sigue usándose como benchmark ligero. Por ejemplo, Ghatoray & Li (2025) probaron 10 modelos pre-entrenados de reconocimiento facial en FER-2013, AffectNet y CK+ para elegir el más generalizable (Ghatoray & Li, 2025). FER-2013 suele emplearse para pruebas rápidas o entrenar modelos simplificados que se puedan ejecutar en tiempo real durante sesiones de UX.

- **WESAD (Wearable Stress and Affect Dataset)**: Publicado en 2018 es un conjunto de datos de sensores wearables enfocado en estrés y afecto, registra señales fisiológicas (cardíacas, GSR, movimientos) de 15 sujetos

mediante un dispositivo tipo banda en el pecho (RespiBAN) y una pulsera, en condiciones de inducción de estrés, relajación y estado neutro, las etiquetas distinguen emociones como estrés vs calma vs diversión. WESAD ha cobrado importancia para entrenar modelos menos intrusivos (solo con *wearables*) que podrían integrarse en evaluaciones de UX móviles o *in-the-wild*. De hecho, estudios recientes privilegian el uso de dispositivos portables para obtener medidas emocionales continuas sin interrumpir la experiencia del usuario.

- **DREAMER**: Dataset de 2018 con 23 sujetos, datos **EEG y ECG** y etiquetas de valencia, activación y dominancia para estímulos audiovisuales emocionales, se destaca porque muchos estudios reportan resultados muy altos de precisión en él, por ejemplo 100% en clasificación binaria de valencia/activación sirviendo como banco de pruebas para nuevos algoritmos, aparece citado en numerosos trabajos recientes de reconocimiento emocional (Khare et al., 2024b).

- **AMIGOS (Augmented Multimodal Interaction dataset for emotion Recognition)**: Publicado en 2017, incluye 40 sujetos con datos multimodales (EEG, ECG, GSR, expresiones faciales en video) mientras ven videos cortos y socializan, con anotaciones de emociones en escalas continuo y discreto, en estudios revisados se menciona que AMIGOS es uno de los conjuntos públicos más usados para emoción multimodal junto con ASCERTAIN (Khare et al., 2024b).

- **ASCERTAIN**: Un dataset de 2018 diseñado para estudiar emociones influenciadas por rasgos de personalidad, registra señales multimodales (EEG, pulsioximetría, expresiones faciales) de 58 participantes expuestos a estímulos audiovisuales, con etiquetas de emoción en dimensiones V/A y también evaluación de rasgos de personalidad. ASCERTAIN ha sido utilizado en al menos 3 estudios recientes según el mapeo realizado (Khare et al., 2024b)

- **AffectNet**: Creado en 2017, es uno de los mayores datasets de expresiones faciales en imágenes estáticas, con ~0.4 millones de fotos de rostros recopiladas de Internet etiquetadas en 11 categorías emocionales + valores de valencia/arousal, es el estándar actual para entrenar y evaluar modelos de reconocimiento facial de emociones en entornos no controlados (Ghatoray & Li, 2025)

- **RAVDESS (Ryerson Audio-Visual Database of Emotional Speech and Song)**: Dataset de 2018 con 24 actores que recitan frases con distintas emociones (calma, alegría, tristeza, enojo, miedo, disgusto, sorpresa) en audio y video, es utilizado para entrenar o evaluar sistemas bimodales de emoción (cara+voz) a pequeña escala. Por ejemplo, proyectos experimentales de UX han usado RAVDESS para probar algoritmos que detecten automáticamente el estado emocional del usuario tanto por su rostro como por su voz en escenarios como videojuegos.

- **Conjuntos de datos de texto (NLP)**: En análisis de sentimiento aplicado a UX, se suelen utilizar corpora estándar de opiniones y también datos específicos del dominio, entre los generales se encuentra IMDb reviews (sentimiento de reseñas de películas), Sentiment140 o SemEval (tweets etiquetados en sentimiento o emoción) y el mencionado GoEmotions (Reddit, 27 emociones). Además, existen datasets enfocados en aspectos de usabilidad, por ejemplo corpus de reseñas de aplicaciones móviles donde cada review está etiquetada con facetas de UX (desempeño, UI, etc.) y polaridad (Alonazi, 2023).

- **DUX (Dataset of User eXperience)**: Publicado en 2023, este conjunto de datos fue diseñado específicamente para la intersección de emociones y UX. Reconociendo que *"*no existía un dataset público para reconocimiento de emociones a partir solo de interacciones (teclado, ratón, táctil)", Leppich et al. (2023) crearon DUX para llenar ese vacío (Leppich et al., 2023).

Tabla 1. *Conjuntos de datos más utilizados para el análisis automático de emociones en UX.*

Conjunto de Datos	Modalidad	Emociones	Uso en investigación UX
FER2013 (Goodfellow et al., 2013)	Imágenes faciales (estáticas)	7 emociones básicas	Referencia estándar para entrenar clasificadores faciales de emociones; ampliamente usado en estudios de UX por su disponibilidad (Santos & Digiampietri, 2024).
AffectNet (Mollahosseini et al., 2019)	Imágenes faciales (in-the-wild)	8 emociones + valores de valencia/arousal	Gran base de datos en condiciones no controladas; permite mejorar la generalización de modelos de expresión facial (Mollahosseini et al., 2019).
IEMOCAP (Busso et al., 2008)	Audio-visual (diálogos actuados)	6 emociones básicas (audio y video)	Muy utilizada para entrenar y evaluar reconocimiento de emociones en la voz y gestos; benchmark en muchos trabajos de HCI (Razzaq et al., 2023).
RAVDESS (Livingstone & Russo, 2018)	Audio-visual (actuaciones)	8 emociones (voz y expresión)	Conjunto controlado de expresiones vocales y faciales, empleado para modelos multimodales en contextos controlados (Razzaq et al., 2023).
EMORepository / Kaggle	Texto (opiniones) o Imágenes	Depende del dataset (sentimiento o emociones básicas)	Colecciones públicas para *sentiment analysis* (p. ej., reseñas) o retos de emociones faciales (FER, Emotion Kaggle); útiles para adaptar IA a casos de UX textuales o visuales (Santos & Digiampietri, 2024).
Datasets propietarios	Multimodal (video UX, sensores)	Emociones definidas por el estudio (e.g., frustración, engagement)	Muchos investigadores crean sus propios datasets de pruebas de usuario (grabaciones de video, interacciones instrumentadas) para entrenar modelos adaptados a su contexto específico (Santos & Digiampietri, 2024).

Como se observa, FER2013 destaca como uno de los conjuntos más frecuentes para reconocimiento facial en UX (Santos & Digiampietri, 2024), probablemente por su fácil acceso y amplia etiqueta de emociones. Sin embargo, también se han incorporado datasets más ricos, como AffectNet que provee cientos de miles de rostros en entornos variados con anotaciones continuas de afecto, lo que ha permitido entrenar modelos más generalizables a situaciones del mundo real (Mollahosseini et al., 2019).

En el dominio del audio, corpus como IEMOCAP y RAVDESS son la referencia para evaluar la

capacidad de la IA en detectar emociones a partir de la voz, incluyendo matices como el tono y la cadencia emocional en el habla (Razzaq et al., 2023), para análisis de sentimientos en texto orientado a UX, es común reutilizar conjuntos de reseñas de usuarios o tweets etiquetados emocionalmente (por ejemplo, datasets de competencias SemEval o colecciones de opiniones de productos). Adicionalmente, la tabla refleja que no existe un único dataset "UX-emotions" estándar, sino que a menudo los investigadores generan sus propios datos durante estudios de usuario instrumentados (Santos & Digiampietri, 2024), esto se debe a que las emociones en UX pueden ser muy contextuales; por ende, grabar sesiones de interacción reales (con cámaras, micrófonos, sensores) y luego etiquetar manualmente las emociones experimentadas ofrece datos más específicos para entrenar modelos enfocados en predecir experiencias particulares (como detectar frustración en el uso de cierto software).

En general, los datasets más utilizados reflejan las distintas modalidades, son los de señales fisiológicas (DEAP, MAHNOB, WESAD, ASCERTAIN) alimentan desarrollos en detección de estados internos; los de expresión facial y vocal (AffectNet, FER-2013, IEMOCAP, RAVDESS) potencian sistemas de observación externa no intrusiva; y datasets de texto (GoEmotions, etc.) que permiten extraer sentimientos de las palabras de los usuarios, se muestra preferencia por datasets multimodales públicos que combinen varias entradas (p.ej., audio+video+EEG) para entrenar modelos integrales (Khare et al., 2024b), si bien aún se carece de suficientes datos multimodales "en el mundo real", una línea emergente es la generación de nuevos conjuntos de datos de emociones específicos de UX, como DUX, que capturen interacciones naturales con sistemas, esta ampliación de datos disponibles seguirá siendo fundamental para avanzar el campo, pues muchos desafíos actuales (generalización, sesgo) se deben en parte a la limitada diversidad de los datasets empleados.

Métricas para validar la precisión y efectividad de los modelos de ia en evaluación de emociones en ux

Para evaluar el desempeño de los modelos de IA en la tarea de reconocer emociones, se utilizan principalmente las mismas métricas clásicas que en otros problemas de clasificación y predicción, adaptadas al contexto de emociones, entre las métricas cuantitativas más comunes reportadas en la literatura se incluyen:

- **Exactitud (accuracy)**: Proporción de aciertos del modelo, es decir, el porcentaje de casos en que la emoción predicha coincidió con la etiqueta real, es una métrica general fácil de interpretar, es así, que una exactitud del 90% indica que en 9 de cada 10 instancias el sistema clasificó correctamente la emoción (Por ejemplo identificó correctamente si el usuario estaba frustrado o no). Muchos trabajos informan esta métrica; de hecho, se cita accuracy en prácticamente todos los estudios de reconocimiento emocional (Khare et al., 2024b). Sin embargo, puede ser engañosa si las clases están desequilibradas (por ejemplo, si el 80% de las muestras son "neutral" el modelo puede lograr 80% de accuracy prediciendo siempre "neutral" sin realmente funcionar para las otras emociones), por ello se complementa con otras medidas.

- **Precisión y Exhaustividad (Precision & Recall)**: Estas métricas evalúan el rendimiento por clase (emociones específicas) considerando falsos positivos y falsos negativos. Precisión (también llamada valor predictivo positivo) mide qué proporción de las predicciones de una emoción fueron

correctas; Recall (o sensibilidad) mide qué proporción de las ocurrencias reales de esa emoción fueron detectadas por el modelo. Por ejemplo, en la detección de "frustración" durante una tarea, la precisión indica cuántos de los casos que el modelo marcó como "frustrado" efectivamente lo estaban (evitando alarmas falsas), mientras que la exhaustividad indica cuántos de todos los usuarios frustrados el modelo logró identificar (evitando omisiones) (Khare et al., 2024b).

- **Puntuación F1**: Es la media armónica de precisión y recall, proporcionando un solo indicador por clase que equilibra ambos. La F1-score es útil para comparar modelos cuando hay clases desbalanceadas o cuando se quiere una métrica que penalice tanto los falsos positivos como los falsos negativos; muchos artículos utilizan el promedio F1 macro (promediado sobre todas las clases de emoción) como métrica principal de desempeño del sistema, ya que resume su capacidad global considerando cada clase por igual (Khare et al., 2024b)

- **Matriz de confusión**: Si bien no es un "índice" numérico único, la matriz de confusión es un resultado esencial que muestran las investigaciones, que detalla para cada emoción verdadera, cómo se distribuyen las predicciones del modelo (aciertos y confusiones con otras emociones), esto permite ver patrones, Por ejemplo si la emoción "sorpresa" suele ser confundida con "alegría", o "neutral" con "aburrimiento". Es muy útil en UX para entender qué errores comete el modelo, lo que puede guiar mejoras (quizás se necesita más datos o ajustar la definición de ciertas emociones).

- **ROC-AUC (Area Under the ROC Curve)**: En escenarios binarios (Por ejemplo, detectar si el usuario está experimentando una emoción negativa vs no), se utiliza la curva ROC que muestra la tasa de verdaderos positivos vs falsos positivos a distintos umbrales, y su área bajo la curva (AUC) como medida de desempeño global, un AUC de 0.5 indica desempeño aleatorio, 0.9 un modelo muy bueno, en problemas multiemoción, a veces se computa el AUC para cada clase versus el resto.

- **Medidas específicas de regresión**: Cuando las emociones se tratan en dimensiones continuas (valencia, activación) en lugar de categorías discretas, se emplean métricas de regresión como RMSE (root mean square error) o coeficiente de correlación de Pearson entre las predicciones continuas del modelo y los valores auto-reportados. Por ejemplo, si un modelo predice nivel de estrés en escala 1–10, se medirá cuánto difiere de las valoraciones reales del usuario promedio.

- **Índices kappa o alfa**: En algunos trabajos, especialmente aquellos que comparan la IA contra evaluadores humanos, se usan métricas de concordancia como Cohen's kappa para ver qué tan de acuerdo está el modelo con etiquetas de referencia teniendo en cuenta la concordancia por azar.

En suma, la exactitud global (accuracy) es la métrica más reportada, indicando el porcentaje de aciertos en la detección de la emoción correcta, Razzaq *et al.* (2023) informan que su modelo multimodal H-MMER alcanza un 98.2% de accuracy promedio reconociendo cuatro estados emocionales básicos, superando abordajes previos; No obstante, dado que la distribución de emociones suele ser desigual, también se emplean métricas por clase como la precisión y recuperación (*precision/recall*) por emoción, y el puntaje F1 que equilibra ambas, para asegurar que emociones minoritarias (como "miedo" o "asco") no queden totalmente opacadas por las

mayoritarias (Santos & Digiampietri, 2024). Es común ver matrices de confusión en los estudios, detallando cuánto se confunden unas emociones con otras y destacando cuáles se reconocen mejor o peor (Razzaq et al., 2023). Por ejemplo, en un experimento de reconocimiento a partir de audio, la emoción *enojo* pudo reconocerse con ~71% de acierto mientras tristeza cayó por debajo de 60%, evidenciando diferencias en detectabilidad según la emoción, además de las métricas puramente algorítmicas, en contexto UX interesa validar cómo esas detecciones reflejan la experiencia del usuario. Por ello, algunos trabajos correlacionan las salidas del modelo con medidas de UX establecidas, un enfoque es comparar la predicción de la IA sobre si un usuario tuvo una UX positiva o negativa con las puntuaciones reales que el usuario dio en cuestionarios de usabilidad/satisfacción. Es así, que Koonsanit & Nishiuchi (2020) extrajeron características emocionales de rostros junto con datos demográficos para predecir el nivel de UX, y luego compararon esa predicción con las respuestas del usuario en un formulario post-uso, obteniendo así una validez concurrente de su método (Santos & Digiampietri, 2024). De manera similar, métricas de correlación (coeficiente de Pearson, etc.) se han utilizado cuando las emociones se miden en dimensiones continuas (valencia/arousal) para ver cuán cerca sigue el modelo las autoevaluaciones emocionales del usuario en escala de agrado, estrés, etc. Concluyentemente, se evidencia que se emplea un conjunto amplio de métricas para validar estos sistemas: desde tasas de clasificación correctas, hasta concordancia con evaluaciones humanas, asegurando tanto la efectividad técnica del modelo como su relevancia práctica para inferir la experiencia del usuario.

Discusión

Principales desafíos y limitaciones en la aplicación de ia para evaluar emociones en ux

Aunque las técnicas de IA para detección de emociones han avanzado notablemente, su aplicación en la evaluación de UX enfrenta desafíos significativos y limitaciones que deben ser considerados:

- **Generalización y robustez limitada**: Un desafío mayor es lograr que los modelos funcionen bien más allá de las condiciones en que fueron entrenados, ya que muchos sistemas de reconocimiento emocional muestran un desempeño excelente en datasets de laboratorio, pero bajan su precisión en escenarios reales de UX donde las condiciones varían (iluminación diferente, ruido de fondo, diversidad de usuarios); La presente investigación ha identificado falta de generalización debido a diferencias en dispositivos de adquisición y duraciones de señales utilizadas (Khare et al., 2024b). Por ejemplo, un modelo entrenado con videos frontales puede fallar si la cámara del usuario está en ángulo lateral; o un modelo de voz entrenado con pocos acentos puede no generalizar a usuarios de otras nacionalidades. Esta sensibilidad reduce la confianza en usar estos modelos directamente en evaluaciones de UX amplias, para lo que se requieren más datos diversos y técnicas como domain adaptation para mejorar la robustez.

- **Falta de explicabilidad y confianza en los resultados**: Las salidas de un modelo de IA emocional a veces contradicen la intuición o la información de otras fuentes, generando desconfianza en stakeholders y expertos humanos (Khare et al., 2024b). Por ejemplo, si un sistema indica “alto nivel de frustración”

pero el usuario en la grabación parece calmado según un observador, se duda del sistema. Por eso se considera que muchos modelos de deep learning son cajas negras, por lo que especialistas en UX son reticentes a basar decisiones de diseño en ellos sin entendimiento del porqué de sus inferencias, eso sin duda es un desafío crítico, ya que se necesitan técnicas de IA explicable (XAI) que permitan interpretar qué indicadores (rasgos faciales, tono, etc.) llevaron a la conclusión de cierta emoción; Es decir, sin explicaciones, es difícil confiar plenamente en la IA, limitando su adopción práctica.

- **Ambigüedad y complejidad de las emociones humanas**: Detectar emociones no es tan sencillo como identificar un color o un objeto; las emociones son estados internos complejos, a veces sutiles, y los observables pueden ser engañosos, porque un mismo gesto (Por ejemplo suspirar) puede significar alivio, aburrimiento o frustración dependiendo del contexto y los modelos actuales aún luchan con contexto, sarcasmo, y múltiples emociones concurrentes (Nandwani & Verma, 2021).

- **Limitaciones en tiempo real e intrusividad**: Algunos métodos de IA aún no son prácticos para uso en tiempo real durante pruebas UX, como procesar señales EEG con modelos complejos puede introducir latencia, dificultando retroalimentación inmediata, también, ciertos sensores (EEG, GSR con electrodos) siguen siendo intrusivos y pueden afectar la naturalidad de la experiencia del usuario durante la evaluación; Si la tecnología de detección interfiere con la UX que se pretende medir, hay un compromiso metodológico, aunque se tiende a métodos más pasivos (cámara, micrófono, *wearables* cómodos), esta sigue siendo una limitación para lograr que la recogida de datos afectivos no altere el comportamiento normal del usuario (Zhang et al., 2024).

- **Integración con flujos de trabajo de UX**: Desde una perspectiva práctica, otra limitación es cómo integrar estas mediciones en el proceso de evaluación UX existente, ya que los equipos de UX tradicionales quizá no cuenten con expertos en datos o en IA para interpretar resultados, ni con infraestructura para almacenar y procesar grandes volúmenes de video/biometría; Existe una curva de adopción y algunas herramientas comienzan a abstraer esto, pero aún es un cambio de paradigma. Además, se debe demostrar valor añadido claro, porque tras implementar un sistema complejo de medición de emociones los hallazgos no difieren mucho de lo que un buen investigador de UX cualitativo habría notado, puede cuestionarse su costo-beneficio (Ghatoray & Li, 2025).

- **Validación cruzada con métricas UX**: Un desafío final es validar que las métricas afectivas que provee la IA realmente reflejen la calidad de la UX. Por ejemplo, si un modelo indica que los usuarios tuvieron valencia promedio de 0.6 (ligeramente positiva) durante una tarea, ¿cómo se relaciona eso con métricas clásicas como éxito de tarea o puntuación SUS de usabilidad? Aún se está investigando la correlación entre las métricas emocionales y las métricas de UX tradicionales, la falta de correlaciones fuertes podría indicar que estamos midiendo algo diferente o que la IA no capta completamente la experiencia; Un tema abierto y de gran importancia, asegurar que las salidas de IA tengan sentido práctico en la evaluación de UX.

Estos desafíos resaltan que, si bien la IA ofrece herramientas poderosas para evaluar emociones, su aplicación exitosa en UX requiere abordar

cuestiones técnicas (mejorar generalización, explicar modelos), aumentar y diversificar los datos de entrenamiento, y considerar factores humanos (privacidad, interpretación), muchos trabajos de revisión recientes concluyen con recomendaciones de investigación orientadas a superar estos retos, como desarrollar modelos adaptativos, fusionar información de manera más inteligente, generar datasets multimodales más amplios, incorporar XAI y cuantificar incertidumbre en las predicciones (Khare et al., 2024b).

Tendencias emergentes y oportunidades

Mirando hacia el futuro, se vislumbran varias tendencias emergentes que presentan oportunidades de avance, así como nuevos desafíos, en la intersección de IA, emociones y UX, una tendencia clara es profundizar en la integración multimodal y contextual de las evaluaciones, si bien ya se combinan rostro, voz y texto, emergen propuestas para agregar aún más fuentes de datos del usuario, por ejemplo, incorporar sensores fisiológicos (EEG, pulso, dilatación pupilar) para obtener una lectura emocional más profunda que complemente las expresiones externas (Ghatoray & Li, 2025), esto podría brindar oportunidades en aplicaciones donde la UX emocional es crítica (salud digital, entrenamiento, VR), al detectar estados internos como estrés o atención de forma más fiable. De hecho, investigaciones en Brain-Computer Interfaces afectivos sugieren que fusionar señales cerebrales con comportamiento podría mejorar notablemente la detección de emociones sutiles (He et al., 2020) . El reto será manejar la complejidad añadida y garantizar la comodidad del usuario al involucrar estos sensores.

Relacionado a lo anterior, se prevé un empuje hacia sistemas de detección emocional en tiempo real totalmente integrados en la interfaz, esto permitiría que las aplicaciones no solo evalúen la UX *a* posteriori*,* sino que adapten dinámicamente la experiencia según las emociones del usuario en el momento (Ghatoray & Li, 2025). Por ejemplo, un software tutor podría simplificar las instrucciones si detecta frustración, o un sitio de comercio podría ofrecer asistencia inmediata si percibe confusión o insatisfacción. Lograr esta "UX adaptable emocionalmente" es una oportunidad emocionante para mejorar la personalización y empatía de los sistemas con el usuario, ya existen trabajos exploratorios donde asistentes conversacionales de UX brindan recomendaciones al evaluador basadas en análisis automáticos previos (De Souza Veriscimo et al., 2021), prefigurando una colaboración humano-IA en la evaluación UX, para que esto sea realidad amplia, deberán superarse desafíos de latencia y garantizar que las respuestas del sistema ante las emociones sean apropiadas y beneficiosas.

Otra tendencia emergente es la aplicación de modelos de lenguaje grandes (LLMs) y enfoques de IA generativa para asistir en el análisis de las emociones. Por un lado, modelos como GPT-4 están siendo utilizados para resumir hallazgos de datos de UX, traduciendo los resultados de análisis emocionales en insights narrativos accionables. Un ejemplo reciente integró un asistente tipo chatbot basado en GPT para que, tras recopilar las emociones detectadas en video y texto de una sesión, respondiera preguntas del diseñador de UX en lenguaje natural sobre dónde tuvo problemas el usuario (Ghatoray & Li, 2025), esto facilita que investigadores de UX, que no son expertos en ciencia de datos, aprovechen el poder de IA avanzadas para interpretar patrones emocionales sin perder tiempo en crudos análisis de señal. Además, los LLM ofrecen la oportunidad de analizar grandes colecciones de feedback textual de usuarios (como miles de comentarios) extrayendo temas emocionales recurrentes y correlacionándolos con elementos de la interfaz – tareas que antes hubieran requerido análisis manual intensivo. La tendencia

sugiere que la IA no solo medirá emociones, sino que ayudará a explicar y contextualizar el rol de esas emociones en la experiencia de usuario de manera comprensible para diseñadores y partes interesadas.

En el horizonte también se encuentran innovaciones en técnicas de fusión y aprendizaje, se exploran frameworks híbridos más sofisticados que combinen lo mejor de la fusión temprana y tardía, e incluso enfoques de aprendizaje federado o en el dispositivo para preservar privacidad (de modo que el modelo aprenda de muchos usuarios sin centralizar sus datos emocionales sensibles). Asimismo, hay oportunidades en emplear aprendizaje por refuerzo donde un agente IA modifique elementos de la interfaz y aprenda, mediante retroalimentación emocional del usuario, qué diseños optimizan la experiencia. Este tipo de sistema autónomo podría iterar mejoras de UX de forma personalizada, aunque conlleva desafíos técnicos y éticos.

Por último, surgen consideraciones éticas y de regulación como tendencia obligada, a nivel global, se debate la regulación de los llamados "sistemas de IA de reconocimiento de emociones" dada la sensibilidad de su uso (Por ejemplo, la Unión Europea ha propuesto restringir aplicaciones que puedan violar derechos o resultar en manipulación emocional) (ibdehere, 2023). En el contexto de UX, esto implica que las investigaciones y herramientas deberán adherirse a principios de diseño ético, transparencia en la inferencia emocional y obtención de consentimiento claro de los participantes, que lejos de ser un obstáculo, esto abre la oportunidad de diseñar mejores prácticas y estándares en la industria para el uso responsable de IA afectiva, lo que podría aumentar la confianza en estas tecnologías y facilitar su adopción.

En síntesis, las tendencias apuntan a sistemas de evaluación de UX cada vez más inteligentes, omnipresentes y centrados en el humano, que aprovechan IA multimodal en tiempo real y análisis avanzado para comprender al usuario a un nivel sin precedentes, las oportunidades para mejorar la personalización, accesibilidad y eficacia de las interfaces mediante la detección emocional son enormes, no obstante, alcanzar esa visión requerirá afrontar retos técnicos (robustez, tiempo real), ampliar repertorios emocionales y navegar cuidadosamente implicaciones éticas, la convergencia de disciplinas desde la ingeniería de datos hasta la psicología y el diseño será crucial en esta próxima etapa.

Conclusiones

La revisión integrativa de trabajos de los últimos siete años muestra que la IA se ha convertido en un aliado prometedor para enriquecer la evaluación de UX mediante el análisis de emociones y sentimientos de los usuarios, se han identificado los métodos más empleados (Visión por computador, audio, PLN, sensores) y constatado que su combinación multimodal potencia la eficacia de la medición emocional en HCI (Razzaq et al., 2023).

La aplicación de IA en este ámbito ha evolucionado rápidamente, pasando de enfoques experimentales a soluciones más maduras que se apoyan en aprendizaje profundo y grandes volúmenes de datos, expandiendo el alcance del análisis emocional a entornos de uso reales y datos no estructurados (Guo et al., 2024) (Alabduljabbar, 2024). Asimismo, se ha destacado los principales recursos (datasets, métricas) que sostienen estas investigaciones, junto con los desafíos vigentes, técnicos, humanos y éticos, que limitan por ahora su máximo potencial (Santos & Digiampietri, 2024), que lejos de ser obstáculos insuperables, estos retos proporcionan una hoja de ruta para futuras investigaciones para mejorar la robustez y rapidez de los modelos, abarcar mayor diversidad

emocional y asegurar equidad y privacidad en las inferencias.

En definitiva, integrar el análisis automatizado de emociones en la evaluación de UX ofrece una visión más rica y holística de la experiencia del usuario, incorporando la dimensión afectiva que tradicionalmente era difícil de captar objetivamente, esto debe permitir a diseñadores e investigadores comprender no solo qué hace el usuario, sino cómo se siente mientras lo hace, lo cual es invaluable para crear productos más satisfactorios, intuitivos y adaptados. Las tendencias emergentes indican que esta línea de trabajo seguirá creciendo, con IA cada vez más sofisticada capaz de empatizar con el usuario y apoyar tanto la evaluación como la optimización continua de las interfaces (Ghatoray & Li, 2025), en un campo tan dinámico, mantener el rigor científico y la centricidad en el ser humano será crucial: los modelos deberán ser validados exhaustivamente y usados como herramientas de apoyo para la toma de decisiones de diseño, y no como sustitutos absolutos de la comprensión humana. Con este equilibrio, la IA aplicada al análisis de emociones en UX se perfila como una pieza clave en la siguiente generación de metodologías de evaluación, brindando oportunidades sin precedente para innovar en la creación de experiencias de usuario más afectivamente conscientes, personalizadas y satisfactorias.

Referencias bibliográficas

Alabduljabbar, R. (2024). User-centric AI: Evaluating the usability of generative AI applications through user reviews on app stores. *PeerJ Computer Science*, *10*, e2421. https://doi.org/10.7717/peerj-cs.2421

Alonazi, M. (2023). Analyzing sentiment in terms of online feedback on top of users' experiences. *International Journal of Advanced Computer Science and Applications*, *14*(11). https://doi.org/10.14569/IJACSA.2023.0141114

Busso, C., Bulut, M., Lee, C.-C., Kazemzadeh, A., Mower, E., Kim, S., Chang, J. N., Lee, S., & Narayanan, S. S. (2008). IEMOCAP: Interactive emotional dyadic motion capture database. *Language resources and evaluation*, *42*(4), 335-359. https://doi.org/10.1007/s10579-008-9076-6

De Souza Veriscimo, E., Bernardes Júnior, J. L., & Digiampietri, L. A. (2021). Facial emotion recognition in UX evaluation: A systematic review. En M. Kurosu (Ed.), *Human-Computer Interaction. Theory, methods and tools* (Vol. 12762, pp. 521-534). Springer International Publishing. https://doi.org/10.1007/978-3-030-78462-1_40

Fernández-Ordóñez, J. M., Jiménez, L. E. M., Torres-Carrión, P., Barba-Guamán, L., Rodríguez-Morales, G.. (2019). Experiencia afectiva usuario en ambientes con inteligencia artificial, sensores biométricos y/o recursos digitales accesibles: Una revisión sistemática de literatura. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, *35*, 35-53. https://doi.org/10.17013/risti.35.35-53

Galindo Monfil, A. R., Rojano Cáceres, J. R., & Mezura Godoy, C. (2025). Evaluación de las emociones y la satisfacción del usuario en el contexto de la interacción humano computadora: Un mapeo sistemático. *ReCIBE, Revista electrónica de Computación, Informática, Biomédica y Electrónica*, *14*(1), C9-12. https://doi.org/10.32870/recibe.v14i1.401

Ghatoray, S. K., & Li, Y. (2025). *Automated UX Insights from User Research Videos by Integrating Facial Emotion and Text Sentiment* (Versión 1). arXiv. https://doi.org/10.48550/ARXIV.2503.22510

Goodfellow, I. J., Erhan, D., Carrier, P. L., Courville, A., Mirza, M., Hamner, B., Cukierski, W., Tang, Y., Thaler, D., Lee, D.-H., Zhou, Y., Ramaiah, C., Feng, F., Li, R., Wang, X., Athanasakis, D., Shawe-Taylor, J., Milakov, M., Park, J., … Bengio, Y. (2013). *Challenges in representation learning: A report on three machine learning contests* (Versión 1). arXiv. https://doi.org/10.48550/ARXIV.1307.0414

Guo, R., Guo, H., Wang, L., Chen, M., Yang, D., & Li, B. (2024). Development and application of emotion recognition technology—A systematic literature review. *BMC Psychology*, *12*(1), 95. https://doi.org/10.1186/s40359-024-01581-4

He, Z., Li, Z., Yang, F., Wang, L., Li, J., Zhou, C., & Pan, J. (2020). Advances in multimodal emotion recognition based on brain–computer interfaces. *Brain Sciences*, *10*(10), 687. https://doi.org/10.3390/brainsci10100687

Hernandez Perez, L. A. (2022). Método para la detección de emociones mediante el análisis de expresión facial en videos de evaluación de la experiencia de usuario. https://rinacional.tecnm.mx/jspui/handle/TecNM/4841

Ibdehere. (2023, junio 19). Inteligencia artificial y reconocimiento biométrico de emociones: Una valoración a la luz de las enmiendas del Parlamento europeo a la Ley de Inteligencia Artificial. *UNA MIRADA CRÍTICA A LAS RELACIONES LABORALES*. https://ignasibeltran.com/2023/06/19/inteligencia-artificial-y-reconocimiento-biometrico-de-emociones-una-valoracion-a-la-luz-de-las-enmiendas-del-parlamento-europeo-a-la-ley-de-inteligencia-artificial/

Khare, S. K., Blanes-Vidal, V., Nadimi, E. S., & Acharya, U. R. (2024). Emotion recognition and artificial intelligence: A systematic review (2014–2023) and research recommendations. *Information Fusion*, *102*, 102019. https://doi.org/10.1016/j.inffus.2023.102019

Koelstra, S., Muhl, C., Soleymani, M., Jong-Seok Lee, Yazdani, A., Ebrahimi, T., Pun, T., Nijholt, A., & Patras, I. (2012). DEAP: A Database for emotion analysis: Using physiological signals. IEEE transactions on affective computing, 3(1), 18-31. https://doi.org/10.1109/T-AFFC.2011.15

Leppich, D., Bieber, C., Proschek, K., Harms, P., & Schubert, U. (2023). DUX: A dataset of user interactions and user emotions. *I-Com*, *22*(2), 101-123. https://doi.org/10.1515/icom-2023-0014

Liu, F. (2024). Artificial intelligence in emotion quantification: A prospective overview. *CAAI Artificial Intelligence Research*, 9150040. https://doi.org/10.26599/AIR.2024.9150040

Livingstone, S. R., & Russo, F. A. (2018). The ryerson audio-visual database of emotional speech and song (RAVDESS): A dynamic, multimodal set of facial and vocal expressions in North American English. *PLOS ONE*, *13*(5), e0196391. https://doi.org/10.1371/journal.pone.0196391

Mollahosseini, A., Hasani, B., & Mahoor, M. H. (2019). AffectNet: A Database for facial expression, valence, and arousal computing in the wild. *IEEE Transactions on Affective Computing*, *10*(1), 18-31. https://doi.org/10.1109/TAFFC.2017.2740923

Nandwani, P., & Verma, R. (2021). A review on sentiment analysis and emotion detection from text. *Social Network Analysis and Mining*, *11*(1), 81. https://doi.org/10.1007/s13278-021-00776-6

Pereira, R., Mendes, C., Ribeiro, J., Ribeiro, R., Miragaia, R., Rodrigues, N., Costa, N., & Pereira, A. (2024). Systematic review of emotion

detection with computer vision and deep learning. sensors, 24(11), 3484. https://doi.org/10.3390/s24113484.

Plisiecki, H., Lenartowicz, P., Flakus, M., & Pokropek, A. (2025). High risk of political bias in black box emotion inference models. *Scientific Reports*, *15*(1), 6028. https://doi.org/10.1038/s41598-025-86766-6

Razzaq, M. A., Hussain, J., Bang, J., Hua, C.-H., Satti, F. A., Rehman, U. U., Bilal, H. S. M., Kim, S. T., & Lee, S. (2023). A hybrid multimodal emotion recognition framework for UX evaluation using generalized mixture functions. *Sensors*, *23*(9), 4373. https://doi.org/10.3390/s23094373

Santos, B. L., & Digiampietri, L. A. (2024). User experience evaluation using machine learning and facial expressions: A systematic review. *Anais do XXI Encontro Nacional de Inteligência Artificial e Computacional (ENIAC 2024)*, 930-941. https://doi.org/10.5753/eniac.2024.245150

Verhoef, T., & Fosch-Villaronga, E. (2023). Towards affective computing that works for everyone. *2023 11th International Conference on Affective Computing and Intelligent Interaction (ACII)*, 1-8. https://doi.org/10.1109/ACII59096.2023.10388169

Zhang, Z., Fort, J. M., & Giménez Mateu, L. (2024). Mini review: challenges in EEG emotion recognition. frontiers in psychology, 14, 1289816. https://doi.org/10.3389/fpsyg.2023.1289816

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/

USO DE BLOCKCHAIN EN LA GESTIÓN CLÍNICA PARA ECOSISTEMAS SANITARIOS RESILIENTES Y CONFIABLES

USING BLOCKCHAIN IN CLINICAL MANAGEMENT FOR RESILIENT AND RELIABLE HEALTHCARE ECOSYSTEMS

Remberto Gonzales Cruz
Universidad San Francisco Xavier
gonzales.remberto@usfx.bo

Recibido: 29 Abril 2025 / Revisado: 20 Agosto 2025 / Aceptado: 1 Septiembre 2025 / Publicado: 23 Septiembre 2025

Resumen

La gestión de historias clínicas plantea desafíos estructurales significativos relacionados con la interoperabilidad, la seguridad y la privacidad de los datos. Estos desafíos se acentuaron durante la pandemia de COVID-19, donde la falta de acceso oportuno y fiable a la información médica afectó directamente la capacidad de respuesta de los sistemas de salud. Este artículo se centra en un análisis teórico del uso de la tecnología blockchain como alternativa para la gestión descentralizada, segura y trazable de los registros clínicos. Se examinan los principios de funcionamiento de esta tecnología, sus componentes arquitectónicos clave, como IPFS, contratos inteligentes e identidad digital. Además, se discute su viabilidad desde una perspectiva jurídica, considerando regulaciones estatales. El estudio propone un marco conceptual que permite evaluar los beneficios potenciales, limitaciones y condiciones necesarias para la implementación de blockchain en sistemas de información sanitaria. A través de una revisión sistemática de literatura y el análisis de casos relevantes, se pretende ofrecer una visión amplia, crítica y fundamentada sobre el impacto transformador de blockchain en la administración de historias clínicas.

Palabras Clave: Blockchain, Ipfs, Seguridad, Trazabilidad, Historia Clínica, Salud

Introducción

La gestión de historias clínicas constituye un desafío estructural en los sistemas de salud, marcado por la falta de interoperabilidad, la escasa protección de la privacidad del paciente y la limitada capacidad de compartir información médica de manera segura entre instituciones. Estos problemas se hicieron especialmente evidentes durante la pandemia de COVID-19, cuando la inaccesibilidad oportuna a los datos clínicos obstaculizó la capacidad de respuesta de los sistemas sanitarios Domingos & Goncalves, (2023) . Esta crisis puso en relieve la necesidad urgente de contar con soluciones tecnológicas que permitan una administración más eficiente, confiable y descentralizada de los registros médicos.

En este contexto, la tecnología Blockchain ha emergido como una alternativa prometedora para transformar la forma en que se gestionan los datos clínicos, al ofrecer propiedades como inmutabilidad, trazabilidad, descentralización y control granular de acceso. No obstante, su adopción en el sector salud requiere un análisis riguroso que contemple tanto los fundamentos técnicos como las implicaciones legales, éticas y organizativas. El presente trabajo tiene como objetivo general analizar desde una perspectiva teórica los principios, ventajas y limitaciones del uso de Blockchain en la gestión de historias clínicas. Específicamente, se propone explorar modelos arquitectónicos descentralizados aplicables a entornos clínicos, evaluar la contribución de tecnologías complementarias como IPFS e identidad digital, y reflexionar sobre los marcos regulatorios asociados a la protección de datos sensibles.

Diversos estudios han abordado el potencial de Blockchain en el ámbito biomédico y sanitario. Vazirani et al., (2019) realizó una revisión sistemática destacando la eficiencia de esta tecnología para mejorar la interoperabilidad clínica. De manera similar, Albiol-Perarnau & Alarcón Belmonte, (2024) enfatizan su aporte en el fortalecimiento de la seguridad de los datos médicos, mientras que Esposito et al., (2018) destaca su utilidad como solución para la privacidad en entornos de nube sanitaria. En el plano regional, investigaciones como la de Riveros Lancheros et al., (2019) ha demostrado la factibilidad técnica de implementar redes Blockchain en sistemas de salud latinoamericanos, aunque también reconocen barreras regulatorias y culturales que deben ser superadas.

Así, este trabajo se inscribe en una línea de investigación que no solo busca introducir tecnologías emergentes en los sistemas de información clínica, sino también fomentar un ecosistema de salud más transparente, seguro y centrado en el paciente.

Metodología

Este estudio adopta un diseño teórico-descriptivo, el cual integra una revisión sistemática de la literatura científica, un análisis conceptual y técnico de arquitecturas, la sistematización de casos piloto documentados y una revisión jurídica y de políticas públicas. El propósito central es combinar evidencia publicada (artículos, revisiones y estudios de caso), desarrollos técnicos y documentos normativos para construir un marco analítico sólido sobre la aplicabilidad de tecnologías blockchain y de sus componentes asociados como IPFS, contratos inteligentes e identidad digital en la gestión de historias clínicas.

La metodología se organiza en los siguientes ejes:

- **Revisión sistemática de literatura científica:** Se identificaron, consultaron y sintetizaron estudios que evalúan o describen aplicaciones,

arquitecturas, experiencias piloto y análisis legales relacionados con blockchain en el ámbito sanitario. Las búsquedas se realizaron en revistas indexadas como *Journal of Medical Internet Research, IEEE Access y Health Informatics Journal*. Esta revisión incluyó estudios de caso, revisiones sistemáticas y artículos teóricos Albiol-Perarnau & Alarcón Belmonte, (2024); Bermúdez Ocampo et al., (2023); Vazirani et al., (2019). Asimismo, se complementó con búsquedas en repositorios académicos como Google Scholar y en documentos institucionales, entre ellos los de AGETIC, con el fin de minimizar sesgos de publicación. Si bien este trabajo no constituye estrictamente una revisión sistemática, se aplicaron criterios de inclusión y exclusión: se incorporaron aquellos estudios con aplicación en salud o análisis técnicos de blockchain con implicaciones sanitarias, además de revisiones y casos con datos empíricos; se excluyeron opiniones sin evidencia técnica y trabajos no vinculados al sector salud.

- **Análisis conceptual y técnico:** Se desarrolló una revisión de arquitecturas propuestas y un análisis crítico de sus componentes (Layer 1 y Layer 2, IPFS, bases de datos cifradas, modelos de identidad KYC y smart contracts). Para ello se empleó una metodología de ingeniería de software orientada a descomponer las soluciones en capas y describir los flujos de datos, identificando fortalezas y limitaciones de cada propuesta.

- **Sistematización de casos documentados:** Se recopilaron experiencias internacionales de uso de blockchain en salud con documentación técnica suficiente (arquitectura, métricas y lecciones aprendidas), priorizando la diversidad geográfica en Europa y América Latina, como las analizadas por Riveros Lancheros et al., (2019). El objetivo fue identificar buenas prácticas, errores recurrentes y recomendaciones aplicables a futuros procesos de adopción.

- **Revisión legal:** Se incluyeron cuerpos normativos y documentos de política relevantes en materia de protección de datos y salud Agetic, (2024; Dulce Villarreal et al., (2023). Los criterios de selección contemplaron la jurisdicción aplicable, la vigencia de la norma, su alcance respecto al tratamiento de datos sensibles y su pertinencia para tecnologías descentralizadas.

- **Triangulación interdisciplinaria y validación:** Finalmente, se consideró la incorporación de perspectivas de actores clave (profesionales de la salud, administradores, auditores legales y pacientes) mediante charlas semiestructuradas, con el propósito de contrastar los hallazgos teóricos y técnicos con la realidad operativa y las expectativas regulatorias.

Fundamentos Tecnológicos

Los fundamentos tecnológicos de la implementación de blockchain en la gestión de historias clínicas se articulan sobre un conjunto de componentes que permiten garantizar la seguridad, disponibilidad y descentralización de los datos en salud. A continuación, se detallan los principales elementos tecnológicos y sus funciones dentro de este ecosistema:

- **Blockchain Layer 2**: Estas soluciones permiten ampliar la escalabilidad de la blockchain principal mediante canales paralelos o de segunda capa que procesan transacciones fuera de la cadena principal, reduciendo tiempos de validación y costos operativos. Su implementación resulta esencial para soportar grandes volúmenes de

datos clínicos en tiempo real Esposito et al., (2018).

- **IPFS (InterPlanetary File System)**: Se trata de un sistema de archivos distribuido que permite almacenar documentos médicos como radiografías, resonancias, y otros tipos de imágenes, con una estructura inmutable y verificable. Los archivos se referencian mediante hashes criptográficos, asegurando la integridad y disponibilidad de los datos sin depender de un servidor centralizado.

- **Bases de datos cifradas**: Complementan la estructura descentralizada permitiendo que información altamente sensible (como datos personales del paciente), se almacenen de forma cifrada. Este cifrado garantiza la confidencialidad, y el acceso controlado mediante llaves privadas y sistemas de autenticación robustos.

- **Identidad digital con protocolos KYC (Know Your Customer)**: Asegura que cada usuario en el sistema (paciente, médico, administrador) esté correctamente autenticado y vinculado a una identidad digital única, reforzando los mecanismos de trazabilidad y gobernanza del sistema Kuo et al., (2017).

- **Interfaces de usuario (web y móvil)**: Aplicaciones que permiten al paciente y a los profesionales consultar, visualizar y administrar datos clínicos bajo una interfaz amigable y segura, facilitando la interacción con el sistema sin requerimientos técnicos avanzados.

- **Contratos inteligentes (Smart Contracts)**: Programas autoejecutables alojados en la blockchain que permiten automatizar procesos como el otorgamiento de permisos de acceso, la validación de recetas, o la verificación de identidad entre instituciones. Estos contratos actúan como intermediarios digitales incorruptibles, asegurando el cumplimiento de reglas preestablecidas sin intervención humana.

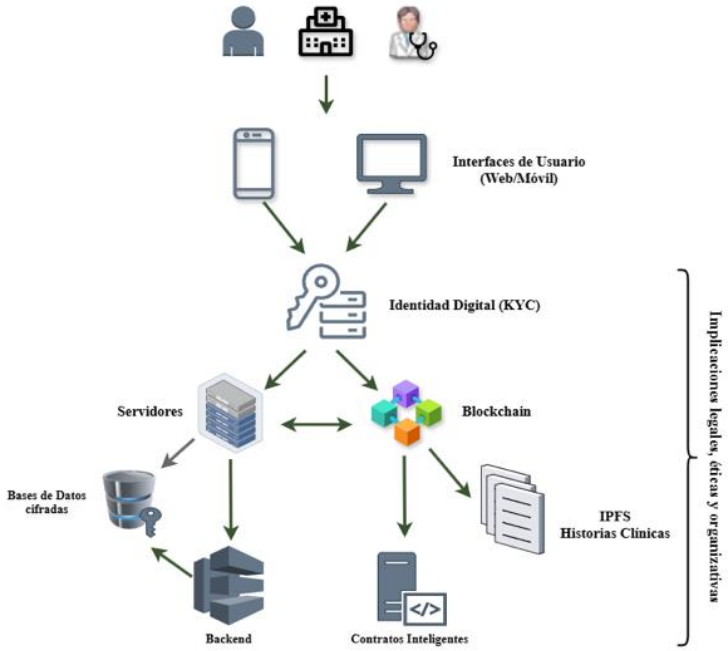

Figura 1. *Arquitectura tecnológica*

Resultados

- **Identificación clara de beneficios de Blockchain en la gestión de historias clínicas:** El documento evidencia que Blockchain puede resolver problemáticas persistentes como la fragmentación de la información médica, la falta de interoperabilidad entre instituciones y la limitada participación del paciente. Entre los beneficios más destacados están la trazabilidad, inmutabilidad de los registros, descentralización del control de datos y fortalecimiento de la privacidad.

- **Marco conceptual sólido para la aplicación de Blockchain en salud:** El trabajo proporciona un marco conceptual que describe los componentes tecnológicos clave (Blockchain, IPFS, contratos inteligentes e identidad digital) y cómo estos se integran en un sistema clínico. Este resultado es valioso como referencia para futuras investigaciones, ya que sintetiza la información técnica y legal en un esquema coherente que puede servir como base para modelos funcionales o simulaciones.

- **Análisis detallado de componentes técnicos aplicables al entorno clínico:** El estudio describe con precisión los elementos técnicos que harían viable un sistema descentralizado de historias clínicas: IPFS para almacenamiento seguro, contratos inteligentes para automatización de reglas, bases cifradas para protección de datos sensibles, e identidad digital con KYC para autenticación confiable.

- **Sistematización de experiencias internacionales y casos piloto:** El artículo recopila y analiza diversos casos documentados de implementación de Blockchain en salud, tanto en Europa como América Latina. Esta revisión permite identificar patrones, buenas prácticas y errores comunes, lo que proporciona una base empírica útil para planificadores, tomadores de decisiones o investigadores que deseen replicar o adaptar estos modelos a sus propios contextos.

- **Fortalecimiento del enfoque interdisciplinario en salud digital:** El documento integra los campos de ingeniería informática, derecho, ética médica y gestión sanitaria, demostrando que el desarrollo de soluciones en salud digital requiere equipos interdisciplinarios. Este enfoque promueve una visión integral donde la tecnología no es un fin en sí mismo, sino una herramienta al servicio de procesos humanos y clínicos.

Discusión

¿Puede Blockchain garantizar plenamente la privacidad de los datos médicos en entornos descentralizados?

La privacidad en Blockchain se basa en mecanismos criptográficos que permiten la inmutabilidad y la verificación sin necesidad de intermediarios. Sin embargo, en el contexto médico, la privacidad va más allá de la integridad de los datos: implica control de acceso, anonimato y confidencialidad. Aunque el almacenamiento descentralizado en IPFS con hashes criptográficos y bases de datos cifradas fortalece la protección, el simple hecho de registrar cualquier información en una cadena inmutable (incluso metadatos) puede representar un riesgo si no se gestiona adecuadamente.

Un desafío clave es la implementación de sistemas de permisos granulares que permitan al paciente decidir quién accede a qué parte de su información, por cuánto tiempo y con qué fines. Además, el uso de identidad digital y autenticación robusta (como el protocolo KYC)

plantea dilemas sobre cómo balancear trazabilidad con anonimato. En este sentido, la privacidad en Blockchain no es automática ni absoluta: depende del diseño cuidadoso de la arquitectura, de políticas de gobernanza y de regulaciones adecuadas.

Viabilidad de la interoperabilidad entre sistemas de salud públicos y privados mediante Blockchain

Uno de los grandes obstáculos de la gestión clínica actual es la fragmentación de los datos entre instituciones. Blockchain puede ofrecer un modelo compartido para registrar información médica que distintos actores (hospitales, aseguradoras, clínicas, farmacias), puedan consultar de forma segura y estandarizada. No obstante, esta interoperabilidad no depende exclusivamente de la tecnología, sino de acuerdos entre actores y de voluntad política.

El desafío reside en integrar la Blockchain con sistemas legados (por ejemplo, historias clínicas almacenadas en software local sin conexión a la red), y en adaptar los formatos a modelos como HL7 FHIR (Fast Healthcare Interoperability Resources - Recursos rápidos de interoperabilidad en el sector sanitario). Además, se deben resolver cuestiones como el control sobre los nodos, la sincronización de datos y la compatibilidad de políticas de acceso. Aun si la infraestructura Blockchain es común, su interoperabilidad solo será real si hay un consenso regulatorio, técnico y operativo.

Desafíos regulatorios y éticos en la implementación de Blockchain en salud

La descentralización que propone Blockchain entra en tensión con marcos regulatorios tradicionales, basados en modelos centralizados de responsabilidad y supervisión. En muchos países, las leyes de protección de datos personales (como el GDPR en Europa o el anteproyecto AGETIC en Bolivia) imponen criterios de localización, control, derecho al olvido y consentimiento explícito, que no siempre encajan con las propiedades de inmutabilidad y replicación de Blockchain.

Además, se abren debates éticos sobre quién decide qué datos se registran, cómo se audita el uso de la tecnología y qué pasa si hay errores o falsificaciones en los registros. La gobernanza ética de un sistema distribuido requiere nuevas figuras normativas: custodios digitales, auditores algorítmicos, o mecanismos de arbitraje que sustituyan al “administrador central” clásico. Por tanto, el marco legal debe evolucionar paralelamente a la tecnología para evitar brechas de responsabilidad.

Implicaciones sociales y culturales del control del paciente sobre su historia clínica

Uno de los mayores aportes de Blockchain es devolver al paciente el control sobre sus datos. Sin embargo, este empoderamiento también supone una carga: administrar claves privadas, entender mecanismos de permisos y asumir decisiones sobre su información médica. En contextos con baja alfabetización digital, este modelo puede generar exclusión o errores involuntarios con consecuencias clínicas graves.

Culturalmente, además, muchos sistemas de salud están estructurados sobre la autoridad del médico o la institución como guardianes de la información. Cambiar hacia una lógica de “autogestión del dato” implica revisar el rol del paciente, el modelo de consentimiento informado, y la corresponsabilidad en el manejo del historial clínico. Este cambio no es solo técnico, sino educativo y cultural.

Impacto económico de adoptar Blockchain en sistemas de salud

Aunque Blockchain promete reducir costos operativos a largo plazo (al eliminar intermediarios y reducir errores), su implementación inicial puede ser costosa y compleja. Requiere inversión en infraestructura, capacitación, rediseño de procesos y adaptación legal. Además, existen dudas sobre si los sistemas actuales de salud pública -muchos de ellos subfinanciados- están en condiciones de asumir esta transición tecnológica.

Un análisis costo-beneficio debe incluir factores indirectos: prevención de fraudes, disminución de repeticiones de exámenes, mejora en el seguimiento de tratamientos, entre otros. Por otro lado, sin una estrategia clara de sostenibilidad, Blockchain puede quedar relegada a pilotos sin impacto real.

Capacidad de escalabilidad y respuesta en tiempo real en contextos de emergencia sanitaria

Durante emergencias como pandemias o desastres naturales, los sistemas de salud requieren agilidad, interoperabilidad y fiabilidad. Blockchain puede ofrecer trazabilidad y control de acceso instantáneo, pero su escalabilidad ha sido históricamente un problema, especialmente en Blockchains públicas. Las soluciones de Layer 2 y cadenas privadas pueden mitigar esto, pero añaden complejidad al diseño.

Se deben prever cuellos de botella, congestión de red y mecanismos de recuperación ante fallos. Un sistema de salud basado en Blockchain solo será útil en emergencias si ha sido diseñado y probado previamente en contextos de alta demanda.

Riesgos técnicos y de gobernanza

La exposición de metadatos, la custodia de claves, los posibles ataques a los contratos inteligentes y la complejidad de las soluciones de segunda capa (L2) representan riesgos latentes en la implantación de blockchain en salud. Para mitigarlos, es necesario definir con precisión qué datos y metadatos deben ser realmente públicos, evitando exponer información sensible de manera innecesaria.

Otro aspecto crítico es la custodia de las claves utilizadas para firmar certificados. Para reducir vulnerabilidades, se recomienda implementar estructuras de multi-firma, en las cuales no solo un par de claves sea responsable de la validación, sino un conjunto de ellas. Esto refuerza el control y disminuye el riesgo de manipulación o pérdida de acceso.

En cuanto a los contratos inteligentes, su despliegue público permite que sean revisados por cualquier persona, lo cual aporta transparencia, pero también aumenta el riesgo de ataques. Por ello, antes de ser implementados deben ser sometidos a auditorías exhaustivas y detalladas, con el objetivo de identificar y corregir posibles vulnerabilidades.

Más allá de los aspectos técnicos, también existen riesgos de gobernanza, regulatorios y socioculturales. La colisión entre el derecho al olvido o la localización de datos frente a la inmutabilidad y replicación puede generar incumplimientos legales. Asimismo, la ausencia de un “administrador central” claro complica la asignación de responsabilidades, mientras que los modelos de identidad y consentimiento pueden entrar en tensión al intentar equilibrar anonimato y trazabilidad.

Conclusiones

El análisis teórico realizado permite inferir que blockchain representa una tecnología con alto potencial para mejorar la gestión de datos médicos en sistemas de salud. Su capacidad para garantizar inmutabilidad, trazabilidad y control de acceso es ampliamente reconocida, especialmente en contextos donde la confianza en los sistemas actuales es baja. No obstante, su adopción requiere considerar aspectos regulatorios, culturales y tecnológicos que condicionan su éxito.

Referencias Bibliográficas

Agetic. (2024, octubre). *Anteproyecto: Ley de Protección de Datos Personales*. https://www.agetic.gob.bo/wp-content/uploads/2024/10/Manual-de-Proteccion-de-Datos-2-firmado.pdf

Albiol-Perarnau, M., & Alarcón Belmonte, I. (2024a). Blockchain en salud: Transformando la seguridad y la gestión de datos clínicos. *Atención Primaria*, *56*(5), 102848. https://doi.org/10.1016/j.aprim.2023.102848

Albiol-Perarnau, M., & Alarcón Belmonte, I. (2024b). Blockchain en salud: Transformando la seguridad y la gestión de datos clínicos. *Atención Primaria*, *56*(5), 102848. https://doi.org/10.1016/j.aprim.2023.102848

Bermúdez Ocampo, J. S., Salazar Marulanda, N. L., & Vélez Rueda, L. (2023). Blockchain y salud: Una herramienta versátil y segura. *Ciencia, Tecnología e Innovación en Salud*, *6*, 52–60. https://doi.org/10.23850/25393871.5617

Domingos, I. M., & Goncalves, R. M. (2023a). Gobernanza Blockchain: Tecnología disruptiva para el control de la corrupción en la salud públicaa (Blockchain governance: disruptive technology for controlling corruption in public health). *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4592779

Domingos, I. M., & Goncalves, R. M. (2023b). Gobernanza Blockchain: Tecnología disruptiva para el control de la corrupción en la salud públicaa (Blockchain governance: disruptive technology for controlling corruption in public health). *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4592779

Dulce Villarreal, E. R., Betancourt Romo, J. H., Solarte Solarte, F. N. J., & Rosero Galíndez, C. M. (2023). BLOCKCHAIN: UNA MIRADA DESDE LA PROTECCIÓN DE DATOS SENSIBLES EN EL SECTOR SALUD. REVISTA COLOMBIANA DE TECNOLOGIAS DE AVANZADA (RCTA), 2(38), 69–78. https://doi.org/10.24054/rcta.v2i38.1279

Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K.-K. R. (2018a). Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Computing*, *5*(1), 31–37. https://doi.org/10.1109/MCC.2018.011791712

Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K.-K. R. (2018b). Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Computing*, *5*(1), 31–37. https://doi.org/10.1109/MCC.2018.011791712

Galván Torres, D. R. (2021). *Prototipo de una aplicación descentralizada de apoyo a los procedimientos de gestión de inventarios de la Universidad Distrital usando Blockchain e IPFS*. http://hdl.handle.net/11349/29176 La - Spanish

Kuo, T.-T., Kim, H.-E., & Ohno-Machado, L. (2017). Blockchain distributed ledger

technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, *24*(6), 1211–1220. https://doi.org/10.1093/jamia/ocx068

Riveros Lancheros, D. F., Martínez Zarama, G., González Arteta, J. D., & Cabrera Venegas, N. E. (2019a). *Diseño e implementación de tecnologías Blockchain para el sector salud en Colombia* [Universidad de los Andes]. https://hdl.handle.net/1992/45108

Riveros Lancheros, D. F., Martínez Zarama, G., González Arteta, J. D., & Cabrera Venegas, N. E. (2019b). *Diseño e implementación de tecnologías Blockchain para el sector salud en Colombia* [Universidad de los Andes]. http://hdl.handle.net/1992/45108

Vazirani, A. A., O'Donoghue, O., Brindley, D., & Meinert, E. (2019a). Implementing Blockchains for Efficient Health Care: Systematic Review. *Journal of Medical Internet Research*, *21*(2), e12439. https://doi.org/10.2196/12439

Vazirani, A. A., O'Donoghue, O., Brindley, D., & Meinert, E. (2019b). Implementing Blockchains for Efficient Health Care: Systematic Review. *Journal of Medical Internet Research*, *21*(2), e12439. https://doi.org/10.2196/12439

ESTEGANOGRAFÍA DE ARCHIVOS DE AUDIO WAV: INSERCIÓN DE EJECUTABLES Y ANÁLISIS DE EVASIÓN ANTIVIRUS

WAV AUDIO FILE STEGANOGRAPHY: EXECUTABLE EMBEDDING AND ANTIVIRUS EVASION ANALYSIS

Jhamil Arturo Zeballos Soruco
Universidad San Francisco Xavier
zeballos.jhamil@usfx.bo

Recibido: 28 Abril 2025 / Revisado: 4 Agosto 2025 / Aceptado: 22 Agosto 2025 / Publicado: 23 Septiembre 2025

Resumen

La esteganografía digital consiste en ocultar información dentro de archivos multimedia con el propósito de que su presencia pase desapercibida. El presente estudio analiza la viabilidad de ocultar archivos ejecutables (.exe, .bat, .dll) en archivos de audio en formato WAV mediante la herramienta Steghide. Se empleó un diseño experimental para evaluar la capacidad de incrustación, la reproducción del archivo modificado y su detección por antivirus convencionales y la plataforma VirusTotal. Los resultados evidencian que es posible incrustar archivos ejecutables sin alterar la calidad perceptible del audio y sin que los sistemas de detección los identifiquen como maliciosos. Este hallazgo subraya un riesgo real en la propagación de malware a través de medios aparentemente inocuos, resaltando la necesidad de reforzar los sistemas de seguridad informática con técnicas de detección más avanzadas.

Palabras clave: Esteganografía, Antivirus, steghide, archivos de audio, archivos ocultos

Introducción

La esteganografía es una técnica utilizada desde la antigüedad entendiendo de que ella data de hace siglos atrás y fue utilizada como una *técnica de ocultar información sensible o privada dentro de algo que parezca que todo es normal* (Zone H, 2024). En el contexto digital, este concepto se ha expandido hacia el uso de imágenes, videos y archivos de audio como portadores o anfitriones de información secreta para ocultar información dentro de un medio que aparenta ser inocuo. A diferencia de la criptografía, cuyo propósito es proteger el contenido frente a la intercepción, la esteganografía busca evitar que la existencia del mensaje sea detectada (Sánchez, 2023).

En los últimos años, la esteganografía digital ha sido utilizada no solo con fines legítimos, sino también en ciberataques. Este fenómeno ha dado lugar al concepto de stegomalware: software malicioso que utiliza técnicas esteganográficas para insertarse en archivos multimedia y evadir mecanismos de seguridad (Badar, 2025). Casos documentados, como Waterbug, han mostrado cómo audios WAV han sido empleados para propagar malware sin ser detectados por antivirus tradicionales (Dittmann, 2024).

Este estudio tiene como objetivo evaluar la viabilidad de ocultar ejecutables en archivos de audio WAV utilizando la herramienta Steghide, analizar los resultados obtenidos y discutir sus implicaciones en el ámbito de la seguridad informática. La relevancia académica de este trabajo radica en exponer una vulnerabilidad frecuentemente ignorada, así como en destacar la necesidad de desarrollar herramientas de detección más sofisticadas.

Estado del arte

La literatura especializada describe múltiples técnicas de esteganografía de audio. El método más común es el de sustitución del bit menos significativo (LSB), que altera de forma imperceptible el último bit de cada muestra para incrustar información (Gupta, 2012). Otros métodos incluyen la codificación de fase, el eco-hiding y transformaciones en el dominio de frecuencia como DWT-SVD, que ofrecen mayor robustez frente a compresión y ruido (Yang, 2024).

Investigaciones recientes han explorado la combinación de esteganografía con criptografía caótica, lo que incrementa la capacidad de ocultación y la resistencia frente a técnicas de detección (Nasr, 2024). Paralelamente, la comunidad forense ha reportado el uso de archivos WAV como vehículos de malware en campañas APT, confirmando el carácter práctico de esta amenaza (Strachanski, 2024). Sin embargo, la detección de estos métodos sigue siendo limitada. Modelos de aprendizaje profundo y redes neuronales multiescalares han mostrado avances en estegoanálisis, aunque aún no alcanzan una tasa de detección suficiente en escenarios reales (Peng, 2025).

Este estado del arte muestra un panorama en el que coexisten técnicas simples y accesibles como Steghide con desarrollos avanzados en ocultación y detección. El presente estudio se centra en la primera categoría para evidenciar que incluso con métodos básicos es posible comprometer la seguridad informática.

Métodos

El diseño de la investigación es experimental-descriptivo, con el propósito de demostrar la viabilidad de ocultar ejecutables en archivos WAV. Se utilizaron los siguientes instrumentos: Steghide v0.5.1 como software esteganográfico, Windows 10/11 como sistema operativo anfitrión y VirusTotal como plataforma de validación antivirus.

El procedimiento incluyó: (1) selección de archivos WAV originales, (2) inserción de ejecutables (.bat, .exe, .dll) en los audios utilizando la herramienta de incrustación steghide, (3) verificación de la reproducción y tamaño resultante, (4) análisis del archivo esteganográfico en antivirus locales y en VirusTotal, y (5) registro de métricas como variación de tamaño, tiempo de procesamiento y detección/no detección de anomalías.

Experimentación y resultados

Los experimentos mostraron que la inserción de archivos ejecutables en audios WAV fue exitosa en múltiples casos, sin alterar la calidad percibida del audio ni generar alertas en antivirus. A continuación, se presentan los resultados acompañados de capturas representativas de cada caso. A continuación, se exponen por casos, las incrustaciones de archivos diferenciados por casos.

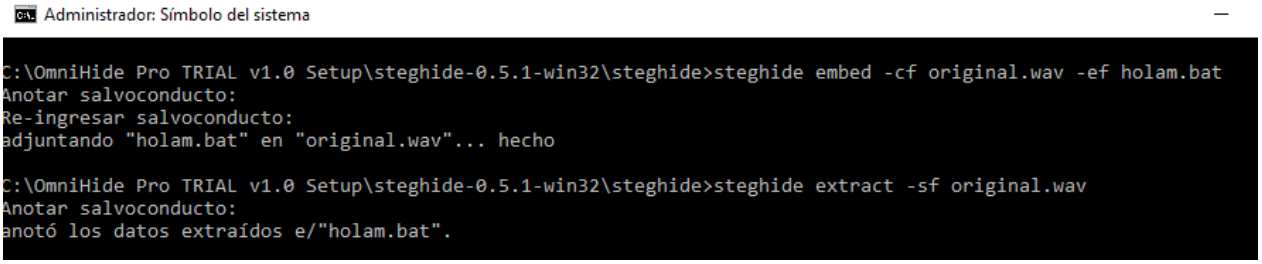

Figura 1: *Captura de Incrustación de archivo .bat y su posterior extracción*

Caso 1: Incrustación archivo bat.

La Figura 1 muestra la ejecución de comandos de Steghide en Windows desde la consola de comandos (cmd), y corresponde a una prueba de incrustación y extracción de un archivo .bat dentro de un archivo de audio .wav. El proceso seguido es el siguiente:

1. Incrustación (primera parte de la ejecución en el cmd): ***steghide embed -cf original.wav -ef holam.bat***

Donde:

- ***-cf original.wav:*** especifica el archivo anfitrión (carrier file), en este caso un audio WAV.
- **-ef holam.bat**: archivo a ocultar dentro del WAV.
- La herramienta solicita la clave (salvoconducto) que sirve como clave de acceso para recuperar posteriormente el archivo (un posible atacante conocerá dicha clave)
- **Resultado:** el archivo holam.bat fue incrustado exitosamente en **original.wav.**

2. Extracción (segunda parte de la ejecución en el cmd): **steghide extract -sf original.wav**

- **-sf original.wav**: indica el archivo donde se ha aplicado esteganografía desde el cual se quiere extraer el contenido oculto.

- El sistema solicita la clave usada en la incrustación.
- **Resultado: Steghide extrajo correctamente el archivo oculto y lo guardó como holam.bat.**

Se evidencia que el procedimiento ejecutado para ocultar y recuperar un archivo ejecutable tipo **(.bat)** en un archivo WAV funciona de manera exitosa con Steghide y se advierten los siguientes resultados iniciales:

- El archivo de audio mantiene una apariencia "normal".
- El archivo oculto se puede recuperar íntegramente con la clave.
- Esto demuestra la factibilidad práctica de la técnica y su potencial uso con fines maliciosos.

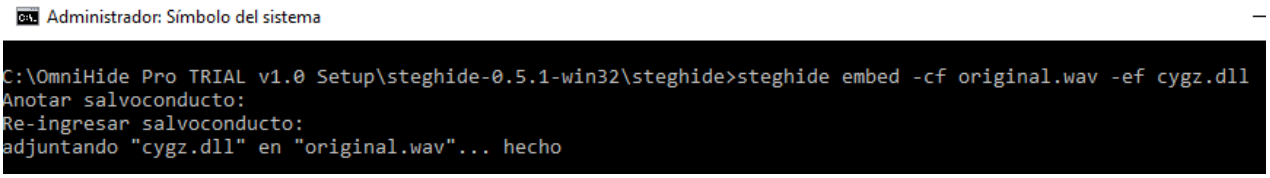

Figura 2: *Captura de Incrustación archivo dll*

Caso 2: Incrustación archivo dll.

La Figura 2 muestra el mismo procedimiento que en la Figura 1, en este caso aplicado a una prueba de incrustación de un archivo .dll dentro de un archivo de audio .wav. con el siguiente proceso:

Incrustación: **steghide embed -cf original.wav -ef cygz.dll**

Donde:

- **-cf original.wav:** archivo anfitrión (un audio en formato WAV).
- **-ef cygz.dll:** archivo a ocultar, en este caso una librería dinámica de Windows (cygz.dll).
- La herramienta solicita la Clave (salvoconducto):
- **Resultado:** El mensaje final indica: adjuntando "cygz.dll" en "original.wav"... hecho. Esto significa que la incrustación del archivo DLL en el WAV se realizó de forma exitosa.

La figura 2 demuestra que, no solo archivos .bat pueden ser ocultados, sino también bibliotecas dinámicas (.dll). Esto amplía la superficie de ataque, ya que una DLL maliciosa podría ser incrustada y distribuida bajo la apariencia de un archivo de audio legítimo.

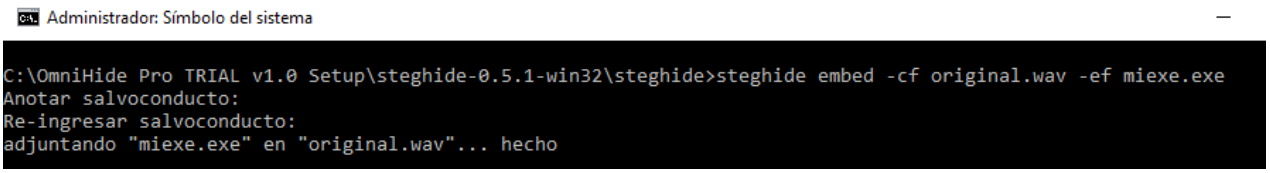

Figura 3: *Captura de Incrustación archivo exe*

Caso 3: Incrustación archivo exe.

Con el mismo procedimiento aplicado en los anteriores casos, la figura 3, muestra la incrustación de un archivo ejecutable .EXE. El proceso es el siguiente:

Incrustación: steghide embed -cf original.wav -ef miexe.exe

Donde:

- **-cf original.wav:** define el archivo portador (archivo de audio en formato WAV).
- **-ef miexe.exe:** indica el archivo a ocultar, en este caso un ejecutable de Windows (miexe.exe, generado desde un compilador).
- La herramienta solicita la Clave (salvoconducto):
- **Resultado:** El mensaje final indica: adjuntando "miex.exe" en "original.wav"... hecho Confirma que el archivo ejecutable fue insertado correctamente en el archivo WAV.

La figura 3 demuestra que Steghide también puede ocultar archivos ejecutables completos (.exe) dentro de un archivo WAV sin alterar su apariencia.

Esto implica un riesgo mayor, ya que los ejecutables pueden ejecutar código malicioso directamente en el sistema al ser recuperados, convirtiendo a un simple archivo de audio en un posible vector de ataque.

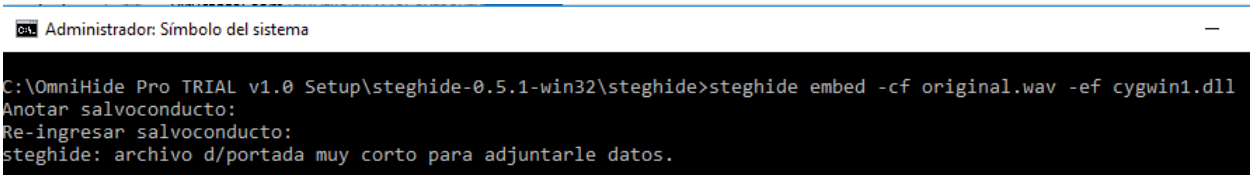

Figura 4: *Captura de Incrustación no exitosa por tamaño*

Caso 4: Incrustación archivo dll fallida.

Para el caso de la Figura 4, la incrustación no es exitosa, debido a que el archivo anfitrión es de 4.18Mb de tamaño, mientras que el dll incrustado de 5.01Mb. En otras pruebas realizadas se ha podido verificar que, para el tamaño del anfitrión, se destina entre 10 y 12% del tamaño del archivo original para poder embeberlo, tamaños mayores no pueden ser incrustados dando resultados fallidos en el experimento. El proceso seguido es el siguiente:

Incrustación: **steghide embed -cf original.wav -ef cygwin1.dll**

Donde:

- **-cf original.wav:** archivo portador (un archivo de audio WAV).
- **-ef cygwin1.dll:** archivo a ocultar, en este caso una librería dinámica de gran tamaño (cygwin1.dll).
- La herramienta solicita la Clave (salvoconducto), pero al continuar el proceso aparece un error: **steghide: archivo d/portada muy corto para adjuntarle datos.**
- **Resultado:** El tamaño del archivo portador (original.wav) no es suficiente para contener el archivo DLL, por lo que la incrustación falló.

La figura 4 demuestra una limitación técnica de Steghide y del método de esteganografía empleado:

- El archivo portador debe tener una capacidad mínima proporcional al tamaño del archivo a ocultar.
- En los experimentos previos se determinó que el límite ronda entre un 10% y 12% del tamaño del archivo anfitrión.
- En este caso, al ser el archivo DLL demasiado grande en relación con el WAV, la incrustación no fue posible.

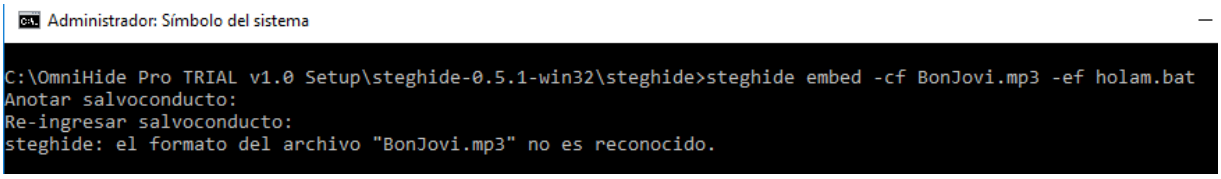

Figura 5: *Captura de Prueba no exitosa con mp3*

Caso 5: Incrustación fallida en archivo mp3.

La figura 5, muestra otro caso de incrustación no exitosa, en este caso se usa un archivo MP3 como anfitrión.El proceso utilizado es el siguiente:

Incrustación: steghide embed -cf BonJovi.mp3 -ef holam.bat

Donde:

- -cf BonJovi.mp3: archivo portador, en este caso un audio comprimido en formato MP3.
- -ef holam.bat: archivo a ocultar, un ejecutable por lotes (holam.bat).
- La herramienta solicita ingresar y reingresar la Clave (salvoconducto), pero la ejecución no continúa con éxito.
- **Resultado:** steghide: el formato del archivo "BonJovi.mp3" no es reconocido.

Esto significa que Steghide no admite el formato MP3 como archivo anfitrión, ya que estos

archivos están comprimidos con pérdida y no conservan el espacio necesario para ocultar datos.

se ha podido validar que dado que estos archivos ya se encuentran comprimidos no guardan espacio para incrustaciones.

Validaciones de tamaño

Por otra parte, se ha realizado la captura de las propiedades del archivo **original.wav** antes de ser sometido a la incrustación del archivo a ocultar dando como resultado la Figura 6:

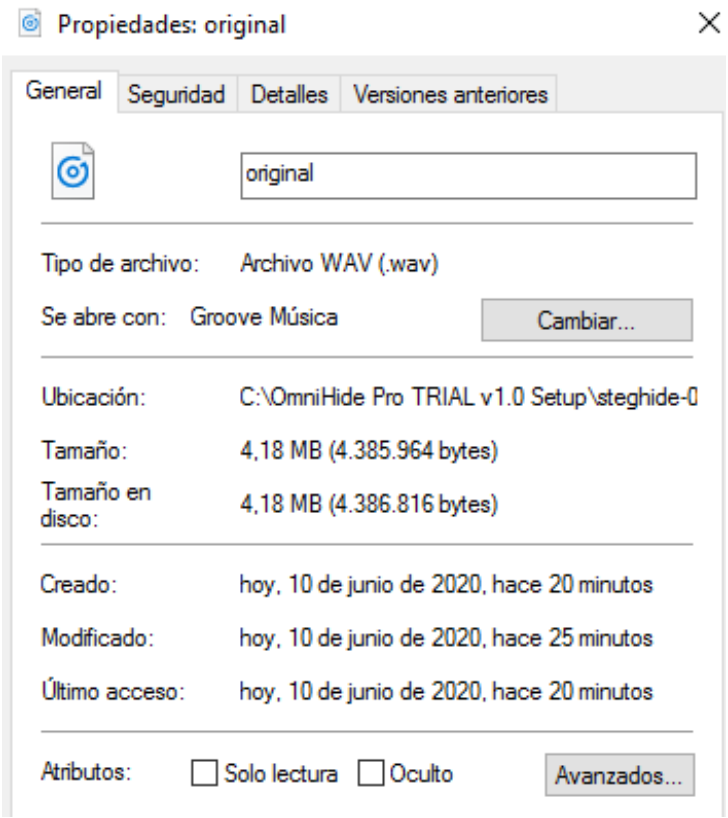

Figura 6: *Propiedades archivo original.wav*

La Figura 6 muestra las propiedades del archivo original.wav antes de realizar la incrustación de archivos ejecutables. Se puede observar su tamaño y metadatos básicos, los cuales sirven como referencia para comparar con el archivo resultante después de la esteganografía.

El análisis experimental indicó que, aun tras insertar archivos .bat, .exe y .dll, el tamaño del archivo WAV no presenta variaciones visibles. Esto refuerza la peligrosidad de la técnica, ya que a simple vista (e incluso mediante verificaciones superficiales) no se detectan cambios, dificultando la identificación del archivo como sospechoso.

Tabla 1: *Métricas básicas de inserción y aplicación antivirus*

Archivo WAV	Tamaño original (MB)	Archivo oculto	Tamaño modificado (MB)	Resultado antivirus
original.wav	4.18	bat (0.2 MB)	4.18	No detectado
original.wav	4.18	exe (0.3 MB)	4.18	No detectado
original.wav	4.18	dll (0.05 MB)	4.18	No detectado
original.wav	4.18	dll (5.01 MB)	—	Incrustación fallida
bonjovi.mp3	4.92	bat (0.2 MB)	—	Incrustación fallida

Análisis en Virustotal

La Figura 8, corresponde al resultado de someter el archivo WAV esteganografiado a la plataforma VirusTotal en el sitio virustotal.com (virustotal, 2025) que integra múltiples motores antivirus (59 en este experimento). El análisis mostró que ninguno de los motores detectó anomalías o malware en el archivo, a pesar de que contenía ejecutables ocultos.

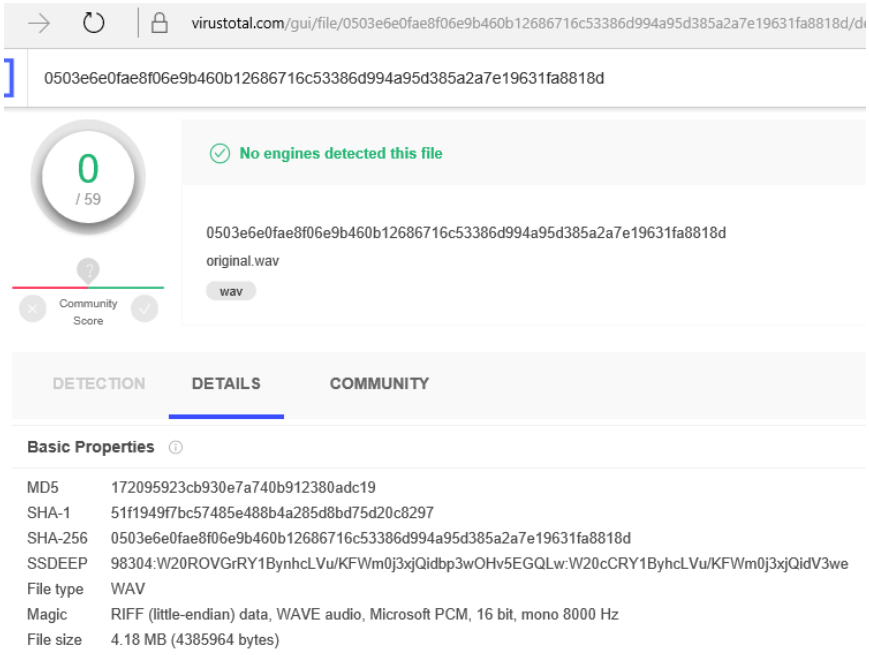

Figura 7: *Análisis archivo modificado*

Este resultado confirma lo planteado por Kaspersky (Kuksov, 2019): la esteganografía es una de las técnicas más difíciles de detectar mediante firmas antivirus tradicionales. El hallazgo enfatiza la necesidad de adoptar técnicas de detección basadas en comportamiento y de fomentar mayor investigación en estegoanálisis aplicado a audio. Llama la atención, que un ejercicio tan simple como la incrustación de archivos de ejecución en entornos Windows como exe, bat o dll puedan ser utilizados tan fácilmente como instrumentos de ataque o de ejecución de instrucciones en los equipos de los usuarios y que estos pasen inadvertidos por los antivirus.

Discusión

Los resultados evidencian que incluso con una herramienta básica como Steghide es posible ocultar ejecutables en archivos WAV y evadir la detección antivirus. Este hallazgo coincide con investigaciones que señalan la dificultad de detectar stegomalware mediante firmas convencionales (Badar, 2025; Strachanski, 2024). Sin embargo, se observaron limitaciones: la capacidad de inserción depende del tamaño del archivo anfitrión y el método no funciona en archivos comprimidos como MP3.

Comparado con técnicas modernas como DWT-SVD o codificación caótica, el enfoque de Steghide es menos robusto, pero su simplicidad representa un riesgo, pues facilita que atacantes con pocos recursos lo utilicen. En este sentido, las implicaciones prácticas son relevantes: archivos de audio, ampliamente compartidos, pueden convertirse en vectores de propagación de malware.

Conclusiones

- Es técnicamente viable ocultar ejecutables en archivos WAV mediante Steghide, manteniendo la reproducción normal y sin ser detectados por los antivirus tradicionales.
- La capacidad de inserción está limitada al tamaño del archivo anfitrión, estimada entre un 10% y 12% de su tamaño total.
- Archivos comprimidos como MP3 no permiten incrustaciones bajo este método.
- Los hallazgos demuestran la necesidad de desarrollar sistemas de detección más sofisticados, basados en análisis de comportamiento o técnicas de inteligencia artificial.
- Se recomienda ampliar las investigaciones hacia formatos comprimidos, plataformas diferentes a Windows y métodos avanzados de estegoanálisis.
- Se recomienda ampliar las investigaciones hacia formas de aprovechamiento de este tipo de vulnerabilidades por parte de los atacantes.

Referencias

Badar, L. T. (2025). A comprehensive survey on stegomalware detection in digital media. Signal Processing.

Dittmann, J. (2024). Forensic trace analysis for MP3-based stego-malware. ACM Transactions on Multimedia Forensics.

Gupta, S. G. (2012). nformation hiding using least significant bit steganography and cryptography. I.J. Modern Education and Computer Science, 27-34, Vol1, Num. 6.

Hetzl, S. (24 de Diciembre de 2003). http://steghide.sourceforge.net/. Recuperado el 10 de Junio de 2025, de http://steghide.sourceforge.net/

Kuksov, I. (4 de Julio de 2019). kaspersky.es. Recuperado el 10 de Junio de 2025, de https://www.kaspersky.es/blog/digital-steganography/18791/

Nasr, M. A.-S.-R.-S.-F.-S. (2024). Robust audio steganography using chaotic maps. Scientific Reports.

Peng, J. (2025). Audio steganalysis using multi-scale feature fusion-based CNN. IET Signal Processing.

Sánchez, A. (26 de 6 de 2023). Proteger mi PC. (Proteger mi PC) Recuperado el 9 de 6 de 2025, de https://protegermipc.net/2018/06/26/introduccion-a-la-esteganografia/

Shailender Gupta, A. G. (2012). Information Hiding Using Least Significant Bit Steganography and Cryptography. I.J.Modern Education and Computer Science, 1(6), 27-34.

Strachanski, F. (2024). A comprehensive pattern-based overview of stegomalware. ACM Computing Surveys.

twoeggz. (29 de Noviembre de 2017). twoeggz. Recuperado el 10 de Junio de 2025, de https://www.twoeggz.com/int/5265059.html

virustotal. (4 de abril de 2025). Recuperado el 10 de Junio de 2025, de virustotal: https://www.virustotal.com/

Yang, G. (2024). An improved phase coding audio steganography algorithm. arXiv preprint.

Zone H. (9 de Junio de 2024). zone-h.org. Obtenido de http://zone-h.org: http://www.infosecwriters.com/text_resources/pdf/Steganography_AMangarae.pdf

ANÁLISIS DE LOS MODELOS NEURONALES PARA EL DISEÑO DE UN SISTEMA DE INTERFERENCIA DE LAS ONDAS ELECTROMAGNÉTICAS NO IONIZANTES EN LA TRANSMISIÓN SINÁPTICA NEURONAL

ANALYSIS OF NEURAL MODELS FOR THE DESIGN OF A SYSTEM FOR INTERFERING WITH NON-IONIZING ELECTROMAGNETIC WAVES IN NEURONAL SYNAPTIC TRANSMISSION

Cristina Vilardell Balasch
Universidad San Francisco Xavier
vilardell.cristina@usfx.bo
https://orcid.org/0000-0002-3136-2130

Recibido: 30 Abril 2025 / Revisado: 3 Agosto 2025 / Aceptado: 19 Agosto 2025 / Publicado: 23 Septiembre 2025

Resumen

La necesidad de comunicación de los seres humanos ha conllevado al uso masivo de tecnologías inalámbricas como redes celulares y WiFi, generando preocupaciones respecto a los efectos de las ondas electromagnéticas no ionizantes (OENI) en la salud humana. Esta investigación propone un modelo neuronal que permita simular la interferencia de estas ondas sobre el proceso de sinapsis neuronal, particularmente sobre el potencial de acción. Se realiza un estudio comparativo de diversos modelos neuronales utilizando análisis documental y el método Delphi. Como resultado, se determinó que el modelo de Hodgkin-Huxley es el más adecuado, al representar con precisión la respuesta bioeléctrica de la neurona frente a estímulos electromagnéticos.

Palabras clave: Tecnologías inalámbricas, radiación no ionizante, salud humana, sinapsis neuronal, modelos neuronales, método Delphi

Introducción

El crecimiento exponencial de las tecnologías inalámbricas ha impulsado investigaciones acerca de sus posibles efectos en el organismo humano. Diversos estudios han mostrado resultados contradictorios respecto a los efectos térmicos y no térmicos de la radiación emitida por dispositivos como celulares y routers WiFi. La comunidad científica y organismos internacionales como la OMS reconocen la necesidad de investigaciones profundas y modelado teórico que permitan entender los mecanismos de interacción entre la radiación y los sistemas biológicos, especialmente a nivel neuronal (Organización Mundial de la Salud [OMS], 2022).

Metodología

Esta investigación utilizó una metodología mixta con predominancia cualitativa, dado que combina análisis documental y método Delphi, ambos de naturaleza cualitativa, complementados con análisis cuantitativo de datos para la validación y ponderación de resultados.

En la primera fase, se realizó un análisis documental de modelos neuronales relevantes Hodgkin-Huxley, FitzHugh-Nagumo y McCulloch & Pitts— a partir de fuentes primarias y revisiones académicas, evaluando criterios como estabilidad, representación eléctrica y formulación matemática. En la segunda fase, se aplicó el método Delphi con 10 expertos en neurociencia que cumplían los siguientes criterios de inclusión:

- Grado académico mínimo de maestría en neurociencia, bioingeniería o áreas afines.
- Experiencia profesional mínima de 10 años en investigación o docencia universitaria sobre actividad neuronal.
- Disponibilidad para responder a dos rondas de cuestionarios en un plazo establecido y disposición para ajustar sus respuestas según la retroalimentación recibida.

El procedimiento incluyó dos rondas Delphi con un intervalo de 10 días entre cada una. En la primera ronda se presentó un cuestionario estructurado con preguntas cerradas (escala Likert de 1 a 5) y abiertas, solicitando la valoración de cada modelo neuronal para simular la interferencia de OENI en la transmisión sináptica. Se garantizó anonimato, iteración y retroalimentación controlada entre rondas, conforme a las directrices metodológicas descritas (Keeney et al., 2011; Hsu & Sandford, 2007).

El nivel de consenso se fijó en un ≥ 80% de concordancia entre participantes (Diamond et al., 2014; Jünger et al., 2017). En caso de no alcanzar este umbral en la primera ronda, se devolvieron a los expertos resúmenes estadísticos y comentarios agregados para reconsideración en la segunda ronda.

Resultados

El análisis documental permitió establecer una matriz comparativa que identificó las ventajas del modelo de Hodgkin-Huxley como el más completo desde el punto de vista biofísico y analítico. Los resultados del Delphi confirmaron esta selección, destacando su capacidad para integrarse con modelos de radiación electromagnética.

A continuación, se presenta una tabla comparativa que resume las principales características evaluadas en los modelos neuronales analizados, destacando la ventaja del modelo de Hodgkin-Huxley para simular interferencias electromagnéticas.

Tabla 1. *Tabla comparativa características modelos neuronales*

Modelo	Tipo de Modelo	Representación eléctrica	Ecuaciones diferenciales	Adecuado para OENI
McCulloch & Pitts	Lógico	No	No	No
FitzHugh-Nagumo	Dinámico simplificado	Parcialmente	Sí	Parcialmente
Hodgkin-Huxley	Biofísico completo	Sí	Sí	Sí

Además, los resultados del método Delphi aplicado a diez expertos en neurociencia se muestran en la siguiente tabla. La puntuación de cada modelo fue de 1 a 5 según su adecuación para simular los efectos de las OENI.

Tabla 2. *Tabla resultados Delphi*

Modelo	Promedio de puntuación Delphi	Nivel de consenso	Comentarios relevantes
McCulloch & Pitts	1.8	Bajo	Modelo simplificado no representa dinámica biofísica.
FitzHugh-Nagumo	3.6	Medio	Aproximación válida pero limitada en precisión.
Hodgkin-Huxley	4.9	Alto	Altamente detallado y adaptable a simulaciones EM.

El análisis documental permitió establecer una matriz comparativa que identificó las ventajas del modelo de Hodgkin-Huxley como el más completo desde el punto de vista biofísico y analítico. Este modelo, formulado con ecuaciones diferenciales no lineales, describe los flujos iónicos a través de la membrana neuronal, permitiendo simular con precisión el potencial de acción (Hodgkin & Huxley, 1952). Se definieron parámetros relevantes para las OENI (frecuencia, potencia, polarización) en relación con la membrana neuronal

Los resultados del Delphi confirmaron esta selección, destacando su capacidad para integrarse con modelos de radiación electromagnética y concluyendo que las frecuencias en el rango de microondas presentan mayor potencial de interacción por resonancia con los ritmos eléctricos neuronales (Foster & Repacholi, 2004).

Discusión

La elección del modelo de Hodgkin-Huxley responde a su base fisiológica demostrada, permitiendo representar el comportamiento eléctrico de la neurona frente a estímulos externos. Su adaptabilidad a circuitos eléctricos permite simular la interferencia de las OENI en ambientes computacionales.

La integración entre el modelo HH y una fuente de campo electromagnético como entrada en la membrana neuronal permite observar variaciones en la generación del potencial de acción, lo cual ha sido teóricamente predicho en otros estudios con modelos similares (Montoya et al., 2003; Gerstner et al., 2014).

Desde una perspectiva biofísica, el modelo HH ofrece una aproximación cuantitativa de las propiedades de conductancia iónica en membranas neuronales, lo que posibilita el acoplamiento con parámetros electromagnéticos como la frecuencia, intensidad y duración de las OENI. Esto proporciona una vía para explorar correlaciones entre exposición crónica y variaciones en la excitabilidad neuronal, hipótesis que han sido sugeridas por estudios experimentales in vitro (López et al., 2014).

Además, diversos autores han resaltado que los efectos de las OENI pueden depender de la modulación de la señal y su proximidad a los ritmos cerebrales (Foster & Repacholi, 2004), lo que hace pertinente utilizar modelos con capacidad para capturar respuestas temporales complejas. En ese sentido, el modelo HH, con su base en ecuaciones diferenciales no lineales, resulta especialmente adecuado para simular la posible sincronización o interferencia con oscilaciones neuronales naturales.

Por otro lado, estudios como los de (Hardell et al.,2009) enfatizan la necesidad de considerar factores individuales y ambientales que podrían amplificar la susceptibilidad a la radiación, sugiriendo que el modelado computacional debe contemplar escenarios variados. Este artículo representa un primer paso en la formulación de modelos teóricos integrados que puedan apoyar estudios clínicos y epidemiológicos en curso.

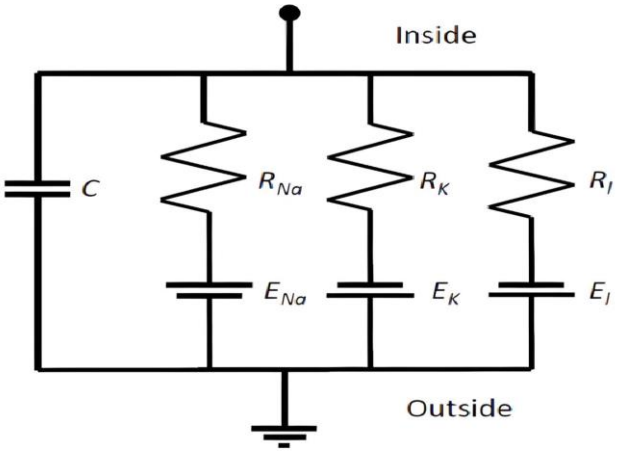

Figura 1. *Representación esquemática del modelo de Hodgkin-Huxley y su equivalente eléctrico.*

Adaptado de Hodgkin, A. L., & Huxley, A. F. (1952). A quantitative description of membrane current and its application to conduction and excitation in nerve. *The Journal of Physiology, 117*(4), 500-544.

Conclusiones

El presente estudio identifica al modelo de Hodgkin-Huxley (HH) como la representación biofísica más adecuada para simular los efectos de las ondas electromagnéticas no ionizantes (OENI) en el proceso de transmisión sináptica neuronal. Su formulación detallada basada en ecuaciones diferenciales no lineales permite modelar con precisión los cambios dinámicos de los potenciales de acción bajo diferentes condiciones de exposición a campos electromagnéticos.

La selección del modelo HH se fundamenta en:

- Su capacidad para reproducir el comportamiento eléctrico real de la membrana neuronal,
- Su adaptabilidad a la integración de parámetros de campos electromagnéticos como frecuencia, potencia y polarización,
- Y su validación a través del método Delphi con alta concordancia entre expertos en neurociencia.

Se destaca que el modelo HH permite no solo simular la generación y propagación del potencial de acción bajo condiciones normales, sino también analizar cómo las OENI podrían alterar estos procesos mediante mecanismos como la modificación de los flujos iónicos y la alteración de la excitabilidad neuronal.

Como línea futura de trabajo, se recomienda:

- Implementar simulaciones computacionales avanzadas mediante plataformas especializadas como **NEURON** o **Genesis**, que permiten la incorporación de fuentes de campos electromagnéticos externas,
- Establecer protocolos experimentales que validen empíricamente los efectos modelados, a través de cultivos neuronales in vitro sometidos a distintas configuraciones de exposición a OENI,
- Explorar la influencia de diferentes parámetros de modulación de la señal, considerando la proximidad de las frecuencias de OENI a los ritmos neuronales endógenos.

Finalmente, el presente modelo ofrece un marco teórico sólido para posteriores investigaciones clínicas y epidemiológicas sobre el impacto neurológico de la exposición prolongada a tecnologías inalámbricas, contribuyendo al diseño de normativas de protección basadas en evidencia científica.

Agradecimientos

Agradezco la colaboración de los expertos participantes del método Delphi y a las instituciones universitarias que facilitaron la difusión del cuestionario.

Referencias Bibliográficas

Foster, K. R., & Repacholi, M. H. (2004). Biological effects of radiofrequency fields: Does modulation matter? Radiation Research, 162(2), 219-225.

FitzHugh, R. (1961). Impulses and physiological states in theoretical models of nerve membrane. *Biophysical Journal, 1*(6), 445-466. https://doi.org/10.1016/s0006-3495(61)86902-6

Gerstner, W., Kistler, W. M., Naud, R., & Paninski, L. (2014). Neuronal Dynamics: From Single Neurons to Networks and Models of Cognition. Cambridge University Press.

Hardell, L., Carlberg, M., & Hansson Mild, K. (2009). Epidemiological evidence for an association between use of wireless phones and tumor diseases. Pathophysiology, 16(2-3), 113-122.

Hodgkin, A. L., & Huxley, A. F. (1952). A quantitative description of membrane current and its application to conduction and excitation in nerve. The Journal of Physiology, 117(4), 500–544.

López, E. P., Saldías, D. P., & Hernández, M. A. (2014). Efectos neurológicos por teléfonos celulares: revisión bibliográfica y modelos matemáticos. Interciencia, 39(12), 843-849.

McCulloch, W. S., & Pitts, W. (1943). A logical calculus of the ideas immanent in nervous activity. *Bulletin of Mathematical Biophysics, 5*(4), 115-133. https://doi.org/10.1007/BF02478259

Montoya, C. B., Calvet, H. C., & Ledesma, A. C. (2003). Análisis y Simulación con INTEGRA del Modelo de FitzHugh-Nagumo para una Neurona. Aportaciones Matemáticas, (32), 31-49.

Nagumo, J., Arimoto, S., & Yoshizawa, S. (1962). An active pulse transmission line simulating nerve axon. *Proceedings of the IRE, 50*(10), 2061-2070. https://doi.org/10.1109/JRPROC.1962.288235

Organización Mundial de la Salud [OMS]. (2022). *Campos electromagnéticos y salud pública: teléfonos móviles*. Recuperado de https://www.who.int/es/news-room/fact-sheets/detail/electromagnetic-fields-and-public-health-mobile-phones

Zavala, R. R. (2013). Posibles efectos provenientes del uso excesivo de la comunicación inalámbrica. Revista Iberoamericana de las Ciencias de la Salud, 2(4), 25-57.

IMPORTANCIA DE LA MATEMÁTICA DISCRETA EN LA IMPLEMENTACIÓN DE ALGORITMOS COMPUTACIONALES

DISCRETE MATHS IMPORTANCE IMPLEMENTED TO COMPUTATIONAL ALGORITHMS

José Enrique Iglesias
Universidad de San Francisco Xavier de Chuquisaca
iglesias.enrique@usfx.bo

Recibido: 4 Mayo 2025 / Revisado: 13 Agosto 2025 / Aceptado: 21 Agosto 2025 / Publicado: 23 Septiembre 2025

Resumen

La Matemática Discreta desempeña un papel importante en el campo de las Ciencias de la Computación y de manera concreta en la implementación de algoritmos computacionales, debido a su capacidad para modelar problemas complejos mediante estructuras lógicas, relaciones finitas y conceptos como la teoría de grafos, conjuntos, lógica proposicional y teoría de números.

El presente artículo se basa en una revisión sistemática de literatura reciente que respalda la importancia de esta disciplina en áreas estratégicas como la inteligencia artificial, la ciberseguridad, las redes de datos y la criptografía. A través del análisis de casos y estudios aplicados, se evidencia que numerosos algoritmos fundamentales, como Dijkstra o Diffie-Hellman, tienen su base en principios discretos, lo cual permite desarrollar soluciones eficientes y robustas en entornos tecnológicos diversos. Asimismo, se explora el rol formativo de la Matemática Discreta en la educación superior, subrayando su contribución al fortalecimiento de habilidades como el pensamiento lógico, la abstracción y la resolución algorítmica. Los resultados de la revisión muestran que existe un grado bajo de inclusión de estos conocimientos en los contextos curriculares de muchas universidades latinoamericanas y nacionales, lo cual representa una debilidad en la formación integral de los futuros profesionales en Ciencias de la Computación.

Palabras clave: Matemática Discreta, Algoritmos, Ciencias de la Computación, Inteligencia Artificial, Criptografía, Currículo

.

Introducción

En la era digital actual, el desarrollo de soluciones computacionales eficientes depende en gran medida del diseño, análisis e implementación de algoritmos computacionales. Estos son de vital importancia porque permiten resolver problemas complejos en diversas áreas tales como la Inteligencia Artificial, Redes de Datos, Ciberseguridad y Procesamiento de la Información, estos algoritmos computacionales tienen una base sólida en los conceptos de la Matemática Discreta, rama de la Matemática que se encarga del estudio de estructuras discretas, tales como grafos, árboles, conjuntos finitos, relaciones, lógicas proposicionales y teoría de números, todos estos conocimientos son fundamentales para la representación, modelación y resolución de problemas computacionales basados en algoritmos.

Bajo este contexto (Aldahdooh, Alshawabkeh, & Al-Smadi, 2023) afirman que "la Matemática Discreta proporciona el lenguaje formal y las herramientas analíticas necesarias que permiten conceptualizar problemas y desarrollar algoritmos eficientes" (p. 148).

Asimismo, la Matemática Discreta implica un conjunto de contenidos tales como la teoría de grafos, la combinatoria y las relaciones de recurrencia que se caracterizan por ser pilares fundamentales para la implementación de algoritmos de búsqueda, optimización, encriptación y aprendizaje automático. En base a (Zhou, Sun, & Li, 2021), existen algoritmos como el de *Dijkstra*, el cual es implementado en los sistemas operativos de los *routers* para calcular las rutas más cortas en protocolos de enrutamiento, también destaca el algoritmo *Diffie-Hellman*, el cual es aplicado en la criptografía moderna para aspectos de seguridad, estos algoritmos muy importantes hoy en día tienen su base sólida en la Matemática Discreta.

Además de su relevancia técnica, la Matemática Discreta cumple una función formativa en la enseñanza de las Ciencias de la Computación, al respecto (Caballero & Solares, 2020) afirman "su inclusión en los planes de estudio permite desarrollar competencias cognitivas como el razonamiento lógico, el pensamiento crítico, la resolución de problemas y la capacidad de abstracción, que son esenciales para enfrentar los desafíos del campo computacional contemporáneo" (p. 138). Sin embargo, a pesar de su importancia, en muchos contextos universitarios de Latinoamérica su presencia en los planes de estudio aún es limitada o superficial, lo cual afecta directamente la preparación profesional de los futuros egresados en áreas tecnológicas.

El presente artículo tiene como propósito mostrar la relevancia e importancia de la Matemática Discreta en relación con las Ciencias de la Computación de manera concreta en la implementación de algoritmos computacionales.

Metodología

Al ser un artículo de revisión, se optó por un enfoque cualitativo, orientado a la identificación y análisis de publicaciones académicas que exploren la relación entre la Matemática Discreta y su importancia en la implementación de algoritmos computacionales.

La búsqueda de literatura se llevó a cabo en cinco bases de datos científicas reconocidas por su cobertura en áreas de ciencias computacionales y educación como ser Scopus, IEEE Xplore, SpringerLink, ScienceDirect y Google Scholar. En cuanto a los aspectos que fueron considerados para la búsqueda de información se abordó temáticas tales como Matemática Discreta, Diseño de Algoritmos, Teoría de Grafos, Ciencias de la Computación, Pensamiento computacional y finalmente Criptografía.

Todos los documentos científicos que fueron seleccionados están enmarcados en los últimos cinco años, esto con el fin de garantizar la actualidad de la información. Por otro lado, la selección de documentos se llevó a cabo en tres etapas, la primera, permitió identificar artículos mediante una búsqueda inicial en base a las temáticas mencionadas. La segunda etapa, permitió eliminar documentos duplicados o similares y finalmente, tras la lectura completa, se seleccionaron los documentos relevantes sobre los cuales se estructura el presente análisis.

Desarrollo

Fundamentos de la Matemática Discreta

La Matemática Discreta se ha consolidado como uno de los pilares fundamentales para el desarrollo de las Ciencias de la Computación, debido a que permite modelar estructuras no continuas basadas en conjuntos finitos, relaciones, funciones, grafos, árboles, álgebra booleana y lógica proposicional. Estas estructuras no sólo permiten representar datos sino también formular algoritmos robustos que posteriormente son utilizados en varias aplicaciones en el diario vivir de las personas.

De acuerdo con (Zhou, Sun, & Li, 2021) “las estructuras discretas permiten representar problemas computacionales mediante grafos, árboles, tablas o matrices, lo cual es esencial para algoritmos de búsqueda, clasificación y optimización” (p. 18).

Además, en entornos computacionales donde los datos no son continuos sino finitos o definidos por relaciones lógicas, la lógica proposicional y los autómatas finitos resultan clave para la validación formal y la verificación de sistemas.

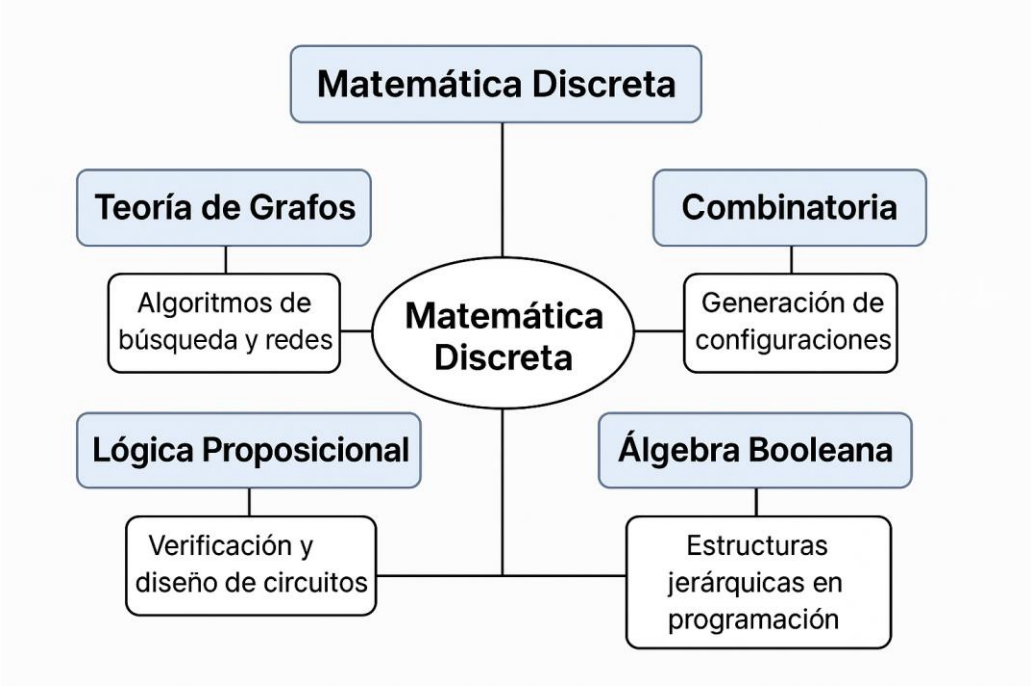

Figura 1: *Relación entre la Matemática Discreta y las Ciencias de la Computación*

Aplicaciones en Algoritmos Computacionales

Los fundamentos de la Matemática Discreta no son simplemente teóricos, su aplicación va más allá y se materializa en la implementación de algoritmos clásicos y modernos utilizados en áreas críticas de la informática.

Por ejemplo, en el área de redes, algoritmos como *Dijkstra* y *Bellman-Ford* se sustentan en la teoría de grafos para determinar caminos óptimos y rutas cortas para el envío de datos, estos son implementados en protocolos de enrutamiento como OSPF y BGP. Según (Wang, Liu, & Tang, 2021), "la aplicación de algoritmos basados en grafos en redes definidas por software ha permitido mejoras sustanciales en la eficiencia del tráfico y la resiliencia de la red de datos" (p. 142).

Por otro lado, en el campo de la ciberseguridad, los algoritmos criptográficos como RSA, *ElGamal* o *Diffie-Hellman* están basados en problemas de teoría de números, como la factorización de enteros o el logaritmo discreto. Al respecto (Kaur & Thakur, 2022), afirman que "la solidez de los algoritmos criptográficos modernos depende directamente de supuestos difíciles de resolver matemáticamente, que emergen justamente de la matemática discreta" (p. 51).

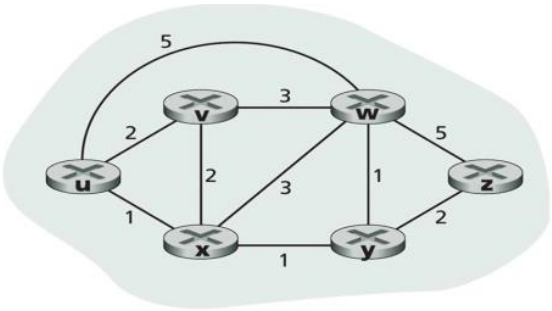

Figura 2. Algoritmo Dijkstra en redes de datos (Luengo, 2020)

Relevancia de la Matemática Discreta en campos tecnológicos emergentes

Los avances en inteligencia artificial, *blockchain* y análisis de redes complejas han reforzado la necesidad de herramientas matemáticas discretas que permitan representar relaciones estructurales y resolver problemas de alto nivel.

Por ejemplo, en la Inteligencia Artificial, las Redes Neuronales basadas en Grafos (GNNs), se han popularizado bastante en los últimos años, como una forma de procesar datos no estructurados. Estas redes se caracterizan por utilizar la teoría de grafos para modelar nodos y relaciones, siendo ampliamente aplicadas en el campo de la bioinformática, en motores de recomendación y análisis de redes sociales.

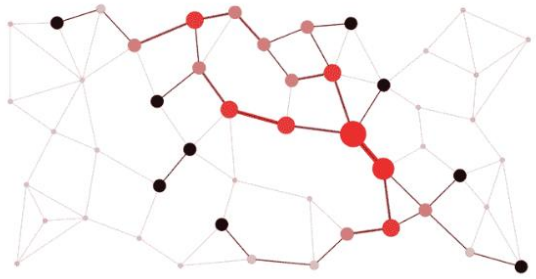

Figura 3. *Red neuronal de grafos (Maldonado, 2021)*

Bajo esta misma línea, en la tecnología *blockchain,* existe una aplicación bastante amplia de los algoritmos de consenso, los árboles de *Merkle* y las funciones hash criptográficas para temas de seguridad, todos estos operan bajo la lógica de algoritmos computacionales fundamentados en la Matemática Discreta.

Matemática Discreta en la formación profesional

Diversos estudios recientes subrayan el impacto positivo de incluir matemática discreta en la

formación de estudiantes del área de Ciencias de la Computación. Esta disciplina no solo desarrolla habilidades técnicas, sino también capacidades cognitivas como el razonamiento lógico, la abstracción y la resolución de problemas complejos.

Al respecto, (Mendoza & Jiménez, 2022) afirman que "la enseñanza de la Matemática Discreta permite mejorar la capacidad de los estudiantes para desarrollar algoritmos computacionales, evaluar estructuras de datos y comprender fundamentos teóricos de sistemas complejos" (p. 35).

No obstante, en base a (Vega, Navarro, & García, 2022), en Latinoamérica la implementación de asignaturas como Matemática Discreta en los procesos formativos es desigual y en algunos casos incluso es nula, esto sin duda alguna conlleva a tener profesionales del área de Ciencias de la Computación con problemas serios en la implementación de soluciones computacionales que tenga esta base discreta.

Resultados

Fruto de la revisión bibliográfica, se identificó que los conceptos fundamentales de la Matemática Discreta como la Teoría de Grafos, la Teoría de números, Lógica Proposicional y la Combinatoria, tienen una aplicación directa en campos claves de las Ciencias de la Computación, especialmente en la implementación de algoritmos de búsqueda y optimización, criptografía, inteligencia artificial, redes neuronales y estructuras de datos complejas. Por ejemplo, la aplicación de la Teoría de Grafos fue ampliamente referenciada, constituyéndose en la base para la implementación de algoritmos de enrutamiento y redes neuronales basadas en grafos, mientras que la Teoría de Números sustentó el diseño de sistemas criptográficos robustos utilizados en blockchain y ciberseguridad.

A continuación, se presenta un resumen de los distintos campos que abarca la Matemática Discreta y su aplicación en las Ciencias de la Computación.

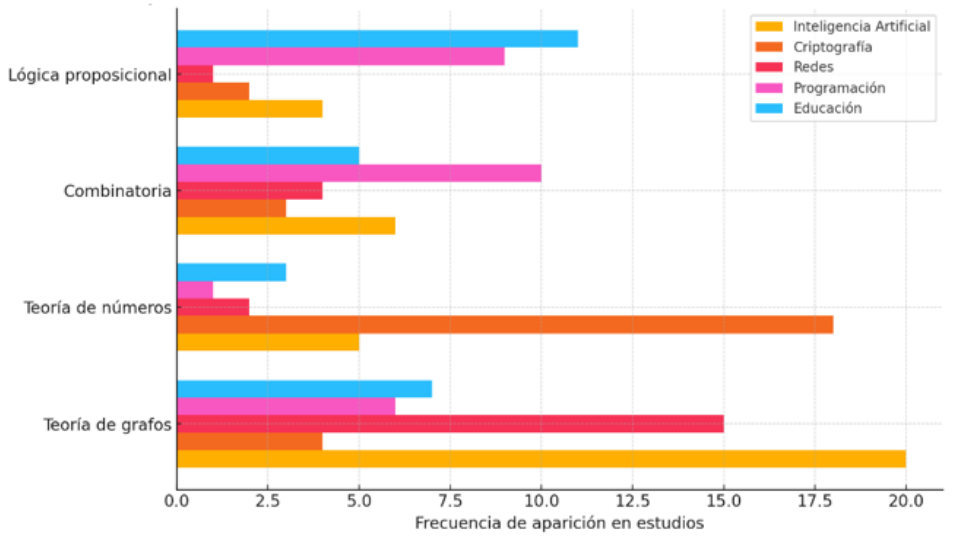

Figura 4: *Aplicación de la Matemática Discreta en campos de la Computación*

Siguiendo esta línea, se evidenció que la inclusión de la Matemática Discreta en la formación profesional mejora significativamente las competencias lógicas, algorítmicas y de pensamiento abstracto de los estudiantes de las áreas de Ciencias de la Computación y ramas afines. Sin embargo, aún persiste una débil integración curricular en muchas universidades latinoamericanas y también nacionales, lo cual limita la preparación técnica en áreas emergentes como la inteligencia artificial y la ciberseguridad. En la Tabla 1, se presenta la inclusión de este campo de conocimientos en el contexto universitario nacional.

Tabla 1. Inclusión de la Matemática Discreta en el contexto universitario nacional

Universidad	Carrera	Contenido Mat. Dis.
Universidad Mayor de San Andrés	Carrera de Informática	Sí
Universidad Mayor de San Simón	Ingeniería Informática	No
Universidad Autónoma Tomás Frías	Ingeniería Informática	Sí
Universidad San Francisco Xavier de Chuquisaca	Ingeniería de Sistemas	No
Universidad San Francisco Xavier de Chuquisaca	Ingeniería en Ciencias de la Computación	No
Universidad Autónoma Juan Misael Saracho	Ingeniería Informática	No
Universidad Autónoma Juan Misael Saracho	Ingeniería de Sistemas	No
Universidad Técnica de Oruro	Ingeniería de Sistemas	No

Discusión

Los resultados obtenidos reflejan una clara consolidación de la importancia de la Matemática Discreta como base teórica indispensable para múltiples áreas de las Ciencias de la Computación. La evidencia revisada muestra que conceptos como la teoría de grafos, los fundamentos de la lógica, la combinatoria y la teoría de números no solo cumplen un rol estructural en el desarrollo de algoritmos, sino que también permiten modelar problemas complejos con alto grado de eficiencia y aplicabilidad. Este fenómeno se observa con especial intensidad en áreas como inteligencia artificial, redes de telecomunicaciones y criptografía, donde la abstracción matemática se traduce en soluciones computacionales prácticas y escalables.

Sin embargo, la revisión documental también pone en evidencia que existe una discrepancia entre la práctica de estos conceptos y su incorporación efectiva en la enseñanza universitaria. Esto genera una brecha formativa que podría limitar la capacidad de los futuros profesionales para abordar los desafíos tecnológicos emergentes, en este sentido, es

necesario replantear los enfoques pedagógicos hacia una enseñanza activa y contextualizada de la Matemática Discreta, vinculándola con problemas reales y proyectos aplicados en el campo de la computación.

Conclusiones

La revisión llevada adelante, confirma que la Matemática Discreta constituye un pilar fundamental en la implementación de algoritmos computacionales, con aplicaciones directas en áreas estratégicas como inteligencia artificial, ciberseguridad, redes de datos y optimización. Conceptos como la teoría de grafos, la teoría de números, la lógica proposicional y la combinatoria no solo sustentan el desarrollo de soluciones tecnológicas, sino que también permiten abordar problemas complejos mediante enfoques eficientes y formales.

Asimismo, se evidencia que la incorporación de la Matemática Discreta en los planes de estudio de carreras afines a Ciencias de la Computación fortalece competencias clave como el pensamiento lógico, la abstracción y la resolución algorítmica de problemas. Sin embargo, persiste una brecha curricular en muchas universidades latinoamericanas, lo cual limita el desarrollo integral de los futuros profesionales. En este sentido, se recomienda fomentar su integración pedagógica mediante enfoques activos, aplicados y contextualizados, que permitan articular la teoría matemática con su impacto real en la tecnología contemporánea.

Referencias bibliográficas

Aldahdooh, A., Alshawabkeh, S., & Al-Smadi, M. (2023). The Impact of Discrete Mathematics on Algorithm Design and Computational Thinking: A Systematic Review. Journal of Computer Science and Technology, 145- 159.

Caballero, R., & Solares, F. (2020). Desarrollo del pensamiento computacional mediante la enseñanza de la matemática discreta en educación superior. *Revista Educación Matemática*, 125 - 143.

Kaur, M., & Thakur, R. (2022). Cryptography and number theory in modern computing. *International Journal of Advanced Computer Science*, 47 - 55.

Luengo D. (2020). *Danilo Luego, Análisis de Algoritmos*. Recuperado el 07 de 04 de 2025, de https://daniloluengo.wordpress.com/unidad-3/algoritmo-dijkstra/

Maldonado, A. (30 de 06 de 2021). *Centro de Innovación Industrial en Inteligencia Artificial*. Recuperado el 30 de 12 de 2024, de https://www.ciiia.mx/noticiasciiia/redes-neuronales-de-grafos-qu-son

Mendoza, O., & Jiménez, A. (2022). La matemática discreta como base en la formación del ingeniero en computación. *Revista Iberoamericana de Tecnologías del Aprendizaje*, 33 - 40.

Vega, R., Navarro, L., & García, A. (2022). Análisis curricular sobre el rol de la matemática discreta en programas de ingeniería informática en América Latina. *Revista de Educación y Tecnología*, 75 - 88.

Wang, H., Liu, Y., & Tang, Y. (2021). Graph algorithms for efficient routing in SDN environments. *Journal of Network and Computer Applications*.

Zhou, M., Sun, X., & Li, Z. (2021). Teoría de grafos y sus aplicaciones en Ciencias de la Computación. *ACM Computing Surveys*, 1 - 38.

Ciencia & tecnología

DIGITAL

Convocatoria 02 - 2025

UNIVERSIDAD MAYOR, REAL Y PONTIFICIA DE SAN FRANCISCO XAVIER DE CHUQUISACA

DIRECCIÓN DE LAS CARRERAS DE INGENIERÍA DE SISTEMAS, INGENIERÍA EN TELECOMUNICACIONES, INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN, INGENIERÍA EN DISEÑO Y ANIMACIÓN DIGITAL E INGENIERÍA EN TECNOLOGÍA DE INFORMACIÓN Y SEGURIDAD

CONVOCATORIA Nº 02/2025

CONVOCATORIA A PRESENTACIÓN DE ARTÍCULOS CIENTÍFICOS

La Dirección de las carreras de **Ingeniería de Sistemas, Ingeniería en Telecomunicaciones, Ingeniería en Ciencias de la Computación, Ingeniería en Diseño y Animación Digital e Ingeniería en Tecnología de Información y Seguridad**, convoca a **académicos, investigadores y estudiantes** a participar en la próxima edición de la **Revista Ciencia y Tecnología Digital**.

Esta iniciativa busca promover la difusión del conocimiento, los avances científicos y tecnológicos, y ofrecer un espacio de visibilidad y debate académico para investigaciones originales y revisiones críticas en estas disciplinas.

1. Tipos de artículos aceptados

Se recibirán:

- ***Artículos científicos originales:*** presentan resultados inéditos con contribución significativa al conocimiento en un área específica.
- ***Artículos de revisión:*** sistematizan, analizan y discuten críticamente literatura científica existente, aportando nuevas perspectivas, tendencias y vacíos de investigación.

Todos los artículos serán sometidos a revisión por pares ciegos para garantizar su validez, relevancia y calidad académica.

2. Participantes

Podrán participar:

Investigadores y docentes de universidades nacionales e internacionales.

3. Estructura del Artículo Científico

Para artículos científicos originales (formato IMRyD):

- Título (máx. 20 palabras, claro y conciso).
- Autor(es), filiación, correo, ORCID
- Resumen (200–220 palabras)
- Palabras clave (3-5 palabras)
- Abstract
- Keywords
- Introducción (antecedentes, problema, relevancia y objetivo)
- Materiales y Métodos
- Resultados (claros, con tablas, gráficos o figuras)
- Discusión (interpretación de resultados, relación con estudios previos, limitaciones y recomendaciones)
- Conclusiones
- Agradecimientos (opcional)
- Referencias (APA 7ª edición)

Para artículos de revisión:

- Título.
- Autor(es) con filiación, correo, ORCID
- Resumen (200–220 palabras)
- Palabras clave (3-5 palabras)
- Abstract
- Keywords
- Introducción (justificación y objetivos)
- Metodología de búsqueda (fuentes, criterios, fechas, palabras clave)
- Desarrollo o Cuerpo de la Revisión
- Conclusiones (hallazgos, vacíos, proyecciones)
- Agradecimientos (opcional)
- Referencias según APA (7ª edición).

4. Líneas de Investigación por Carrera

Las siguientes líneas de investigación se proponen como áreas prioritarias de desarrollo científico y tecnológico. No obstante, la revista acepta trabajos relacionados o afines que contribuyan al avance del conocimiento en campos vinculados.

Ingeniería de Sistemas:

- Desarrollo de software, testing funcional y aseguramiento de la calidad.
- Inteligencia artificial, aprendizaje automático y sistemas inteligentes.
- Sistemas de información, gestión de datos y analítica de negocios.
- Ingeniería de requisitos, arquitectura de software y metodologías ágiles.
- Tecnologías emergentes aplicadas a la transformación digital.
- Modelado y simulación de sistemas.

Ingeniería en Telecomunicaciones:

- Redes y comunicaciones inalámbricas de nueva generación (5G/6G).
- Internet de las cosas (IoT) y aplicaciones en telecomunicaciones.
- Seguridad de redes, comunicaciones seguras y ciberresiliencia.
- Sistemas satelitales, radiofrecuencia y microondas.
- Señales, procesamiento digital y telecomunicaciones ópticas.

Ingeniería en Ciencias de la Computación:

- Computación de alto rendimiento, cloud computing y edge computing.
- Algoritmos, estructuras de datos y optimización computacional.
- Ciberseguridad, privacidad y protección de datos.
- Computación cuántica y aplicaciones emergentes.
- Minería de datos, aprendizaje profundo y visión por computadora.

Ingeniería en Diseño y Animación Digital

- Animación 2D, 3D y motion graphics.
- Realidad aumentada (AR), realidad virtual (VR) y metaverso.
- Diseño interactivo, experiencia de usuario (UX) y usabilidad.
- Arte digital, modelado y escultura digital.
- Producción audiovisual, efectos visuales (VFX) y narrativa transmedia.

- Videojuegos, gamificación y entornos virtuales interactivos.
- Inteligencia artificial aplicada al arte y la animación.
- Cultura digital, comunicación visual y nuevas tecnologías creativas.

Ingeniería en Tecnología de Información y Seguridad:

- Gestión de la seguridad informática, ciberdefensa y continuidad del negocio.
- Sistemas de encriptación, blockchain y tecnologías distribuidas.
- Auditoría, control y gobierno de sistemas de información.
- Forensia digital y gestión de incidentes de ciberseguridad.
- Políticas de seguridad, regulación y normativas internacionales.

5. Normas de Presentación

- Formato: **Documento en Word, con una extensión máxima de 10 páginas tamaño carta.**
- Fuente: Times New Roman 12 pts, con espaciado 1.5 e interlineado de 10 puntos antes y después.
- Márgenes: 3 cm en todos los lados.
- Elementos gráficos: Se podrán incluir tablas, figuras o gráficos, numerados y titulados conforme a las normas APA (7ª edición).
- Redacción: clara, sintética y coherente.

6. Proceso de Revisión

1. **Comisión Editorial:** Evalúa el cumplimiento del formato, la pertinencia temática y decide la admisión del artículo al proceso de revisión.
2. **Comisión Técnica:** Verifica la originalidad y el porcentaje de similitud mediante software especializado.
3. **Revisión por Pares Ciegos:** Evalúa fondo y forma, con una de las siguientes recomendaciones:

    - Aceptación sin modificaciones
    - Aceptación con correcciones menores
    - Aceptación con correcciones mayores
    - Rechazo

El autor será notificado mediante un informe final de evaluación.
La decisión final de publicación corresponde a la Comisión Editorial.

7. Declaraciones del autor

El autor deberá adjuntar la carta de autorización. El formato correspondiente está disponible para descarga en la página web oficial de la revista. El contenido de la carta incluye:

- **Declaración de originalidad:** El artículo es inédito y de autoría propia, y no ha sido postulado simultáneamente en otro medio de publicación.
- **Licenciamiento:** El autor autoriza la difusión, reproducción y almacenamiento digital del artículo en la revista, bajo los términos establecidos por la política editorial.
- **Conflicto de intereses:** El autor declara no tener conflictos de interés y garantiza el anonimato durante el proceso de revisión por pares.
- **Derechos de Autor:** Los artículos se rigen por la Ley N.º 1322 de Derecho de Autor, comprometiéndose el autor a evitar cualquier forma de fraude científico, plagio o autoplagio.

8. Fecha y lugar de recepción

- **Plazo:** Hasta el **31 de octubre de 2025, 16:00 horas**.
- **Presentación:**
    - Digital a la dirección de correo electrónico: revista.ctd@usfx.bo
    - Adjuntar carta de autorización.
    - Los formatos de los documentos solicitados y las plantillas para el desarrollo de los artículos están disponibles en: https://revistas.usfx.bo/index.php/rctd

Ciencia & tecnología
DIGITAL

UNIVERSIDAD MAYOR REAL Y PONTIFICIA DE
SAN FRANCISCO XAVIER
DE CHUQUISACA

2025

sis | INGENIERÍA DE SISTEMAS

tel | INGENIERÍA EN TELECOMUNICACIONES

dad | INGENIERÍA EN DISEÑO Y ANIMACIÓN DIGITAL

cic | INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN

tic | INGENIERÍA EN TECNOLOGÍA DE LA INFORMACIÓN Y SEGURIDAD