



Ciencia & tecnología **DIGITAL**



Volumen 2
Número 1 (2026)

ISSN
Impreso: 3107-1929
Virtual: 3107-1937



UNIVERSIDAD MAYOR REAL Y PONTIFICIA DE
SAN FRANCISCO XAVIER
DE CHUQUISACA



Ciencia & tecnología **DIGITAL**

Publicada por

Dirección de carrera - Ing. Franz Armando Villalpando Amonzabel
Ing. de Sistemas, Ing. en Diseño y Animación Digital,
Ing. en Ciencias de la Computación, Ing. en Ciberseguridad
e Ing. en Telecomunicaciones

Periodicidad

Semestral

Volumen y Número

Volumen 2, Número 1

Fecha de publicación

Agosto 2026

ISSN (Impreso)

3107-1929

ISSN (Virtual)

3107-1937

Sede editorial

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

Web y contacto

[https://revistas.usfx.bo/index.php/rctd/
revista.ctd@usfx.bo](https://revistas.usfx.bo/index.php/rctd/revista.ctd@usfx.bo)

Comité Editorial

Viktoría Belianskaya

Directora Editorial

María Claudia Saavedra Pacheco

Editora

Juan José Orihuela Palacios

Diseño y Diagramación

Alicia Vaca Vargas

Asistente de diseño

Autoridades Institucionales

Ing. Franz Armando Villalpando Amonzabel

Director de Carrera Ing. de Sistemas, Ing. en Diseño y Animación Digital, Ing. en Ciencias de la Computación, Ing. en Ciberseguridad e Ing. en Telecomunicaciones

Comité Arbitral

GGH, Ph.D., IPNM, México

GASS, Ph.D., UPB, Bolivia

RJNF, M.Sc., PUJ, Colombia

MCSP, M.Sc., USFX, Bolivia

AGM, Ph.D., UNS, Argentina

ECB, M.Sc., UM, Uruguay

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, Ciberseguridad, 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.

Las opiniones expresadas en los artículos son responsabilidad exclusiva de sus autores y no comprometen la postura editorial ni institucional de la revista.

Contenidos

CRIPTOGRAFÍA DE CURVA ELÍPTICA: IMPORTANCIA, APLICACIONES Y COMPARATIVA FRENTE AL ALGORITMO RSA (Pag. 1 -9)

José Enrique Iglesias, USFX

EFFECTO DE LA COMPUTACIÓN CUÁNTICA EN LA CRIPTOGRAFÍA ACTUAL Y PREPARACIÓN PARA LA POST-CUÁNTICA: ARTÍCULO DE REVISIÓN (Pag. 11-22)

Deyler Roca Malale, USFX

ANÁLISIS DE LA DIMENSIÓN HUMANA DURANTE UN CIBERATAQUE (PAG. 23-34)

Ricardo Naranjo Faccini, Universidad Javeriana

EVALUACIÓN DEL IMPACTO DE LAS EMISIONES ELECTROMAGNÉTICAS NO IONIZANTES EN EL DISTRITO I DE SUCRE (PAG. 35-49)

Cristina Vilardell Balasch, USFX

USO DE INTELIGENCIA ARTIFICIAL Y SIMULADORES VIRTUALES COMO ESTRATEGIA PEDAGÓGICA EN LA ENSEÑANZA DE ROBÓTICA (PAG. 51-61)

Kevin Joaquín Díaz Colque, USFX

INTEGRACIÓN DE AGENTES DE IA PARA PROCESAMIENTO SEMÁNTICO Y ANIMACIÓN PROCEDURAL EN SIMULACIONES DEL ECOE CON REALIDAD VIRTUAL (PAG. 63-71)

Pablo Saavedra Rodríguez, USFX

CRIPTOGRAFÍA DE CURVA ELÍPTICA: IMPORTANCIA, APLICACIONES Y COMPARATIVA FRENTE AL ALGORITMO RSA

ELLIPTIC CURVE CRYPTOGRAPHY: IMPORTANCE, APPLICATIONS AND COMPARISON WITH RSA ALGORITHM

José Enrique Iglesias

Universidad San Francisco Xavier

iglesias.enrique@usfx.bo

<https://orcid.org/0009-0009-2390-8453>

Bolivia

Recibido: 19 Mayo 2026 / Revisado: 29 Junio 2026 / Aceptado: 12 Julio 2026 / Publicado: 4 Agosto 2026

Resumen

La seguridad de las comunicaciones en redes públicas se ha vuelto un pilar fundamental del contexto digital actual, donde la criptografía asimétrica desempeña un rol central. La criptografía de Curva Elíptica (ECC), propuesta de manera independiente por Neal Koblitz y Victor Miller en 1985, constituye una alternativa relevante a los esquemas clásicos basados en la factorización de números enteros, como el algoritmo RSA. Su seguridad se fundamenta en el Problema del Logaritmo Discreto sobre Curvas Elípticas (ECDLP), que permite alcanzar niveles equivalentes de seguridad con tamaños de clave significativamente menores.

El presente artículo analiza, mediante una revisión sistemática de literatura reciente, la importancia, aplicaciones y rendimiento comparativo de la ECC frente al algoritmo RSA. La metodología consistió en una búsqueda cualitativa en Scopus, IEEE Xplore, ScienceDirect, MDPI y SpringerLink, limitada a publicaciones de los últimos cinco años. Los resultados evidencian que la ECC se ha consolidado como esquema asimétrico preferente en escenarios con recursos restringidos, particularmente en IoT, TLS, blockchain y firma digital, donde sus variantes principales (P-256, secp256k1, Curve25519 y Ed25519) presentan ventajas demostradas en eficiencia computacional, consumo de memoria y tamaño de claves. Se concluye que la ECC redefine las condiciones de viabilidad de la criptografía asimétrica contemporánea.

Palabras clave: Criptografía de curva elíptica, ECC, ECDSA, Seguridad informática, Criptografía asimétrica

Abstract

The security of communications in public networks has become a fundamental pillar of the current digital context, where asymmetric cryptography plays a central role. Elliptic Curve Cryptography (ECC), independently proposed by Neal Koblitz and Victor Miller in 1985, constitutes a relevant alternative to classical schemes based on the factorization of integers, such as the RSA algorithm. Its security relies on the Elliptic Curve Discrete Logarithm Problem (ECDLP), which enables equivalent security levels with significantly smaller key sizes.

This article analyzes, through a systematic review of recent literature, the importance, applications, and comparative performance of ECC against the RSA algorithm. The methodology consisted of a qualitative search in Scopus, IEEE Xplore, ScienceDirect, MDPI, and SpringerLink, limited to publications from the last five years. The results show that ECC has consolidated as the preferred asymmetric scheme in resource-constrained scenarios, particularly in IoT, TLS, blockchain, and digital signatures, where its main variants (P-256, secp256k1, Curve25519, and Ed25519) present demonstrated advantages in computational efficiency, memory consumption, and key size. It is concluded that ECC redefines the conditions of viability of contemporary asymmetric cryptography.

Keywords: *Elliptic curve cryptography, ECC, ECDSA, Information security, Asymmetric cryptography.*

Introducción

En la actualidad, la seguridad de las comunicaciones y la protección de la información se han convertido en pilares fundamentales para garantizar la integridad, confidencialidad y autenticidad de los datos que se transmiten a través de redes públicas, las cuales se caracterizan por ser inseguras. La criptografía asimétrica o de clave pública desempeña un papel importante en este contexto, ya que permite cifrar la información sin necesidad de compartir previamente una clave secreta entre el emisor y el receptor. Durante décadas, el algoritmo RSA (Rivest, Shamir y Adleman) ha sido el referente en este tipo de criptografía, el cual es ampliamente utilizado en certificados digitales, intercambio de claves y firma electrónica.

Bajo este contexto, el crecimiento exponencial del Internet de las Cosas (IoT), los dispositivos móviles y las tecnologías blockchain ha planteado nuevos desafíos de

seguridad que requieren soluciones criptográficas con altos niveles de seguridad y bajos requerimientos computacionales y de procesamiento. La criptografía de Curva Elíptica (ECC), propuesta de manera independiente por Neal Koblitz y Victor Miller en 1985, permite responder a estas necesidades y se constituye en una alternativa a los sistemas de criptografía basados en la factorización de números enteros. La ECC se fundamenta en la dificultad del Problema del Logaritmo Discreto sobre Curvas Elípticas (ECDLP), un problema matemático que permite alcanzar niveles equivalentes de seguridad al algoritmo RSA, pero con tamaños de clave significativamente menores.

De acuerdo con Adeniyi et al. (2024), la ECC se ha consolidado como algoritmo criptográfico en sistemas IoT, debido a su eficiencia y rendimiento. Asimismo, Shah et al. (2025) sostienen que el tamaño reducido de las claves y el alto nivel de seguridad han posicionado a la ECC como uno de los algoritmos asimétricos más relevantes en la

actualidad. Esta tendencia se observa en la adopción de variantes como secp256k1 en Bitcoin y Ethereum, Curve25519 en protocolos de mensajería segura y los estándares NIST P-256 y P-384 en certificados y firmas digitales.

El presente artículo tiene como objetivo principal analizar la importancia, aplicaciones y rendimiento comparativo de la criptografía de curva elíptica frente a otros esquemas asimétricos clásicos. A partir de este objetivo general, se realiza un estudio de los fundamentos matemáticos esenciales de la ECC, la comparación de tamaños de clave, eficiencia y aplicabilidad frente a RSA, la identificación de sus principales aplicaciones en TLS, blockchain, IoT y firma digital.

Metodología de búsqueda

Al tratarse de un artículo de revisión, se adoptó un enfoque cualitativo enmarcado en la identificación y análisis sistemático de literatura científica relacionada con la ECC, considerando tanto sus fundamentos teóricos como sus aplicaciones prácticas. La búsqueda de información se realizó en bases de datos científicas ampliamente reconocidas por su rigor académico y su cobertura en áreas como ciencias de la computación, seguridad de la información y criptografía, entre las que se incluyen Scopus, IEEE Xplore, ScienceDirect, MDPI y SpringerLink.

Las estrategias de búsqueda se construyeron empleando términos clave en inglés, esto debido a la escasa literatura que existe en español, los mismos fueron articulados mediante los operadores booleanos AND y OR, con el objeto de combinar los aspectos teóricos en relación con los contextos aplicativos. Las cinco cadenas utilizadas fueron: "Elliptic Curve Cryptography" AND ("RSA comparison" OR "key size"); "ECC" AND

IoT security"; "ECDSA" OR "Ed25519" AND "digital signature"; "secp256k1" AND "blockchain"; "Elliptic Curve Diffie-Hellman" AND "TLS". La búsqueda se restringió a publicaciones comprendidas entre 2021 y 2025, este aspecto es fundamental ya que la ciberseguridad es un campo de rápida evolución.

En cuanto a la pertinencia y calidad de los estudios revisados, se definieron los siguientes criterios de inclusión: (a) artículos publicados en revistas científicas indexadas, (b) estudios que aborden aspectos teóricos, comparativos o aplicados de la ECC, y (c) publicaciones disponibles en texto completo. Como criterios de exclusión se establecieron los siguientes: (a) registros duplicados entre bases de datos, (b) publicaciones sin revisión por pares y actas de congresos sin arbitraje riguroso, y (c) trabajos enmarcados en aspectos puramente matemáticos sin vinculación criptográfica.

En relación al proceso de selección, el mismo se llevó a cabo en tres etapas. En la primera etapa, tras aplicar las cadenas de búsqueda, se identificaron 38 registros iniciales que abordaban la temática de la ECC en sus distintas dimensiones. En la segunda etapa, se eliminaron 9 registros duplicados entre bases de datos y 18 registros que no cumplían los criterios de inclusión tras la revisión de títulos y resúmenes, quedando 11 documentos preseleccionados. Finalmente, en la tercera etapa, tras la lectura de los documentos y la evaluación de pertinencia temática y calidad metodológica, se incluyeron 7 estudios que constituyen la base bibliográfica sobre la cual se estructura el presente análisis.

Finalmente, los ejes temáticos que se utilizaron para la construcción de las cadenas de búsqueda fueron los siguientes: Criptografía de Curva Elíptica, Criptografía Asimétrica, algoritmo ECDSA, curvas

estandarizadas, seguridad en IoT, aplicaciones en TLS y Blockchain. Esta cobertura permitió abordar de manera integral los fundamentos, las variantes actuales y los principales escenarios de aplicación de la ECC en el contexto actual.

Desarrollo y discusión

Fundamentos matemáticos de la criptografía de curva elíptica

Una curva elíptica se define de forma simplificada como $y^2 = x^3 + ax + b$, donde los coeficientes a y b satisfacen la condición de no singularidad $4a^3 + 27b^2 \neq 0$. Esta condición

garantiza que la curva no presente puntos singulares como intersecciones consigo misma o discontinuidades, lo cual es necesario para que su estructura matemática sea válida en criptografía.

La seguridad de la ECC se basa en la dificultad del Problema del Logaritmo Discreto sobre Curvas Elípticas (ECDLP), el cual consiste en: dados dos puntos P y Q pertenecientes a la curva tales que $Q=kP$, determinar el valor escalar k que satisface dicha relación. En la actualidad, no se conocen algoritmos eficientes para resolver el ECDLP, lo que permite alcanzar niveles equivalentes de seguridad al algoritmo RSA con tamaños de clave significativamente menores (Abhishek y Raj, 2021).

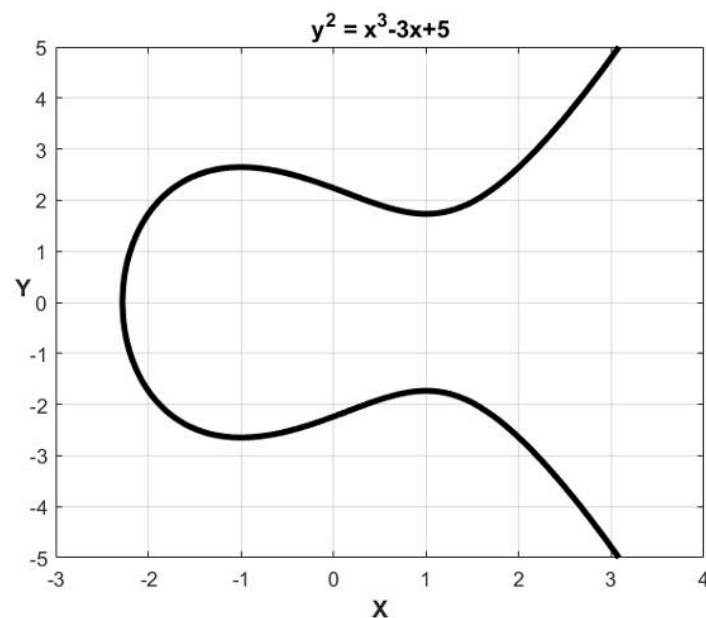


Figura 1. Representación gráfica de una curva elíptica - Condición de no singularidad

Geométricamente, sobre el conjunto de puntos de una curva elíptica se define una operación de suma entre dos puntos P y Q , esta suma se realiza trazando la recta que pasa por ambos puntos, la cual interseca nuevamente la curva elíptica en un tercer punto (R'). Luego, este punto se refleja respecto al eje horizontal para obtener el

resultado final de la operación. Cuando los puntos coinciden ($P = Q$), la suma se calcula utilizando la recta tangente a la curva en ese punto, siguiendo el mismo procedimiento de intersección y reflexión. Este mecanismo de suma es la base de las operaciones utilizadas en la criptografía de curva elíptica (Tanksale, 2024).

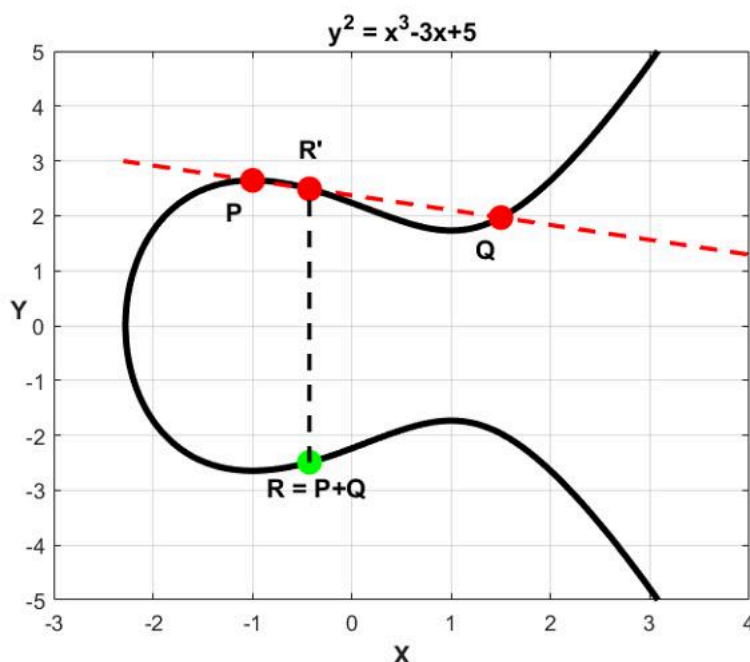


Figura 2. Suma de puntos $P + Q = R$ sobre una curva elíptica

A partir de la operación de suma de puntos se define la operación central de la criptografía de curva elíptica que es la multiplicación escalar, expresada como kP , que consiste en sumar el punto P consigo mismo k veces. Esta operación posee una propiedad fundamental centrada en que calcular $Q = kP$ a partir de k y P es computacionalmente eficiente, pero recuperar k a partir de P y Q corresponde al Problema del Logaritmo Discreto sobre Curvas Elípticas, problema que no posee soluciones eficientes conocidas. Esta asimetría es la que sustenta el funcionamiento de la ECC, donde el escalar k actúa como clave privada y el punto $Q = kP$ como clave pública, de manera que esta última puede compartirse abiertamente sin comprometer a la primera. Sobre este principio se construyen aplicaciones como el intercambio de claves Diffie-Hellman sobre curva elíptica (ECDH) y los esquemas de firma digital ECDSA y EdDSA.

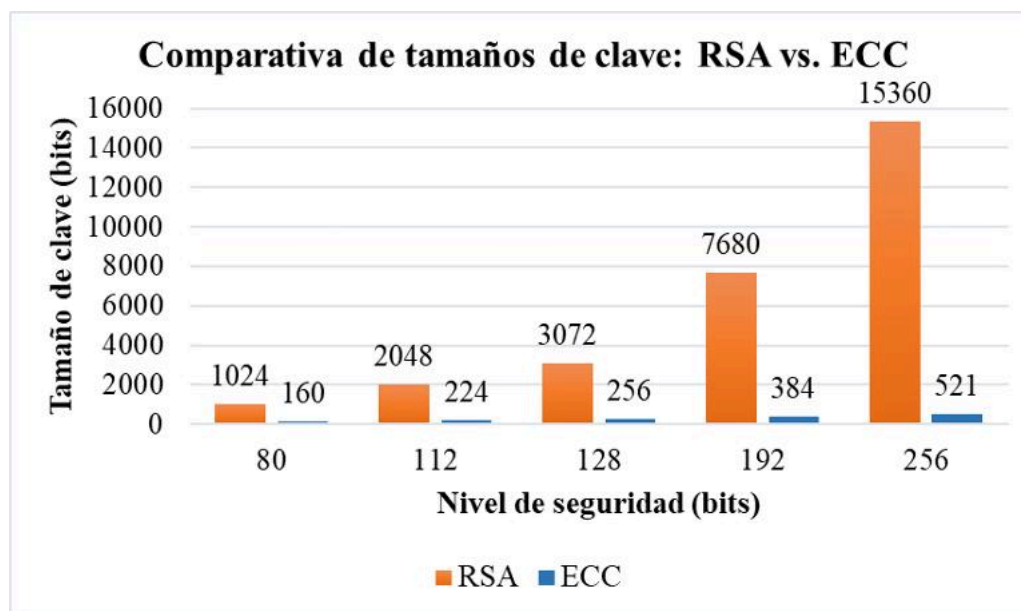
Comparativa entre ECC y el algoritmo RSA

Una de las principales razones por las que la ECC ha tomado ventaja sobre el algoritmo de criptografía RSA es su eficiencia para alcanzar niveles equivalentes de seguridad, mientras que RSA requiere tamaños de clave de 2048 a 3072 bits para garantizar entre 112 y 128 bits de seguridad, la ECC alcanza el mismo nivel con claves de apenas 224 a 256 bits (Ntayagabiri et al., 2024). Esta diferencia se traduce en ventajas importantes a nivel operativo, ya que el uso de claves más pequeñas permite reducir el costo computacional manteniendo niveles de seguridad equivalentes, además de acelerar ciertos procesos tales como la generación de claves y las firmas digitales.

Tabla 1. Equivalencia de niveles de seguridad entre ECC y RSA

Nivel de seguridad (bits)	Tamaño clave RSA (bits)	Tamaño clave ECC (bits)	Ejemplo de curva ECC
80	1024	160	secp160r1
112	2048	224	secp224r1
128	3072	256	P-256, secp256k1
192	7680	384	P-384
256	15360	521	P-521

Nota. Elaborada a partir de Ntayagabiri et al. (2024) y Shah et al. (2025)

**Figura 3.** Tamaños de clave entre RSA y ECC para distintos niveles de seguridad

Lo expuesto anteriormente muestra la diferencia entre el algoritmo RSA y la Criptografía de Curva Elíptica. Mientras que RSA requiere un aumento considerable del tamaño de clave para mantener niveles equivalentes de seguridad desde 1024 hasta 15360 bits, ECC logra los mismos niveles utilizando claves mucho más pequeñas, entre 160 y 521 bits. Esta diferencia muestra la eficiencia de ECC en términos de costos

computacionales y consumo de memoria. Asimismo, se presentan algunas curvas representativas para criptografía de curva elíptica, entre las que se incluyen secp160r1, NIST P-256 y secp256k1, las cuales se aplican en protocolos de comunicación segura (TLS), firmas digitales, blockchain, sistemas de Internet de las Cosas (IoT) y protocolos de intercambio de claves.

Aplicaciones de la Criptografía de Curva Elíptica

La consolidación de la ECC en aplicaciones reales ha favorecido el desarrollo de distintos ámbitos, tales como las comunicaciones seguras en Internet, las tecnologías blockchain y criptomonedas, el Internet de las Cosas (IoT) y la firma digital.

En el ámbito de las comunicaciones seguras, TLS 1.3, la versión más reciente de este protocolo, ha adoptado masivamente el uso de las Curvas Elípticas como mecanismo predeterminado de intercambio de claves.

Existen variantes como Curve25519 que se destaca por ofrecer velocidades de handshake superiores y resistencia a vulnerabilidades de implementación frente a esquemas tradicionales. La inclusión de X25519 y X448 en el estándar TLS 1.3 para el intercambio de claves entre dos partes a través de un canal inseguro representa un punto de inflexión en la adopción de la criptografía elíptica moderna.

En el ámbito de blockchain y criptomonedas, la curva secp256k1 sustenta el esquema de firmas digitales ECDSA utilizado en Bitcoin, Ethereum y en gran parte de las criptomonedas derivadas.

En este contexto, Balasubramanian (2024) señala que su adopción se debe, por un lado, a la eficiencia computacional que ofrece, por otro lado, a la transparencia de sus parámetros, es decir, a que los valores que definen la curva fueron generados de manera pública y verificable, sin procedimientos ocultos o dependientes de entidades centralizadas. En consecuencia, la seguridad de las direcciones de Bitcoin y la integridad de las transacciones se fundamentan directamente en la dificultad del Problema del

Logaritmo Discreto sobre Curvas Elípticas (ECDLP) asociado a esta curva.

En el contexto del Internet de las Cosas, la criptografía de curva elíptica se ha posicionado como una alternativa adecuada para dispositivos que tienen restricciones de procesamiento, memoria y energía.

Adeniyi et al. (2024) concluyen que la ECC ha recibido mayor atención y es más frecuentemente empleada en sistemas IoT que otros métodos criptográficos. Bajo este contexto, Zhao et al. (2022) propusieron un protocolo de autenticación de tres factores basado en ECC para el Internet Industrial de las Cosas (IIoT), demostrando su viabilidad práctica con propiedades formales de seguridad verificadas mediante la herramienta Scyther, la cual sirve para analizar y verificar la seguridad de protocolos de comunicación.

En el ámbito de la firma digital, los esquemas ECDSA y EdDSA se consolidan como los más utilizados para garantizar autenticación, integridad y no repudio. En particular, EdDSA se construye sobre las curvas conocidas como Curve25519 y Curve448, las cuales se caracterizan por generar firmas de manera determinista, es decir, sin depender de valores aleatorios en cada operación, esta propiedad reduce significativamente el riesgo de fallos de seguridad asociados a una mala generación de números aleatorios, una debilidad conocida en implementaciones incorrectas de ECDSA.

Adicionalmente, estos esquemas han sido incorporados formalmente en el estándar FIPS 186-5 publicado por el NIST en 2023, donde se definen los métodos aprobados para la generación y verificación de firmas digitales.

A continuación, se presentan las principales Curvas Elípticas utilizadas en criptografía y sus aplicaciones.

Tabla 2. Principales Curvas Elípticas estandarizadas y sus aplicaciones

Curva	Tamaño	Estándar / Origen	Aplicaciones principales
secp256r1 (P-256)	256 bits	NIST FIPS 186	TLS, certificados X.509, S/MIME
secp256k1	256 bits	SECG	Bitcoin, Ethereum, criptomonedas
Curve25519 (X25519)	256 bits	RFC 7748	Intercambio de claves TLS, Signal, WhatsApp
Ed25519	256 bits	RFC 8032; FIPS 186-5	SSH, firma digital, autenticación
Curve448 / Ed448	448 bits	RFC 7748 / RFC 8032	TLS 1.3, escenarios de mayor nivel de seguridad

Nota. Elaborada a partir de Shah et al. (2025) y Tanksale (2024).

Conclusiones

La revisión realizada permite concluir que la pertinencia de la criptografía de curva elíptica no reside únicamente en su capacidad de igualar la seguridad ofrecida por el algoritmo RSA, sino en redefinir las condiciones bajo las cuales la criptografía asimétrica resulta viable. Mientras que RSA fue diseñado para entornos con recursos abundantes, la ECC abre la posibilidad de implementar mecanismos de clave pública en escenarios donde antes resultaba inviable, particularmente en dispositivos con limitaciones de hardware, energéticas o de procesamiento.

Asimismo, se observa que la elección de una curva elíptica debe responder a criterios de transparencia y propósito de aplicación. Por ejemplo, la adopción de secp256k1 en sistemas blockchain por su origen abierto, las curvas NIST P-256 y P-384 en entornos de certificados digitales, o Curve25519 y Ed25519 en aplicaciones de mensajería por sus propiedades de seguridad, evidencia que la ECC ha tenido avances considerables al punto

de ofrecer alternativas diferenciadas según el contexto de uso.

Finalmente, fruto del proceso de revisión se pudo identificar dos vacíos importantes que deben ser considerados en futuras investigaciones. En primer lugar, la producción académica en español sobre criptografía de curva elíptica sigue siendo limitada en comparación con la amplia literatura anglosajona, lo que restringe su difusión y apropiación en el contexto regional, es así que se abre una oportunidad para fortalecer el desarrollo científico en el ámbito latinoamericano. En segundo lugar, se evidencia la necesidad de contar con más estudios comparativos de carácter experimental en entornos específicos, como el Internet de las Cosas industrial y los sistemas embebidos, de tal manera que permitan contrastar los fundamentos teóricos de la ECC con resultados prácticos y verificables en escenarios reales.

Referencias Bibliográficas

Abhishek, K., y Raj, E. G. (2021). Evaluation of computational approaches of short Weierstrass elliptic curves for cryptography. *Cybernetics and Information Technologies*, 21(4), 70-88. <https://doi.org/10.2478/cait-2021-0045>

Adeniyi, A. E., Jimoh, R. G., y Awotunde, J. B. (2024). A systematic review on elliptic curve cryptography algorithm for internet of things: Categorization, application areas, and security. *Computers and Electrical Engineering*, 118. <https://doi.org/10.1016/j.compeleceng.2024.109330>

Balasubramanian, K. (2024). Security of the Secp256k1 elliptic curve used in the Bitcoin blockchain. *Indian Journal of Cryptography and Network Security*, 4(1), 9-15. <https://doi.org/10.54105/ijcns.A1426.04010524>

Ntayagabiri, J. P., Ndikumagenge, J., Bentaleb, Y., y El Makhtoum, H. (2024). Comparative analysis of elliptic curve-based cryptographic approaches for Internet of Things security. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 10(6), 568-583. <https://doi.org/10.32628/CSEIT2410457>

Shah, N. H., Ismail, S. A., Azizan, A., Anoop, A., Khan, D. T., y Ahamed, S. (2025). Lightweight Authentication Protocols in Internet of Things - A Review. *International Journal of Engineering Trends and Technology*, 73(3). <https://doi.org/10.14445/22315381/IJETT-V73I3P108>

Tanksale, V. (2024). Efficient elliptic curve Diffie-Hellman key exchange for resource-constrained IoT devices. *Electronics*, 13(18). <https://doi.org/10.3390/electronics13183631>

Zhao, X., Li, D., y Li, H. (2022). Practical Three-Factor Authentication Protocol Based on Elliptic Curve Cryptography for Industrial Internet of Things. *Sensors*, 22(19). <https://doi.org/10.3390/s22197510>

EFFECTO DE LA COMPUTACIÓN CUÁNTICA EN LA CRIPTOGRAFÍA ACTUAL Y PREPARACIÓN PARA LA POST- CUÁNTICA: ARTÍCULO DE REVISIÓN

EFFECT OF QUANTUM COMPUTING ON CURRENT CRYPTOGRAPHY AND PREPARATION FOR POST- QUANTUM: REVIEW ARTICLE

Deyler Roca Malale

Universidad San Francisco Xavier

Roca.deyler@usfx.bo

<https://orcid.org/0009-0000-7476-3674>

Bolivia

Recibido: 10 Mayo 2026 / Revisado: 20 Julio 2026 / Aceptado: 31 Julio 2026 / Publicado: 4 Agosto 2026

Resumen

El avance acelerado de la computación cuántica ha despertado un creciente interés en la comunidad científica y tecnológica debido a su potencial para transformar profundamente diversos campos, entre ellos la criptografía. A diferencia de los sistemas computacionales clásicos, los ordenadores cuánticos aprovechan fenómenos como la superposición y el entrelazamiento para realizar cálculos de forma exponencialmente más eficiente. Esta capacidad pone en riesgo los algoritmos criptográficos actuales, especialmente aquellos basados en la factorización de enteros y el logaritmo discreto, pilares de la seguridad digital moderna. Este estudio tiene como objetivo analizar y evaluar los potenciales efectos que la computación cuántica tendría en los sistemas criptográficos vigentes y examinar las principales propuestas de criptografía post-cuántica desarrolladas como respuesta a esta amenaza emergente. Esto se realizó mediante una revisión de artículos publicados en el periodo comprendido entre los años 2020 y 2025, para ello se aplicó el protocolo PRISMA 2020 a 283 artículos consultados en bases de datos como Scopus, ScienceDirect y PubMed, aplicando una estrategia de búsqueda a través de palabras clave y operadores booleanos, descartando duplicados, y aplicando criterios de inclusión y exclusión, hasta seleccionar 15 artículos, que conformaron la muestra final de análisis, con la ayuda de Rayyan y VOSviewer. La revisión evidencia que la transición hacia la criptografía post-cuántica ya constituye un proceso tecnológico en desarrollo, impulsado por la estandarización de algoritmos resistentes como ML-KEM y ML-DSA, la implementación de esquemas criptográficos híbridos y la validación experimental de su desempeño en entornos como redes 5G, infraestructuras SDN, computación en la nube y centros de datos de alta capacidad.

Asimismo, los estudios analizados coinciden en que la principal amenaza no radica únicamente en el incremento de la capacidad de cómputo cuántico, sino también en la necesidad de rediseñar las estrategias de gestión criptográfica, la administración de claves y los mecanismos de migración hacia infraestructuras resilientes. En consecuencia, esta revisión concluye que, aunque la computación cuántica aún no posee la madurez suficiente para comprometer de forma generalizada los sistemas criptográficos actualmente desplegados, la adopción progresiva de soluciones post-cuánticas constituye una prioridad estratégica para preservar la seguridad de la información en el mediano y largo plazo.

Palabras clave: Computación cuántica, Algoritmos cuánticos, Criptografía post-cuántica, qubits, hash.

Abstract

The rapid advancement of quantum computing has sparked growing interest in the scientific and technological community due to its potential to profoundly transform various fields, including cryptography. Unlike classical computing systems, quantum computers leverage phenomena such as superposition and entanglement to perform calculations exponentially more efficiently. This capability puts current cryptographic algorithms at risk, especially those based on integer factorization and discrete logarithms, pillars of modern digital security. This study aims to analyze and verify the potential impact that quantum computing would have on current cryptographic systems and examine the main post-quantum cryptography proposals developed in response to this emerging threat. This was achieved through a review of articles published between 2020 and 2025. The PRISMA 2020 protocol was applied to 283 articles searched in databases such as Scopus, ScienceDirect and PubMed. A search formula was applied using keywords and Boolean operators, discarding duplicates, and applying inclusion and exclusion criteria. The final result was 15 articles, which were analyzed and studied with the help of Rayyan and VOSviewer. The discussion shows that while current cryptographic algorithms have evolved rapidly, obtaining robust cryptographic algorithms that are even highly resilient in terms of encryption and cryptography. The review concludes that, although quantum computing has not yet reached the maturity necessary to breach production systems, early preparation and the development of quantum-resistant cryptographic schemes are essential to guarantee information security in the near future.

Keywords: Quantum computing, Quantum algorithms, Post-quantum, cryptography, qubits, hash.

Introducción

En la era digital actual, la protección de la información se ha convertido en un pilar esencial para el funcionamiento de las sociedades modernas. Desde las comunicaciones personales hasta las infraestructuras críticas de los Estados, una vasta cantidad de datos circula diariamente por redes que dependen de sistemas criptográficos para garantizar la confidencialidad, integridad y autenticidad de la información. Estos sistemas se sustentan, en su mayoría, en supuestos de seguridad ligados a problemas matemáticos difíciles de resolver para los ordenadores clásicos, como la factorización de números primos y el cálculo de logaritmos discretos (Bernstein et al., 2017).

Sin embargo, el desarrollo de la computación cuántica está reconfigurando radicalmente este escenario. A diferencia de la computación tradicional, la computación cuántica emplea principios de la mecánica cuántica, como la superposición y el entrelazamiento, para realizar operaciones con una eficiencia exponencialmente mayor en ciertos tipos de cálculos. Esta capacidad ha demostrado, al menos teóricamente, su potencial para romper los sistemas criptográficos que hoy se consideran seguros (Arute et al., 2019). El conocido algoritmo de Shor, por ejemplo, puede factorizar grandes números primos en un tiempo significativamente menor al requerido por los métodos clásicos, comprometiendo la seguridad de estándares como RSA y ECC (Shor, 1997; Chen et al., 2016).

Este panorama plantea un problema de gran envergadura: ¿qué tan preparada está la infraestructura digital actual frente al avance de la computación cuántica? Y más aún, ¿Cuáles son los caminos tecnológicos y científicos que se están desarrollando para

proteger la información en una era post-cuántica?. La revisión de la literatura evidencia una creciente preocupación, pero también una serie de vacíos teóricos y prácticos. Por un lado, existen múltiples propuestas de algoritmos resistentes a ataques cuánticos, conocidos colectivamente como criptografía post-cuántica; por otro, la estandarización, la evaluación empírica y la adopción práctica de estas tecnologías todavía se encuentran en una fase inicial (National Institute of Standards and Technology [NIST], 2022).

El presente artículo tiene por objetivo analizar de manera crítica y reflexiva el efecto que puede tener la computación cuántica sobre la criptografía actual, con énfasis en la preparación hacia un entorno post-cuántico. Para ello se han revisado artículos publicados en el periodo comprendido entre los años 2020 y 2025, analizando las principales amenazas, los avances en criptografía resistente a la computación cuántica y las iniciativas institucionales en torno a la estandarización. La presente revisión bibliográfica se limita al análisis de investigaciones publicadas entre 2020 y 2025 e indexadas en las bases de datos Scopus, ScienceDirect y PubMed, seleccionadas mediante el protocolo PRISMA 2020 y criterios previamente establecidos de inclusión y exclusión.

En consecuencia, los resultados obtenidos representan el estado del conocimiento derivado únicamente de los estudios que cumplieron dichos criterios metodológicos. Esta revisión no incluye literatura gris, capítulos de libros, actas de congresos, tesis, documentos técnicos ni investigaciones no indexadas, así como tampoco aborda el desarrollo experimental del hardware cuántico o aplicaciones de la computación cuántica ajenas al ámbito de la criptografía y la seguridad de la información. Por ello, las

conclusiones deben interpretarse dentro del alcance de la evidencia científica analizada y no como una evaluación exhaustiva de todas las investigaciones existentes sobre computación cuántica. La variable central de esta revisión es la relación entre capacidad computacional cuántica y robustez de los sistemas criptográficos actuales y futuros. El marco conceptual se apoya en la teoría de la complejidad computacional, la seguridad informática y los modelos de transición tecnológica ante disrupciones emergentes. Todo ello permitió sintetizar el estado actual de la criptografía y comprender el funcionamiento y las posibilidades de aplicación de los principales algoritmos resistentes a la computación cuántica.

Metodología

Para llevar adelante la presente investigación, se realizó una revisión sistemática y pormenorizada de la literatura científica con el propósito de identificar y analizar los estudios más relevantes relacionados con la computación cuántica y cuáles podrían ser los efectos en la criptografía actual y qué estrategias de mitigación pueden adoptarse en la era post-cuántica, para ello, se consultaron bases de datos indexadas como Scopus, PubMed y ScienceDirect. La búsqueda se efectuó utilizando combinaciones de palabras clave como: “Efecto de la computación cuántica”, “criptografía”, “criptografía actual”, “post-cuántica”. Los términos de búsqueda se formularon en inglés con el propósito de ampliar la recuperación de publicaciones internacionales indexadas, empleando operadores booleanos como AND y OR para delimitar los resultados obtenidos en las búsquedas.

El rango temporal considerado comprendió los años 2020 a 2025. La búsqueda inicial permitió identificar 283 artículos,

posteriormente se establecieron como criterios de inclusión, artículos originales de investigación, en idioma inglés y solo artículos de acceso abierto. Se excluyeron artículos de revisión, conferencias, capítulos de libro, libros y duplicados, así como áreas temáticas como física y astronomía, ciencias de la decisión y materiales. Posteriormente, los artículos fueron exportados al software Rayyan, el cual facilitó el proceso de cribado y la identificación de 46 artículos duplicados, que fueron eliminados. Finalmente, se seleccionaron para el análisis completo 15 artículos que cumplieran los criterios de inclusión y abordaban directamente la temática del estudio de este artículo de revisión.

Para el presente artículo, se adoptó el protocolo PRISMA 2020 para estructurar el proceso de revisión sistemática, el cual permitió visualizar de forma clara y transparente el flujo de identificación, cribado, elegibilidad e inclusión de los artículos (Haddaway et al., 2022). La figura correspondiente al diagrama de flujo PRISMA 2020 (Figura 1) resume cada etapa del proceso, indicando el número de artículos identificados, los duplicados eliminados y los criterios de inclusión y exclusión aplicados para la selección final.

Complementariamente, se utilizó el software VOSviewer para realizar un análisis bibliométrico de los artículos incluidos, construyendo mapas de coocurrencia de palabras clave y redes de coautoría, con el objetivo de visualizar de manera más clara y precisa las tendencias temáticas predominantes con respecto al tema investigado y las colaboraciones académicas más significativas dentro del campo estudiado.

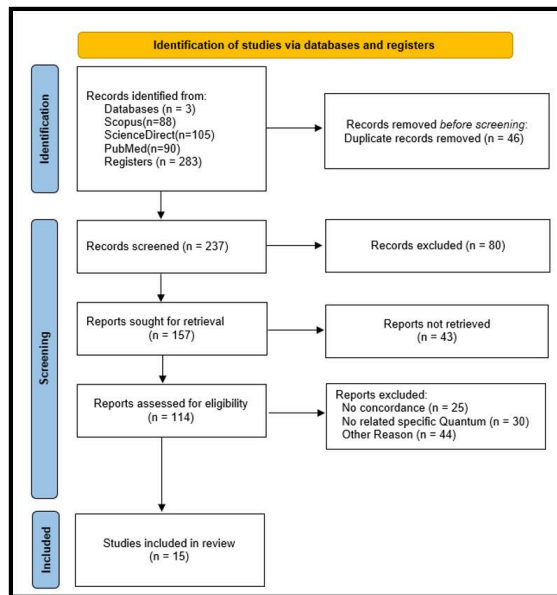


Figura 1. Diagrama de flujo PRISMA 2020.

Nota. Adaptado de McGuinness, L. A. (2022).PRISMA2020

Desarrollo y resultados

En la Tabla 1, se presenta un resumen estructurado de los 15 artículos científicos seleccionados para este estudio. En ella se detallan el título, los autores, el resultado principal, el año de publicación y el DOI.

Esta recopilación permite observar de forma comparativa la diversidad de enfoques, estudios, tendencias de los algoritmos criptográficos y distintas propuestas de soluciones criptográficas para la era poscuántica.

Tabla 1. Artículos incluidos en la investigación

No	Título	Autores	Resultado	Año	DOI
1	Understanding instance hardness for optimisation algorithms: Methodologies, open challenges and post-quantum implications	Kate Smith-Miles	El artículo se centra posteriormente en los algoritmos cuánticos para la optimización y argumenta que las lecciones clave aprendidas sobre la prueba de algoritmos de optimización en las últimas décadas son muy relevantes para los esfuerzos actuales por explorar la ventaja cuántica para la optimización.	2025	https://doi.org/10.1016/j.apm.2025.115965
2	Hybrid Quantum-Safe integration of TLS in SDN networks	Jaime S. Buruaga a,*, Ruben B. Méndez a, Juan P. Brito b, Vicente Martin	En este trabajo, se ha seleccionado la Seguridad de la Capa de Transporte (TLS), uno de los protocolos más utilizados, como base para hibridar la criptografía clásica, cuántica y poscuántica de forma que se adapte a su amplia adopción en las Redes Definidas por Software (SDN) el paradigma de red más flexible utilizado para implementar redes cuántico-clásicas integradas.	2025	https://doi.org/10.1016/j.comnet.2025.111355
3	Review of Distributed Quantum Computing: From single QPU to High Performance Quantum Computing	David Barral A , F. Javier Cardama B , Guillermo Díaz Camacho A, Daniel Fáilde A.	Este artículo presenta un estudio exhaustivo del estado actual del arte en el campo de la computación cuántica distribuida, explorando sus principios fundamentales, el panorama de logros, los desafíos y las prometedoras direcciones para futuras investigaciones.	2025	https://doi.org/10.1016/j.cosrev.2025.100747
4	An approach for automated generation of quantum computing models using deep learning.	Niyazi Furkan Bar ,* Mehmet Karakose	El estudio propone un enfoque basado en la generación automática de circuitos y códigos cuánticos mediante aprendizaje profundo.	2025	https://doi.org/10.1016/j.asej.2025.103327
5	Post-quantum cryptography Algorithm's standardization and performance analysis	Manish Kumar	Este artículo analiza en detalle el esfuerzo global para el diseño, desarrollo y estandarización de diversos algoritmos de criptografía de seguridad cuántica, junto con el análisis del rendimiento de algunos de los posibles algoritmos de seguridad cuántica. El objetivo del artículo es analizar la viabilidad de diversos algoritmos de criptografía cuántica segura.	2022	https://doi.org/10.1016/j.array.2022.100242

No	Título	Autores	Resultado	Año	DOI
6	Investigating Quantum-Resilient Security Mechanisms for Flying Ad-Hoc Networks (FANETs)	Abdulnasser AbdulJabbar Abbood, Mahmood A. Al-Shareeda 1, Faris K. AL-Shammri 2, Zainab marid Alzamili 3*, Mohammed Amin Almaiah 5, Rommel AlAli 6*	El estudio analiza algoritmos clásicos y esquemas post-cuántico actuales para FANET, incluyendo soluciones criptográficas lo suficientemente ligeras para entornos con recursos limitados. Los resultados numéricos del experimento muestran que, si bien la criptografía basada en celosía implica un riesgo mínimo de infracciones, su consumo de energía es un 25 % mayor que el de otros sistemas y su tiempo de procesamiento un 30 % más lento. Por el contrario, la criptografía polinómica multivariante es mejor en métricas como el consumo de electricidad: solo consume un 10 % más de energía y necesita un 15 % más de ciclos de CPU para el procesamiento. La introducción de algoritmos y arquitecturas post-cuántico resultó en una reducción del 5-10 % en el rendimiento de la red y un aumento de la latencia del 20 % en algunos escenarios.	2025	https://doi.org/10.18196/jrc.v6i1.25351
7	Quantum Assisted Blockchain Security Model Using Artificial Intelligence to Reduce Quantum Attacks	Ammar AbdRaba Sakran 1*, Ruwaida Mohammed Yas2, Ali Fadhil Rashid 3, Massila Kamalrudin 4, Mustafa Musa 5	En esta investigación se ha propuesto un modelo mejorado de seguridad de blockchain asistido por cuántica mediante la técnica de inteligencia artificial (EQ-BSM-AI). Este modelo valida los criptosistemas y las tecnologías blockchain para determinar su vulnerabilidad a ataques cuánticos.	2025	https://doi.org/10.54216/FPA.180210
8	Generic Quantum Blockchain-Envisioned Security Framework for IoT Environment: Architecture, Security Benefits and Future Research	Mohammad Wazid 1 Ashok Kumar Das and Oungho Park 2,3 4 (member, iee)	En este artículo, se propone un marco de seguridad genérico, basado en blockchain cuántico, para un entorno del Internet de las Cosas (IoT). A continuación, se analiza algunas posibles aplicaciones del marco propuesto. También se destaca las ventajas de seguridad de los sistemas basados en criptografía cuántica. Se explica el funcionamiento de blockchain, sus aplicaciones, tipos de blockchain, su estructura, la estructura de blockchain en una blockchain clásica y la estructura de un bloque en un contexto de blockchain cuántico.	2024	https://doi.org/10.1109/OJCS.2024.3397307
9	Post-Quantum Key Exchange and Subscriber Identity Encryption in 5G Using ML-KEM (Kyber)	Kaiser Khan *, Sourav Purification and Sang-Yoon hang	En este artículo, se estudia la incorporación de los cifrados post-cuánticos en el cálculo de SUCI tanto en el equipo del usuario como en la red central, lo que implica el intercambio de claves compartidas y el uso posterior de la clave resultante para el cifrado del ID. Se experimenta en diferentes plataformas de hardware para analizar el intercambio de claves post-cuántico y el cifrado utilizando CRYSTALS-Kyber estandarizado por el NIST (que ahora se denomina ML-KEM después de la selección de estandarización por parte del NIST).	2025	https://doi.org/10.3390/info16070617
10	The Impact of Quantum Computing on Cryptographic Security Protocols	Mrs. Swati Dixit 1, Dr. Ujwal amesh Shirode ,Dr. Yogita D. Bhise 2 ,Santoshkumar Vaman Chobe 3 , Swati Nikam 4 5	Este breve resumen analiza los importantes efectos que la computación cuántica tendrá en la seguridad de la criptografía. Examina las vulnerabilidades de seguridad que crean los algoritmos cuánticos y destaca la importancia de encontrar soluciones para la criptografía post-cuántica (CPQ). La CPQ busca crear programas que no puedan ser descifrados por ataques cuánticos. Esto garantizará que las interacciones digitales sigan siendo privadas, seguras y reales en un mundo impulsado por computadoras cuánticas. Además, la transición al post-cuántico conlleva numerosos problemas, como la implementación de algoritmos, la garantía de que sean uniformes y la adaptación a entornos tecnológicos muy diversos.	2024	https://doi.org/10.52783/anvi.v27.1419
11	Practical Implementation of Post-Quantum Cryptography for Secure Wireless Communication	Babatunde Ojetunde 1, *, Takuya Kurihara 1,1., Kazuto Yano, Toshikazu Sakano 1 and Hiroyuki Yokoyama 2	Este artículo presenta un nuevo marco para protocolos de cifrado de clave pública (PKE) post-cuántico independientes y post-cuántico-AES (Estándar de Cifrado Avanzado). Con base en resultados previos, nos centramos en la seguridad de aplicaciones como la transferencia de archivos, la transmisión de vídeo y la comunicación por chat mediante protocolos mejorados basados en post-cuántico.	2025	https://doi.org/10.3390/network5020020
12	Quantum-computing-and-the-law-navigating-the-legal-implications-of-a-quantum-leap	Kasim Balarabe	Este artículo investiga las principales implicaciones legales de la computación cuántica, centrándose en la propiedad intelectual, la seguridad de los datos, la regulación y las consideraciones éticas. Las características únicas de los algoritmos y el hardware cuánticos plantean desafíos significativos para el sistema de patentes actual, lo que requiere un marco claro y consistente para proteger las innovaciones cuánticas y fomentar la colaboración.	2025	https://doi.org/10.1017/err.2025.8

No	Título	Autores	Resultado	Año	DOI
13	In-line rate encrypted links using pre-shared post-quantum keys and DPUs	Abraham Cano Aguilera 1,2*, Carlos Rubio Garcia 1, Daniel Lawo 1,2, José Luis Imaña 3, Idelfonso Tafur Monroy 1 & Juan José Vegas Olmos 2	Este trabajo tiene como objetivo ayudar con la transición a esquemas criptográficos resistentes a la cuántica mediante la provisión de una comparación experimental exhaustiva del rendimiento de los cuatro algoritmos seleccionados por el Instituto Nacional de Estándares y Tecnología (NIST) para la estandarización cuando se implementan en una unidad de procesamiento de datos (DPU). Los experimentos se llevan a cabo a velocidad de línea, lo que demuestra por primera vez el funcionamiento a casi 100 Gbit/s y, por tanto, la idoneidad para entornos de centros de datos de alta capacidad.	2024	https://dx.doi.org/10.1038/s41598-024-71861-x
14	Post-quantum cryptography and the quantum future of cybersecurity	Yi-Kai Liu 1, Dustin Moody	Este artículo revisa el estado actual de los esfuerzos para desarrollar e implementar criptografía post-cuántica en Internet. Luego sugerimos formas específicas en las que se podrían utilizar las tecnologías cuánticas para mejorar la ciberseguridad en el futuro cercano y más allá. Nos centramos en dos objetivos: proteger las claves secretas que se utilizan en la criptografía clásica y garantizar la confiabilidad de los cálculos cuánticos.	2024	https://dx.doi.org/10.1103/physrevapplied.21.040501
15	A compact public key encryption with equality test for lattice in cloud computing	Junfei He 1 1, Qing Ye, Zhichao Yang , Shixiong Wang 2 & Jiasheng Wang 1	En este artículo se propone un esquema PKEET compacto. El nuevo esquema no cifra inmediatamente el valor hash del texto simple, sino que lo incorpora a la trampa de prueba. El estudio demuestra que una nueva construcción es unidireccional y segura según el modelo de seguridad cuántica. Con esos esfuerzos, nuestro esquema puede resistir los ataques de texto cifrado elegidos siempre que se cumpla el supuesto de aprendizaje con errores (LWE). Además, evaluamos el rendimiento del nuevo esquema y descubrimos que solo cuesta aproximadamente la mitad del espacio de almacenamiento en comparación con los esquemas anteriores.	2021	https://doi.org/10.1038/s41598-025-12018-2

Las Figuras 2 y 3 muestran los resultados del análisis bibliométrico realizado con el software VOSviewer v1.6.20. La Figura 2 destaca las palabras clave más frecuentes en la literatura revisada, revelando los principales enfoques temáticos sobre el efecto de la computación

cuántica en los algoritmos criptográficos. La Figura 3 representa la red de coautoría, ilustrando las colaboraciones entre los autores más influyentes del campo. La Figura 4 representa el mapa de calor de concurrencia de palabras clave, con más relevancia.

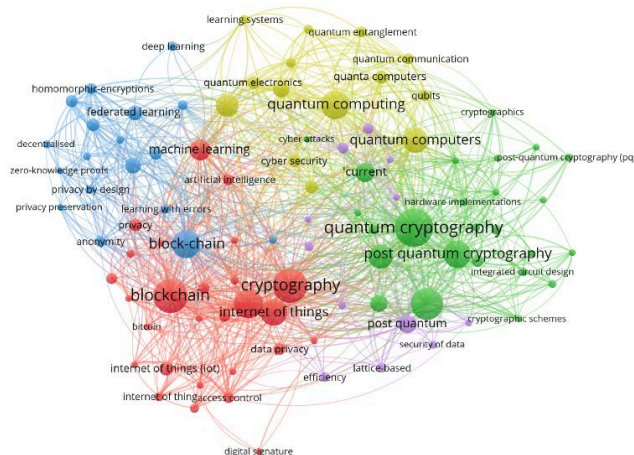


Figura 2. Red de concurrencia de palabras clave.

Nota. Elaboración propia mediante VOSviewer.

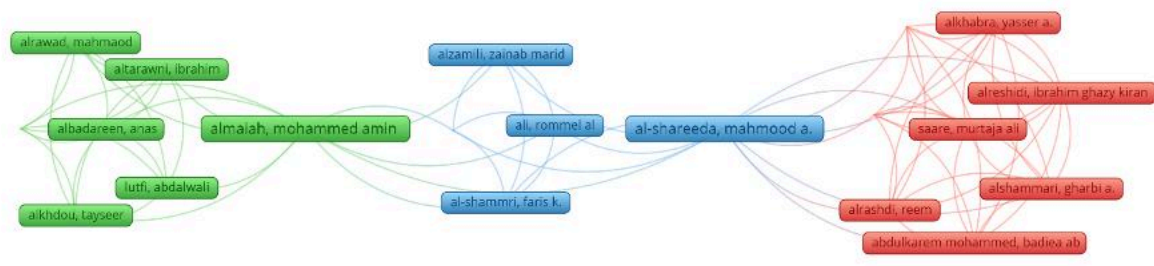


Figura 3. Contribuciones realizadas entre las redes de coautores.

Nota. Elaboración propia mediante VOSviewer.

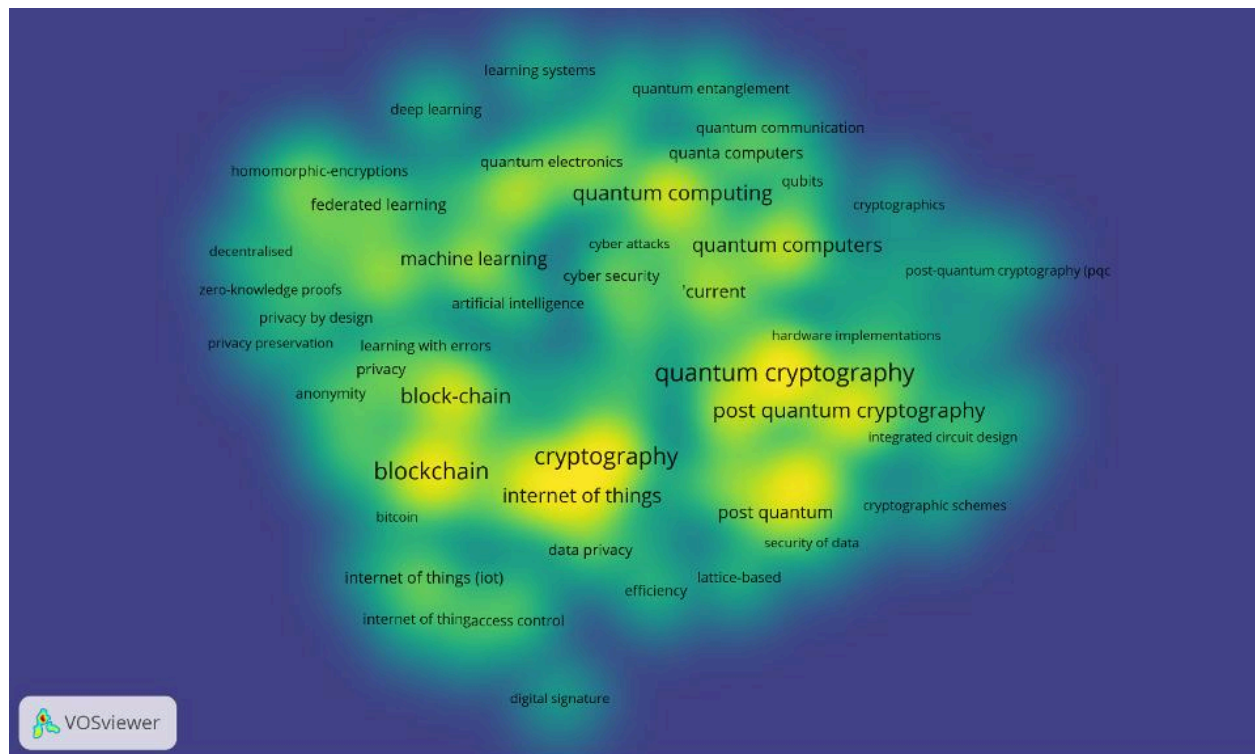


Figura 4. Mapa de calor de concurrencia de palabras clave, con más relevancia.

Nota. Elaboración propia mediante VOSviewer.

Discusión

Esta revisión sistemática, realizada conforme a la metodología PRISMA 2020 y basada en el análisis de 15 estudios, evidencia avances significativos en el desarrollo de la criptografía moderna, aunque también pone de manifiesto las debilidades de los algoritmos criptográficos convencionales frente al avance de la computación cuántica.

En este contexto, los estudios sobre TLS/SDN, VPN/IPsec y redes 5G muestran que la hibridación constituye una estrategia viable para mantener la compatibilidad con la infraestructura existente durante la transición hacia la criptografía post-cuántica, al tiempo que mitiga el riesgo asociado al escenario recolectar ahora y descifrar después (*harvest now, decrypt later*). Jaime S. Buruaga, et al. (2025). La evidencia se presenta en diferentes niveles de análisis.

En la capa de redes y seguridad TLS, las implementaciones de TLS poscuántico, basadas en integraciones PQ-TLS con ML-KEM optimizado mediante instrucciones AVX-512, permiten aumentar el rendimiento de los procesos de negociación criptográfica (*handshakes*) y acercar su desempeño al observado en TLS 1.3 clásico, lo que respalda despliegues a gran escala en entornos operativos extremos.

La propuesta de TLS híbrido en dominios programables mantiene control fino sobre qué flujos usan suites post-cuánticas y cuáles quedan en clásico, útil para migraciones por etapas (*"migración gradual"*). Diversos estudios experimentales muestran mejor tiempo y menor energía en el UE respecto a X25519/secp256r1, pese al aumento de tamaño de claves. Estos resultados sugieren que *"la idea de que la criptografía post-cuántica es necesariamente más lenta"* en todos los casos.

En redes y enlaces troncales, el cuello de botella puede mitigarse mediante la aceleración del procesamiento con unidades de procesamiento de datos (DPU), permitiendo alcanzar velocidades de cifrado de hasta 100 Gbit/s con claves post-cuánticas precompartidas, sin afectar significativamente la latencia, siempre que el diseño y la rotación de las claves sean adecuados. Estos hallazgos evidencian la utilidad de esta estrategia en entornos con elevados requerimientos de procesamiento, como los Centros de Operaciones de Seguridad (SOC).

Dirección estratégica NIST: ML-KEM/ML-DSA y futuro cuántico. El mapeo de NIST (Moody & Liu. 2024) sostiene el plan de estandarización (FIPS 203/204/205) dibuja un horizonte donde la PQC convive con tecnologías cuánticas (p.ej., QKD, RNGs cuánticos) para blindar llaves y verificar cómputos. Esto toma la noción de que paradigma, no es solo cambiar algoritmos, es rediseñar confianza y generación de entropía.

Los hallazgos de fondo que enriquecen o refuerzan los algoritmos criptográficos: FANETs / Mahmood A. Al-Shareeda (2025), redes aéreas y algoritmos resistentes a la computación cuántica para asignación de trayectorias demuestran que la criptografía post-cuántica (PQC) puede operar eficazmente bajo restricciones severas de energía, ancho de banda y tamaño de mensaje. Esto consolida la viabilidad operativa y la robustez del modelo en escenarios tácticos post-cuánticos.

Los avances en los esquemas de cifrado de clave pública con prueba de igualdad (PKEET) basados en retículos evidencian mejoras en la eficiencia del almacenamiento y mantienen un nivel adecuado de seguridad frente a ataques cuánticos. Estas características amplían su potencial de aplicación en entornos de computación en la nube, al facilitar la

realización de búsquedas seguras y tareas de análisis forense sobre información cifrada, tal como señalan He et al. (2025).

La revisión general de los artículos evidencia que la transición hacia la criptografía post-cuántica ya no es un ejercicio teórico, sino un proceso en marcha que combina avances técnicos y estrategias de despliegue pragmáticas. Se observa un consenso en que la hibridación entre algoritmos clásicos y post-cuánticos es la vía más segura para migrar sin interrumpir operaciones, aplicándose en protocolos como TLS, IPsec y 5G con mejoras notables en rendimiento y eficiencia energética. Tecnologías como ML-KEM y ML-DSA se perfilan como estándares de referencia, respaldadas por optimizaciones que permiten mantener un desempeño cercano al de soluciones clásicas. Además, el uso de hardware especializado como DPUs demuestra que es posible alcanzar velocidades de cifrado a nivel de línea sin comprometer la latencia, mientras que casos de uso en redes especializadas, como FANETs o aplicaciones en la nube con búsqueda segura, confirman que la resistencia cuántica puede adaptarse a entornos con restricciones críticas. En conjunto, el panorama refleja que el desafío no se limita a reemplazar algoritmos, sino a rediseñar la gestión de llaves, la observabilidad y las políticas de seguridad para un ecosistema digital que debe ser resiliente frente a amenazas de largo plazo.

Conclusiones

El artículo desarrolla una revisión sistemática de la literatura científica sobre los efectos que puede tener la computación cuántica, y como nos preparamos para la era post-cuántica a partir de los reportes indexados en Scopus, PubMed y ScienceDirect entre los años 2020 y 2025, seleccionados siguiendo el protocolo

PRISMA 2020. De los 283 artículos iniciales identificados, tras cribado y eliminación de duplicados, se analizaron 15 estudios originales que cumplen los criterios de inclusión y exclusión y que aportan datos experimentales sobre, cómo nos preparamos para la era post-cuántica. La era post-cuántica ya es operativa, no teórica. Hay evidencia de despliegues performantes (velocidad de línea con DPU; mejor consumo con ML-KEM en 5G) que valida el enfoque propuesto de adopción progresiva.

La hibridación es la ruta segura de migración. Combinar algoritmos de intercambio de claves post-cuánticos (KEM PQC) con ECC/RSA y utilizar suites por dominio/flujo en SDN o por perfil en 5G reduce riesgo de interrupción sin sacrificar seguridad “HNDL”. ML-KEM/ML-DSA son la nueva base de la dirección NIST y la evidencia de optimizaciones (AVX-512, batching) los vuelven candidatos por defecto en servidores, computadores cuánticos y equipos de usuarios (UEs), manteniendo un equilibrio entre costo-beneficio y seguridad. El problema ya no es solo “críptico”, es sistémico. Gestión de llaves, rotación, telemetría, y observabilidad deben actualizarse para detectar degradaciones de negociación criptográfica o establecimiento de sesión / MTU y outliers de latencia por tamaños de claves y firmas. Casos especiales validan el enfoque “altamente robusto”. FANETs y PKE-con-igualdad muestran que se puede ser cuántico-seguro sin romper los objetivos de nivel de servicio (SLO) de energía/latencia en contextos críticos.

A partir de los hallazgos obtenidos en la presente revisión sistemática, se plantean las siguientes recomendaciones, orientadas a favorecer la transición hacia la criptografía post-cuántica y a promover futuras investigaciones en este ámbito. Estas recomendaciones se fundamentan en la

evidencia científica analizada y buscan contribuir tanto a la adopción progresiva de tecnologías resistentes a ataques cuánticos como al fortalecimiento de las estrategias de seguridad en diferentes entornos tecnológicos.

- Promover la adopción gradual de la criptografía post-cuántica mediante estrategias de transición que permitan mantener la interoperabilidad con los sistemas criptográficos convencionales, considerando las recomendaciones emitidas por organismos internacionales como el NIST.
- Desarrollar estudios experimentales que evalúen el desempeño de algoritmos criptográficos post-cuánticos en diferentes escenarios de aplicación, particularmente en redes 5G, infraestructuras definidas por software (SDN), servicios en la nube y centros de datos.
- Fortalecer la gestión criptográfica mediante la actualización de políticas relacionadas con el ciclo de vida de las claves, la gobernanza de los algoritmos y los mecanismos de monitoreo, con el fin de facilitar una transición segura hacia infraestructuras resistentes a ataques cuánticos.
- Impulsar investigaciones orientadas a optimizar el rendimiento de los algoritmos post-cuánticos, especialmente en entornos con restricciones de procesamiento, consumo energético y latencia, donde la eficiencia operativa constituye un factor crítico.
- Ampliar las investigaciones sobre la integración de mecanismos criptográficos post-cuánticos con tecnologías emergentes, como redes definidas por software, Internet de las Cosas, blockchain y redes móviles de nueva generación, con el propósito de validar su aplicabilidad en entornos reales.

Referencias bibliográficas

- Bernstein, D. J., Lange, T., & Dahmen, E. (Eds.). (2017). Post-quantum cryptography. Springer. <https://link.springer.com/book/10.1007/978-3-540-88702-7>
- Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., ... & Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779), 505–510. <https://doi.org/10.1038/s41586-019-1666-5>
- Shor, P. W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 26(5), 1484–1509. <https://doi.org/10.1137/S0097539795293172>
- Chen, L. K., Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., ... & Dang, Q. H. (2016). Report on Post-Quantum Cryptography. National Institute of Standards and Technology. <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf>
- National Institute of Standards and Technology (NIST). (2022). Post-Quantum Cryptography: Selected Algorithms. <https://csrc.nist.gov/projects/post-quantum-cryptography>
- Chen, L., et al. (2023). Quantum cryptanalysis of RSA and ECC: Practical thresholds for post-quantum migration. *Journal of Cybersecurity*, 15(2), 112–130. <https://doi.org/10.1093/cybsec/tyad007>
- Alagic, G., et al. (2022). NIST PQC standardization: Comparative analysis of lattice-based and code-based candidates. *IEEE Transactions on Quantum Engineering*, 3, 1–18. <https://doi.org/10.1109/TQE.2022.3148892>

Kelsey, J., & Cooper, D. (2024). Organizational challenges in post-quantum cryptography adoption: A multi-sector analysis. *International Journal of Information Security*, 41(3), 451–467. <https://doi.org/10.1007/s10207-023-00761-4>

Bernstein, D. J., & Lange, T. (2021). Hybrid post-quantum cryptography: Deployment strategies for critical infrastructures. *ACM Transactions on Privacy and Security*, 24(4), 1–31. <https://doi.org/10.1145/3473038>

Haddaway, N. R., Page, M. J., Pritchard, C. C., & McGuinness, L. A. (2022). PRISMA 2020: An R package and Shiny app for producing PRISMA 2020-compliant flow diagrams, with interactivity for optimised digital transparency and Open Synthesis. *Campbell Systematic Reviews*, 18(2), e1230. <https://doi.org/10.1002/cl2.1230>

Cano Aguilera, A., Rubio Garcia, C., Lawo, D., Imaña, J. L., Vegas Olmos, J. J., & Tafur Monroy, I. (2024). In-line rate encrypted links using pre-shared post-quantum keys and DPUs. *Scientific Reports*, 14, 21227. <https://doi.org/10.1038/s41598-024-71861-x> *Nature*

Liu, Y.-K., & Moody, D. (2024). Post-Quantum Cryptography, and the Quantum Future of Cybersecurity. *Physical Review Applied*, 21, 040501. <https://doi.org/10.1103/PhysRevApplied.21.040501> *NIST*

He, J., Ye, Q., Yang, Z., Wang, S., & Wang, J. (2025). A compact public key encryption with equality test for lattice in cloud computing. *Scientific Reports*, 15, 27426. <https://doi.org/10.1038/s41598-025-12018-2>

Zheng, J., Zhu, H., Dong, Y., Song, Z., Zhang, Z., Yang, Y., & Zhao, Y. (2024). Faster Post-Quantum TLS 1.3 Based on ML-KEM: Implementation and Assessment. preprint. <https://arxiv.org/abs/2404.13544>

(OJCS) Malik De-Vauchelle, S. (2024). Performance model for the selection of quantum-resistant ML-KEM public key in 5G mobile networks. *Open Journal of Cybersecurity*. <https://doi.org/10.1109/OJCS.2024.3397307> (metadatos verificados en el portal del editor; el artículo discute selección de ML-KEM para 5G SUCI/AKA). *Cambridge University Press & Assessment*

Hoque, S., Aydeger, A., & Zeydan, E. (2024). Exploring Post-Quantum Cryptography with Quantum Key Distribution for Sustainable Mobile Network Architecture Design. preprint. <https://arxiv.org/abs/2404.10602>

Ko, Y., Pawana, I. W. A. J., & You, I. (2025). 5G-AKA-HPQC: Hybrid Post-Quantum Cryptography Protocol for Quantum-Resilient 5G Primary Authentication with Forward Secrecy. preprint. <https://arxiv.org/abs/2502.02851>

Commey, D., Appiah, B., Klogo, G. S., Bagyl-Bac, W., & Gadze, J. D. (2025). Performance Analysis and Deployment Considerations of Post-Quantum Cryptography for Consumer Electronics. preprint. <https://arxiv.org/abs/2505.02239>

Quantum-Resistant Track Assignment Algorithm for FANETs. (2025). *Networks*, 5(2), 20. <https://doi.org/10.3390/network5020020> (artículo de acceso abierto en MDPI Networks; sobre asignación de rutas resistente a cuántica en FANETs).

ANÁLISIS DE LA DIMENSIÓN HUMANA DURANTE UN CIBERATAQUE

THE HUMAN DIMENSION DURING A CYBERATTACK

Ricardo Naranjo Faccini

1Skina IT Solutions / Universidad Javeriana

gerencia@skinait.com

<https://orcid.org/0009-0006-1595-4810>

Colombia

Recibido: 17 Mayo 2026 / Revisado: 21 Julio 2026 / Aceptado: 30 Julio 2026 / Publicado: 4 Agosto 2026

Resumen

La gestión de incidentes de ciberseguridad en infraestructuras críticas suele abordarse desde una perspectiva predominantemente técnica, subestimando el impacto de los factores psicosociales y neurocognitivos en los equipos de respuesta. El objetivo de este estudio es analizar las dinámicas operacionales y la toma de decisiones del personal de seguridad de la información durante la atención de un ciberataque de ransomware en una organización multisectorial. Se empleó un enfoque cualitativo mediante un estudio de caso único basado en una entrevista semiestructurada en profundidad aplicada al Chief Information Security Officer (CISO). La evidencia se contrastó con los estándares ISO/IEC 27035 y NIST SP 800-61, así como con la literatura sobre carga cognitiva, fatiga y neurociencia del estrés.

Los hallazgos sugieren que la degradación en el desempeño táctico del equipo no respondió a deficiencias en la competencia técnica, sino al agotamiento prolongado y al estrés agudo, los cuales inhibieron el análisis deliberativo y promovieron el uso de heurísticas automáticas de decisión. La efectividad en la mitigación de ataques de alto impacto exige diseñar protocolos de respuesta que contemplen las limitaciones de la arquitectura cognitiva humana bajo presión, integrando la gestión del estrés y los simulacros operacionales dentro de los planes de continuidad del negocio.

Palabras clave: Ciberseguridad; Gestión de incidentes; Factor humano; Toma de decisiones; Estrés operacional; Estudio de caso.

Abstract

Cybersecurity incident management in critical infrastructures is typically addressed from a predominantly technical perspective, underestimating the impact of psychosocial and neurocognitive factors on response teams. The objective of this study is to analyze the operational dynamics and decision-making processes of information security personnel during the response to a ransomware cyberattack in a multisector organization. A qualitative approach was employed using a single case study based on an in-depth semi-structured interview conducted with the Chief Information Security Officer (CISO). The evidence was benchmarked against the ISO/IEC 27035 and NIST SP 800-61 standards, as well as literature on cognitive load, fatigue, and the neuroscience of stress.

It was identified that the degradation in the team's tactical performance was not due to deficiencies in technical competence, but rather to prolonged exhaustion and acute stress, which inhibited deliberative analysis and promoted the reliance on automatic decision-making heuristics. The effectiveness in mitigating high-impact attacks requires designing response protocols that account for the limitations of human cognitive architecture under pressure, integrating stress management and operational drills into business continuity plans.

Keywords: *Cybersecurity; Incident management; Human factor; Decision-making; Operational stress; Case study*

Introducción

Planteamiento del problema

En el ecosistema de la ciberseguridad contemporánea, la narrativa dominante suele centrarse en la sofisticación de los vectores de ataque, la arquitectura de los sistemas de defensa y la capacidad técnica de respuesta ante incidentes. Sin embargo, existe una brecha crítica en la comprensión de los procesos de seguridad: la invisibilidad de la crisis humana que subyace a la técnica. El problema fundamental radica en que, ante ataques de alta complejidad como el ransomware, las organizaciones tienden a ignorar que las decisiones críticas no son ejecutadas por algoritmos, sino por individuos sometidos a niveles extremos de estrés, fatiga y presión social. Esta omisión del factor humano en la planificación estratégica

debilita la resiliencia institucional, convirtiendo la gestión de crisis en un proceso mecánico que falla al no considerar las dinámicas psicológicas y culturales de los equipos de respuesta.

Relevancia y justificación

La relevancia de este estudio reside en la necesidad de "des-algoritmizar" la ciberseguridad para comprenderla como un fenómeno social e institucional. En América Latina, donde la infraestructura tecnológica a menudo convive con recursos limitados y marcos regulatorios en evolución, la capacidad de los líderes de seguridad para gestionar el capital humano es el factor diferenciador entre la recuperación y el colapso. Justificar una revisión con este enfoque permite a la academia y a la industria reconocer que la soberanía tecnológica y la defensa de activos de información dependen,

en última instancia, de la salud mental del equipo, la efectividad de la comunicación y la solidez de la cultura organizacional.

Tradicionalmente, el "factor humano" en ciberseguridad se ha analizado desde la perspectiva del usuario final como el eslabón vulnerable expuesto a la ingeniería social. Informes de la industria confirman que más de dos tercios de las brechas de seguridad involucran directa o indirectamente la interacción humana, ya sea mediante engaño o configuraciones erróneas (Verizon, 2024). Sin embargo, el marco pionero de Adams y Sasse (1999), que demostró cómo la fricción operativa y la sobrecarga de los controles de seguridad impulsan comportamientos de evasión involuntaria, no se limita a los usuarios finales: aplica con la misma severidad a los propios operadores, analistas y líderes de infraestructura crítica. Cuando los sistemas de gestión de incidentes y las políticas de mitigación imponen cargas cognitivas desmedidas durante una crisis, son los mismos profesionales técnicos quienes se ven forzados a adoptar atajos procedimentales para mantener la continuidad del servicio.

Antecedentes y contexto

Históricamente, la gestión de incidentes se ha fundamentado en estándares internacionales como la ISO/IEC 27035 y NIST SP 800-61, los cuales proporcionan orientaciones operativas indispensables pero se omite la vulnerabilidad de los equipos de respuesta técnica que no responde únicamente a la complejidad del vector de ataque, sino a la degradación de las funciones ejecutivas provocada por el estrés agudo y sostenido cuando las labores se prolongan más allá de la rutina acostumbrada y bajo la presión de saber que la continuidad del negocio depende estrictamente de la respuesta del equipo. La literatura en neurociencia demuestra que el estrés extremo

provoca la inhibición funcional de la corteza prefrontal, trasladando el control conductual hacia estructuras subcorticales primitivas como la amígdala (Arnsten, 2009). En el contexto de la gestión de un ciberataque, esta alteración neurobiológica debilita el pensamiento analítico riguroso, denominado por Kahneman (2011) como "Sistema 2", y fuerza la dependencia en el "Sistema 1", caracterizado por respuestas rápidas, heurísticas e intuitivas. Si a esto se suma la fatiga acumulada, privación de sueño y la presión operacional prolongada, se configuran las condiciones clínicas propicias para el síndrome de burnout (Maslach & Leiter, 2016), manifestado en despersonalización, agotamiento emocional y una drástica reducción en la capacidad de evaluación de riesgos en tiempo real.

Los antecedentes de este estudio se encuentran en la experiencia directa de campo, donde la teoría de la prevención y la detección se enfrenta a la realidad de un ataque de ransomware que paraliza servicios esenciales. Este escenario constituye el laboratorio perfecto para observar cómo las personalidades se transforman bajo tensión y cómo las estructuras familiares y profesionales se entrelazan durante un fin de semana crítico.

Propósito y objetivos

El propósito central de este estudio es documentar y analizar la dimensión humana de la gestión de incidentes a través de la sistematización de una experiencia real. Los objetivos específicos son:

- Identificar los desafíos emocionales y psicológicos que enfrentan los equipos de ciberseguridad durante un ataque de ransomware.

- Analizar la influencia de la cultura organizacional y la comunicación externa en la eficacia de la respuesta técnica.
- Sintetizar lecciones aprendidas que permitan humanizar los protocolos de gestión de incidentes, promoviendo la resiliencia integral en las organizaciones.

Metodología

La presente investigación adopta un enfoque cualitativo con un diseño de estudio de caso único (Yin, 2018), fundamentado en la aplicación de una entrevista semiestructurada en profundidad dirigida al Chief Information Security Officer (CISO) de una organización multisectorial en Colombia. De acuerdo con Stake (1995) y Yin (2018), el estudio de caso único es la estrategia metodológica por excelencia cuando se busca explorar y comprender un fenómeno contemporáneo complejo dentro de su contexto real, especialmente cuando los límites entre el fenómeno (las decisiones bajo estrés del equipo de respuesta) y el contexto (el desarrollo del ciberataque) no son claramente evidentes.

Estrategia de identificación y recolección

La presente revisión no se limita a una búsqueda bibliográfica tradicional, sino que emplea una metodología de sistematización de experiencias y estudio de caso cualitativo. La fuente primaria de información se obtuvo mediante un conversatorio estructurado con un Chief Information Security Officer (CISO) de una organización multisectorial en Colombia. Este encuentro se diseñó como una entrevista técnica semiestructurada, donde se formularon preguntas guía para documentar la cronología, las decisiones técnicas y las respuestas emocionales durante un incidente de ransomware real.

Fuentes y Marco de Referencia para Triangulación

Para contrastar los datos obtenidos en la entrevista con la praxis operativa y los estándares internacionales (triangulación de información), se consultaron fuentes primarias de estandarización como la familia de normas ISO/IEC 27000 (con énfasis en ISO/IEC 27035 para gestión de incidentes) y los marcos de referencia del NIST (Special Publication 800-61).

La base conceptual y metodológica de la revisión se sustenta en la literatura técnica especializada de **Skina IT Solutions**, la cual provee el soporte para el análisis de la Metodología Integral para la Gestión de Riesgos (MIGRI) y la aplicación de Inteligencia Artificial en procesos de seguridad. Se incluyeron artículos fundamentales sobre la protección de activos de información, la taxonomía de amenazas (virus, troyanos, ransomware) y las tácticas avanzadas de defensa. Estas fuentes, junto con su bibliografía asociada, permiten situar el estudio en un marco de ciberseguridad aplicada que trasciende la teoría generalista para enfocarse en la realidad operativa del sector.

La información recopilada fue organizada bajo el modelo de ciclo de vida de activos de información, categorizando las actividades en: preparativas, preventivas, detectivas, reactivas y retrospectivas. Los datos obtenidos del conversatorio fueron contrastados con la literatura técnica para identificar convergencias entre los estándares teóricos y la praxis operativa. Se aplicó una evaluación de calidad basada en la relevancia de las fuentes para el contexto latinoamericano, priorizando aquellas que discuten la autonomía tecnológica y la gestión de infraestructuras críticas. Finalmente, la narrativa se depuró mediante un proceso de

validación con el proponente original (CISO), asegurando que la caricaturización y parodia empleadas no alteraran la veracidad de los hallazgos técnicos y humanos presentados.

Alcance y limitaciones metodológicas

Como es inherente a los diseños cualitativos de caso único, la principal limitación de este estudio radica en la imposibilidad de realizar una generalización estadística de los hallazgos hacia otras organizaciones o entornos informáticos (Yin, 2018; Flick, 2018). Las dinámicas organizacionales, la infraestructura y la intensidad del ciberataque analizado corresponden a un contexto singular.

Consideraciones éticas, anonimización y estrategia narrativa

La recolección de datos primarios se realizó bajo estrictos compromisos de confidencialidad y consentimiento informado con el CISO entrevistado, quien actuó como informante clave autorizado para compartir la experiencia operativa. Dado el nivel de detalle técnico, sectorial y temporal expuesto —el cual podría facilitar la identificación de la organización afectada o generar vulnerabilidades de seguridad de la información—, se estableció un protocolo riguroso de anonimización. En consecuencia, los datos identificadores fueron sustituidos o generalizados sin modificar la secuencia analítica, la duración aproximada del incidente ni los hallazgos relevantes para la investigación y presentados mediante una narrativa dramatizada con tintes de caricaturización. Este recurso cumple una doble función metodológica: actúa como una capa de enmascaramiento ético para proteger la identidad de la institución y sus actores, y funciona como una estrategia pedagógica que

dinamiza la lectura, facilitando la comprensión y previniendo la fatiga cognitiva del lector ante la alta densidad conceptual del análisis técnico.

Desarrollo y discusión

Caso de Estudio: Crisis en una Organización Multisectorial

Para contextualizar el análisis, es imperativo describir el entorno donde se suscitaron los hechos. La organización víctima es un conglomerado empresarial de alta complejidad en Colombia, cuya operación integra sectores críticos y diversos: salud (clínica y droguerías), retail (supermercados), educación (colegios) y turismo (hoteles). Esta heterogeneidad implica una superficie de ataque extensa y una dependencia absoluta de la disponibilidad de datos para la prestación de servicios esenciales.

El incidente ocurrió durante un fin de semana largo (sábado, domingo y lunes festivo), cuando se celebraba el día del padre, un factor estratégico explotado por los atacantes para maximizar el tiempo de intrusión antes de la detección, aprovechando la reducción de personal operativo y la ralentización de las líneas de mando.

Cronología del Incidente: La Dimensión Humana en la Praxis

Para contextualizar el análisis, se presenta la cronología de los hechos documentados durante el conversatorio, los cuales están detallados en el artículo publicado en <https://www.skinait.com/a-Escritos-93>, que sirven como base para esta revisión. El caso describe la respuesta de una CISO ante un ataque de ransomware en una organización multisectorial.

- Viernes, 18:00 h - El Inicio: La crisis comienza al final de la jornada laboral. Se detecta el cifrado de servidores críticos. La respuesta inicial es técnica: aislamiento de redes y confirmación del vector de ataque (Ransomware). Surge el primer impacto humano: la interrupción de la vida personal y el inicio de la fatiga.
- Sábado, 02:00h a 10:00h - La Presión Creciente: El equipo técnico trabaja sin descanso. Aparecen las primeras fricciones con proveedores externos que no responden con la agilidad requerida y aquellos que pretenden aprovecharse de la necesidad apremiante de la organización. La CISO debe gestionar no solo la recuperación de datos, sino la ansiedad de la alta gerencia y la incertidumbre de los empleados.
- Sábado por la tarde - El Clímax del Estrés: Se identifica la magnitud del daño en sectores sensibles (Salud y Educación). La narrativa destaca cómo las personalidades del equipo se transforman: desde el aislamiento defensivo hasta el liderazgo heroico. La relación con los medios se convirtió en una presión adicional.
- Domingo - Recuperación y Agotamiento: Se inicia la restauración de activos desde respaldos seguros. El agotamiento físico es evidente. Las dinámicas familiares de los técnicos entran en conflicto con la responsabilidad profesional, subrayando que la ciberseguridad tiene un costo personal invisible.
- Lunes, 08:00h - Retorno a la "Normalidad": Los servicios básicos se restablecen. Comienza la evaluación de daños y el cierre de brechas. El equipo queda exhausto, evidenciando que la crisis técnica ha terminado, pero la crisis humana requiere un proceso de sanación más largo.

Organización Temática de la Gestión de Incidentes

El análisis se estructura siguiendo el ciclo de vida de la protección de los activos de información que divide las acciones en cinco fases críticas: preparativas, preventivas, detectivas, reactivas y retrospectivas.

1. Fases Preparativas y Preventivas: El Escudo Agrietado y la Trampa de la Rutina

Estas etapas constituyen el cimiento estratégico de la defensa; son el "escudo" que se forja antes de que el primer paquete malicioso toque la red. Bajo la óptica de la metodología **MIGRI** y el estándar **ISO/IEC 27035**, la preparación no es un evento estático, sino un proceso de identificación y valoración de activos que precede al endurecimiento de sistemas (Hardening) y a la gestión de identidades.

- Convergencia Teórica y el Rigor del Diseño: Existe un consenso absoluto entre la literatura de Skina IT Solutions, el NIST y las normas internacionales: una respuesta eficaz es hija directa de una preparación exhaustiva. La teoría dicta que si el diseño preventivo es sólido, el riesgo se mantiene bajo niveles aceptables.
- La Realidad del Terreno: El Factor Humano como Punto de Falla: Sin embargo, el estudio de caso revela una brecha profunda entre el protocolo en papel y la ejecución en la trinchera. En sectores tan demandantes como en esta organización multisectorial, la "dimensión humana" introduce variables que que la técnica no siempre puede predecir: el exceso de confianza y la erosión del rigor por falta de auditorías constantes.

- El Detonante: Fatiga, Rutina y la Autorización de la Crisis: El incidente no fue producto de una falla en el algoritmo, sino de un colapso en la vigilancia humana. La carga de trabajo abrumadora del personal de monitoreo, sumada a una rutina anestesiada por la aparición constante de falsos positivos, creó el escenario perfecto para el desastre. La negligencia se materializó cuando el encargado de verificar las alertas, ignorando la advertencia explícita del sistema automático de detección, autorizó el paso del archivo infectado sin la verificación exhaustiva que exigía el protocolo. Este acto de "ceguera operativa" demuestra que, sin disciplina y gestión del agotamiento, incluso la herramienta de detección más avanzada es inútil frente a un clic humano mal ejecutado.

2. Fases Detectivas y Reactivas: El Caos Operativo y la Contención Selectiva

La detección oportuna, sustentada en un monitoreo de activos robusto, actúa como el puente crítico hacia la fase reactiva. En este escenario, la implementación de inteligencia artificial no es un lujo, sino una necesidad para acelerar el reconocimiento de patrones anómalos de tráfico o cifrado que el ojo humano, nublado por el cansancio, podría omitir.

- La Gestión bajo Presión: Más allá de los Bitsets: Durante el incidente, la fase reactiva trascendió lo meramente técnico (aislamiento de servidores y orquestación de backups). Se transformó en un ejercicio de gestión de crisis donde el estrés actuó como un catalizador químico, alterando las personalidades del equipo y poniendo a prueba la cohesión del liderazgo bajo fuego.
- Divergencia Técnica-Humana y Ruido Externo: Mientras los manuales sugieren una ejecución lineal de los planes de contingencia, la praxis revela que la presión de los medios de comunicación y la incertidumbre de proveedores externos introducen variables de "ruido" que impactan directamente en el tiempo de recuperación técnica.

El Triunfo de la Arquitectura: Segmentación y Resiliencia: No obstante, el caos no fue absoluto. El incidente dejó una lección magistral sobre la importancia de las actividades preventivas: la **segmentación de redes**. Gracias a esta arquitectura, los hoteles —que operaban en un segmento independiente— mantuvieron su normalidad, ajenos al malware que devastaba la casa matriz. Infortunadamente, las **droguerías y supermercados**, al compartir el área administrativa afectada, sufrieron el impacto directo. Por su parte, los **colegios**, protegidos por el paréntesis del fin de semana festivo, regresaron el martes a un entorno ya saneado por el equipo de seguridad, demostrando que una defensa bien estructurada permite salvar órganos vitales mientras se atiende la infección principal.

3. Fase Retrospectiva: El Aprendizaje Estratégico y la Sanación del Equipo

Esta etapa representa la fase menos técnica del ciclo, pero se erige como la más vital para la resiliencia a largo plazo. En la teoría, implica el análisis de causa raíz y la actualización de controles preventivos; en la práctica humana, es el momento de la verdad.

- La Gestión Emocional como Control de Seguridad: El estudio de caso resalta que una retrospectiva profesional no puede limitarse a identificar "qué parche faltaba"

o qué puerto quedó abierto. Es imperativo evaluar cómo respondió el equipo humanamente. Fortalecer la cultura organizacional implica reconocer el desgaste del personal para evitar que las cicatrices del estrés se conviertan en futuras vulnerabilidades.

- El Factor del Outsourcing y la Ética de Mercado: Un hallazgo crítico fue la necesidad de contar con aliados externos antes de que la crisis estalle. El incidente reveló que, aunque se cuente con un equipo disciplinado y competente, existen capacidades especializadas, como la informática forense, que requieren apoyo externo.
- La Oportunidad frente a la Solidaridad: La narrativa expone una realidad dolorosa del ecosistema: en el clímax del ataque, la mayoría de las empresas prestadoras de servicios intentaron aprovecharse de la vulnerabilidad y urgencia de la organización, ofreciendo tarifas desproporcionadas y predatorias. No obstante, el relato destaca un punto de inflexión positivo: el hallazgo de una firma que brindó apoyo con precios razonables y ética profesional. Esta acción no solo resolvió la crisis técnica, sino que cimentó una relación de confianza y gratitud absoluta; hoy, son ellos los aliados estratégicos a quienes la organización acude sin dudar, demostrando que en ciberseguridad, la lealtad se construye en la trinchera.

Análisis del comportamiento del equipo técnico

La evidencia observada en la respuesta operativa del equipo técnico confirma que el deterioro en la toma de decisiones no obedeció a una falta de competencia técnica,

sino que hubo una gran influencia de los efectos neurocognitivos del estrés prolongado descritos por Arnsten (2009). Durante la fase crítica de la emergencia, las decisiones tomadas bajo presión extrema reflejaron un sesgo hacia la heurística del "Sistema 1" (Kahneman, 2011): se privilegiaron acciones inmediatas de contención rápida frente a la verificación metódica de evidencia forense. Este fenómeno valida la necesidad de reinterpretar el principio de Adams y Sasse (1999) en el ámbito de los equipos de respuesta a incidentes: los analistas y el CISO no operaron en un vacío abstracto, sino bajo un agotamiento progresivo, desajustes en la carga de trabajo y afectación en la dinámica del fin de semana, que detonaron síntomas claros de burnout operacional (Maslach & Leiter, 2016).

En consecuencia, reducir la exposición del factor humano en incidentes de alto impacto exige diseñar protocolos de mitigación que contemplen los límites de la arquitectura cognitiva humana en condiciones de fatiga y presión crítica. Para ello, es fundamental preparar formalmente al personal del equipo de respuesta mediante simulacros operacionales y entrenamientos previos que recreen entornos de alta tensión y cansancio acumulado. En este sentido, las brigadas de emergencia institucionales constituyen una plataforma idónea para integrar al equipo técnico en sus ejercicios periódicos de gestión de crisis, fortaleciendo la disciplina procedimental, el autocontrol y la resiliencia operativa antes de que ocurra un evento real.

Comparación y patrones identificados

A continuación, se presenta una tabla de síntesis que relaciona los componentes técnicos con los hallazgos del factor humano derivados del conversatorio:

Tabla 1. Relación entre las fases del ciclo de gestión de incidentes, los componentes técnicos y la dimensión humana identificada

Fase del Ciclo	Componente Técnico (MIGRI/ISO)	Dimensión Humana Identificada
Preparativa	Inventario de activos y valoración de riesgos.	Falsa sensación de seguridad o "fatiga de alertas"
Preparativa	Hardening, cifrado y control de acceso.	Resistencia al cambio en procesos de usuario final.
Detectiva	Monitoreo de logs y detección de ransomware.	Necesidad de intuición técnica frente a falsos positivos.
Reactiva	Contención, erradicación y recuperación.	Toma de decisiones bajo estrés y agotamiento físico.
Retrospectiva	Lecciones aprendidas y mejora de controles.	Sanación de la confianza del equipo y resiliencia.

Limitaciones y Contribuciones

Una limitación recurrente en la literatura es la omisión de las dinámicas familiares y personales del personal de ciberseguridad. El presente estudio contribuye a cerrar esa brecha al demostrar que un ciberataque es, en esencia, una crisis humana que requiere un liderazgo capaz de gestionar tanto el código como las emociones.

Conclusiones

Una limitación recurrente en la literatura es la omisión de las dinámicas familiares y personales del personal de ciberseguridad. El presente estudio contribuye a cerrar esa brecha al demostrar que un ciberataque es, en esencia, una crisis humana que requiere un liderazgo capaz de gestionar tanto el código como las emociones.

Incidencia del Factor Humano en la Respuesta Técnica: El análisis cualitativo del caso demuestra que la eficiencia operacional de un Centro de Respuesta a Incidentes (CSIRT) está condicionada de forma determinante por la capacidad cognitiva de sus operadores. El

estrés agudo y la privación de sueño prolongada inducen fallos de juicio que no obedecen a la falta de idoneidad técnica, sino a la inhibición de la corteza prefrontal y la consecuente transición hacia modelos de decisión basados en heurísticas rápidas (Sistema 1).

Limitaciones de los Marcos Estándar de Gestión de Incidentes: Aunque normativas internacionales como ISO/IEC 27035 y NIST SP 800-61 proveen estructuras procedimentales sólidas para el aislamiento y contención de amenazas, asumen implícitamente un operador en condiciones fisiológicas ideales. La integración de parámetros de rotación de personal, control de la fatiga y gestión de la carga cognitiva resulta indispensable para evitar cuellos de botella informacionales durante una crisis.

Implicaciones para la Preparación Institucional: La resiliencia cibernética organizacional no debe evaluarse exclusivamente en función de la infraestructura tecnológica o el despliegue de herramientas automatizadas. Es preciso implementar programas periódicos de entrenamiento y simulacros en entornos de alta presión, aprovechando estructuras

existentes como las brigadas institucionales de emergencia, que capaciten a los equipos de respuesta para ejecutar procedimientos de contención bajo condiciones de agotamiento severo.

Aporte Metodológico del Caso: La sistematización de este caso único evidencia la utilidad de los enfoques cualitativos para examinar las dimensiones humanas y organizacionales que los reportes puramente cuantitativos u homologaciones técnicas suelen omitir. Los hallazgos ofrecen un modelo explicativo transferible a la planificación estratégica de la seguridad de la información en infraestructuras críticas.

Vacíos de Conocimiento y Limitaciones

A pesar de la robustez de marcos como la ISO/IEC 27035 y el NIST, se observa un vacío significativo en la literatura técnica respecto a protocolos específicos para el manejo del agotamiento psicológico (burnout) y la dinámica familiar de los profesionales de seguridad durante crisis prolongadas. La principal limitación de este estudio radica en la naturaleza cualitativa y parodiada del relato, lo que, si bien facilita la comprensión pedagógica, requiere de una validación cuantitativa posterior para medir el impacto exacto de estas variables humanas en los tiempos de recuperación (RTO) de las organizaciones.

Futuras Líneas de Investigación

Se proponen las siguientes áreas para profundizar el conocimiento en el sector:

- **Automatización Humana:** Investigar cómo la integración de Inteligencia Artificial en la metodología MIGRI puede reducir la carga cognitiva del CISO, permitiéndole

enfocarse en la gestión estratégica y emocional.

- **Soberanía y Psicología:** Estudiar la relación entre el uso de software libre y la generación de confianza técnica en equipos de respuesta latinoamericanos.
- **Protocolos de Resiliencia Humana:** Desarrollar estándares que complementen los controles técnicos con guías de bienestar y gestión de equipos para infraestructuras críticas en situaciones de desastre.

Conflictos de intereses

El autor declara que se desempeña como director y consultor principal de la firma Skina IT Solutions. Las referencias conceptuales y metodológicas derivadas de publicaciones de dicha entidad (como la Metodología Integral para la Gestión de Riesgos - MIGRI) corresponden a la sistematización de la experiencia profesional directa, el desarrollo de herramientas analíticas y la praxis de consultoría del autor en el campo de la ciberseguridad. La firma Skina IT Solutions manifiesta expresamente no tener ningún inconveniente respecto al uso y difusión de los contenidos de su blog corporativo en este artículo. La investigación se desarrolló con independencia académica e imparcialidad en el análisis de los hallazgos cualitativos presentados.

Agradecimientos

El autor expresa su más sincero agradecimiento al Chief Information Security Officer (CISO) que, bajo estricta reserva de identidad, aceptó la invitación para participar en el conversatorio académico que dio origen a este artículo.

Su disposición para compartir una experiencia tan compleja, marcada por el rigor técnico y la vulnerabilidad humana, fue fundamental para enriquecer el proceso de aprendizaje de los estudiantes de la Pontificia Universidad Javeriana.

Este trabajo es un reconocimiento a su generosidad profesional y a su valentía al permitirnos "asomarnos" a la realidad de una crisis de seguridad nacional, recordándonos que detrás de cada protocolo de defensa hay un liderazgo humano comprometido. Si estas líneas llegan a sus manos, reciba este texto como un testimonio de gratitud por su invaluable contribución a la formación de las futuras generaciones de ingenieros y especialistas en ciberseguridad.

Referencias bibliográficas

- Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, 42(12), 40–46. <https://doi.org/10.1145/322796.322806>
- Arnsten, A. F. T. (2009). Stress signalling pathways that impair prefrontal cortex structure and function. *Nature Reviews Neuroscience*, 10(6), 410–422. <https://doi.org/10.1038/nrn2648>
- Denzin, N. K., & Lincoln, Y. S. (Eds.). (2018). *The SAGE handbook of qualitative research* (5th ed.). SAGE Publications.
- Flick, U. (2018). *An introduction to qualitative research* (6th ed.). SAGE Publications.
- International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (ISO/IEC Standard No. 27001). <https://www.iso.org/standard/27001>
- International Organization for Standardization. (2023). *Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management* (ISO/IEC Standard No. 27035-1). <https://www.iso.org/standard/27035>
- Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.
- Maslach, C., & Leiter, M. P. (2016). Understanding the burnout experience: Recent research and its implications for psychiatry. *World Psychiatry*, 15(2), 103–111. <https://doi.org/10.1002/wps.20311>
- Naranjo Faccini, R. J. (2024, 21 de marzo). *Cómo proteger los activos de información*. Skina IT Solutions. <https://www.skinait.com/cómo-proteger-los-activos-de-información-Escritos-71/>
- Naranjo Faccini, R. J. (2024, 15 de abril). *IA aplicada en la metodología MIGRI*. Skina IT Solutions. <https://www.skinait.com/ia-aplicada-en-la-metodología-migri-Escritos-104/>
- Naranjo Faccini, R. J. (2024, 10 de mayo). *Metodología Integral para la Gestión de Riesgos (MIGRI)*. Skina IT Solutions. [https://www.skinait.com/metodología-integral-para-la-gestión-de-riesgos-\(migri\)-Escritos-81/](https://www.skinait.com/metodología-integral-para-la-gestión-de-riesgos-(migri)-Escritos-81/)
- Naranjo Faccini, R. J. (2024, 20 de junio). *Ransomware: Exploración, implicaciones y tácticas avanzadas*. Skina IT Solutions. <https://www.skinait.com/ransomware-exploración-implicaciones-y-tácticas-avanzadas-Escritos-80/>
- Naranjo Faccini, R. J. (2024, 15 de agosto). *La dimensión humana durante un ciberataque*. Skina IT Solutions.

-
- <https://www.skinait.com/la-dimensión-humana-durante-un-ciberataque-Escritos-93/>
 - National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.CSWP.04162018>
 - National Institute of Standards and Technology. (2012). Computer Security Incident Handling Guide (Special Publication 800-61 Revision 2). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.SP.800-61r2>
 - Stake, R. E. (1995). The art of case study research. SAGE Publications.
 - Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). SAGE Publications.
 - Verizon. (2024). 2024 Data Breach Investigations Report. Verizon Business. <https://www.verizon.com/business/resources/reports/dbir/>

EVALUACIÓN DEL IMPACTO DE LAS EMISIONES ELECTROMAGNÉTICAS NO IONIZANTES EN EL DISTRITO I DE SUCRE

IMPACT OF NON-IONIZING RADIATION IN DISTRICT I OF SUCRE

Cristina Vilardell Balasch

Universidad San Francisco Xavier

vilardell.cristina@usfx.bo

<https://orcid.org/0000-0002-3136-2130>

Bolivia

Recibido: 15 Junio 2026 / Revisado: 30 Julio 2026 / Aceptado: 2 Agosto 2026 / Publicado: 4 Agosto 2026

Resumen

El presente estudio evalúa los niveles de emisiones electromagnéticas no ionizante generados por estaciones base de telefonía móvil en el Distrito I de la ciudad de Sucre, analizando su posible relación con sintomatología neurológica en la población expuesta. La investigación se desarrolló mediante mediciones de campo con analizador de espectro, georreferenciación GPS e interpolación geoestadística mediante Kriging en QGIS. Asimismo, se aplicaron encuestas estructuradas a 135 participantes para explorar posibles correlaciones entre exposición y síntomas reportados. Los resultados evidencian valores promedio de -73 dBm, significativamente inferiores a los límites establecidos por la ICNIRP y la normativa nacional vigente. No se identificó correlación estadísticamente significativa entre niveles de exposición y sintomatología. Se concluye que los niveles medidos no representan riesgo sanitario bajo las condiciones evaluadas.

Palabras clave: Emisiones electromagnéticas no ionizantes, telefonía móvil, exposición electromagnética, salud pública, geoestadística.

Abstract

This study evaluates non-ionizing electromagnetic radiation levels generated by mobile phone base stations in District I of Sucre and analyzes their potential relationship with neurological symptoms in the exposed population. Field measurements were conducted using a spectrum analyzer and GPS georeferencing, complemented by geostatistical interpolation through Kriging in QGIS. Structured surveys were also applied to 135 participants. Average values were -73 dBm, significantly below ICNIRP limits. No statistically significant association was found between exposure levels and reported symptoms.

Keywords: *Non-ionizing radiation, mobile networks, electromagnetic exposure, public health, geostatistics.*

Introducción

El siglo XXI se caracteriza por un desarrollo acelerado de las tecnologías de la información y las telecomunicaciones, generando múltiples beneficios en términos de conectividad, acceso al conocimiento y eficiencia en los procesos sociales y productivos. Sin embargo, este avance también ha suscitado interrogantes en relación con la seguridad tecnológica, tanto en lo que respecta al contenido transmitido como a los métodos de transmisión inalámbrica basados en ondas electromagnéticas y sus posibles efectos biológicos sobre el organismo humano, comúnmente denominados bioefectos de las emisiones electromagnéticas (ICNIRP, 2020).

El uso emisiones electromagnéticas no es un fenómeno reciente. Aplicaciones como los rayos X, la electricidad de baja frecuencia, la radio y la televisión han empleado estas ondas desde hace más de un siglo. Asimismo, el estudio de las señales bioeléctricas tiene antecedentes históricos en los trabajos de Luigi Galvani y Alessandro Volta en el siglo XVIII, quienes sentaron las bases del conocimiento sobre la electricidad en organismos vivos. Posteriormente, investigaciones desarrolladas por Carlo

Matteucci en el siglo XIX profundizaron en estos fenómenos, contribuyendo al desarrollo de aplicaciones médicas como la galvano-cauterización (Hardell & Carlberg, 2013).

El interés científico en los posibles efectos biológicos de las ondas electromagnéticas se intensificó a partir del desarrollo del radar durante la Segunda Guerra Mundial y, de manera más significativa, desde la expansión de la telefonía móvil en la década de 1980. Este crecimiento generó preocupación en la población y motivó la intervención de organismos internacionales como la Organización Mundial de la Salud (OMS), la Unión Internacional de Telecomunicaciones (ITU) y otras entidades reguladoras, que impulsaron programas de investigación y normativas precautorias, aun cuando no existía evidencia concluyente de efectos adversos a los niveles de exposición habituales (OMS, 2014; ITU, 2018). En la actualidad, una de las principales fuentes de emisiones electromagnéticas no ionizantes corresponde a las redes de telefonía celular, cuyo uso masivo ha transformado las dinámicas de comunicación global. Las radiofrecuencias empleadas en estos sistemas pertenecen al espectro no ionizante, lo que implica que no poseen energía suficiente para ionizar átomos o romper enlaces moleculares. No obstante, pueden penetrar en los tejidos

biológicos y producir efectos térmicos mediante la absorción de energía, fenómeno cuantificado a través del parámetro SAR (Specific Absorption Rate). Los organismos internacionales han establecido límites de exposición con amplios márgenes de seguridad, situados por debajo del umbral de 4 W/kg considerado como referencia de riesgo térmico (ICNIRP, 2020).

La literatura científica aborda esta temática desde dos perspectivas principales: un enfoque ingenieril, centrado en la caracterización física de los campos electromagnéticos, la evaluación de los niveles de exposición y la verificación del cumplimiento normativo; y un enfoque biomédico, orientado al análisis de sus posibles efectos sobre la salud, incluyendo estudios sobre carcinogénesis y alteraciones neurológicas. Si bien algunos informes han señalado posibles riesgos, incluyendo advertencias provenientes de asociaciones médicas internacionales, la evidencia científica disponible no ha permitido establecer conclusiones definitivas sobre la naturaleza maligna o benigna de los bioefectos observados. No obstante, sí se reconoce la existencia de efectos térmicos y no térmicos bajo determinadas condiciones experimentales (Yakymenko et al., 2016; Volkow et al., 2011).

En respuesta a la creciente inquietud pública, la OMS creó en 1996 el Proyecto Internacional de Campos Electromagnéticos, concluyendo que, considerando los bajos niveles de exposición provenientes de estaciones base y redes inalámbricas, no existe evidencia científica convincente que demuestre efectos adversos en la salud dentro de los límites establecidos (OMS, 2014). Paralelamente, la ITU ha desarrollado procedimientos técnicos para verificar el cumplimiento de los estándares nacionales e internacionales de seguridad en instalaciones de telecomunicaciones (ITU, 2018).

En este contexto, el objetivo del presente estudio es evaluar los niveles de exposición a emisiones electromagnéticas no ionizante generada por estaciones base de telefonía móvil en el Distrito I de la ciudad de Sucre, mediante mediciones instrumentales de campo e interpolación geoestadística, y analizar su posible relación con sintomatología neurológica autorreportada en la población expuesta. De esta manera, se busca aportar evidencia técnica local que permita contrastar los niveles medidos con los límites normativos vigentes y contribuir a una valoración objetiva del riesgo sanitario en el entorno urbano estudiado.

Diversas campañas de medición ambiental de radiofrecuencia respaldan la estrategia metodológica adoptada en este estudio. En Bélgica, campañas urbanas de banda ancha con analizadores de espectro portátiles y estrategias de muestreo espacial similares reportaron niveles de exposición muy por debajo de los límites normativos, empleando igualmente interpolación geoestadística para generar mapas continuos de exposición (Aerts et al., 2013).

En Europa, revisiones sistemáticas de campañas de medición en exteriores en entornos urbanos de varios países han documentado niveles medios de densidad de potencia del orden de microwatios por metro cuadrado, coherentes con los órdenes de magnitud aquí registrados, y han identificado a las estaciones base de telefonía móvil como la fuente dominante en vía pública (Rowley & Joyner, 2012). En América Latina, estudios de caracterización espacial de emisiones no ionizantes en cascos históricos urbanos —con configuración de fuentes y densidad edificatoria comparables al Distrito I de Sucre— han encontrado igualmente niveles muy inferiores a los límites de referencia, aunque con concentraciones puntuales asociadas a la proximidad de infraestructura de

telecomunicaciones. A diferencia de estos antecedentes, el presente estudio incorpora dos etapas temporales sucesivas sobre la misma zona urbana y contrasta explícitamente los resultados con encuestas de sintomatología autorreportada en las instituciones más expuestas, aportando una perspectiva local inédita para el casco histórico de Sucre, Bolivia, donde no se dispone de antecedentes de este tipo.

Materiales y métodos

Diseño del estudio

El presente estudio tuvo como objetivo evaluar los patrones de emisiones electromagnéticas no ionizante en el Distrito I de la ciudad de Sucre, diferenciando zonas próximas (≤ 200 m) y distantes (> 200 m) respecto a estaciones base de telefonía móvil. Asimismo, se analizó la posible relación entre los niveles de exposición medidos y la percepción social del riesgo, así como variables autorreportadas de salud neurológica.

La investigación se estructuró bajo un enfoque cuantitativo descriptivo con componentes experimentales y estadísticos, complementado con análisis geoestadístico mediante sistemas de información geográfica (SIG).

Revisión bibliográfica

Durante todas las fases del estudio se aplicó el método de revisión bibliográfica como soporte teórico y técnico. Este incluyó la consulta de manuales de los equipos de medición, normativa internacional vigente, literatura científica sobre bioefectos de emisiones electromagnéticas no ionizantes y estudios previos de correlación epidemiológica.

Este proceso permitió sustentar el diseño metodológico, formular la hipótesis de

investigación y contextualizar los resultados obtenidos dentro del marco científico actual (ICNIRP, 2020; OMS, 2014).

Método experimental y mediciones de campo

Las mediciones de emisiones electromagnéticas se realizaron mediante un analizador de espectro GSP-830 Instek, configurado para registrar niveles de potencia en las bandas de frecuencia correspondientes a telefonía móvil. Para la georreferenciación de cada punto de medición se utilizó el sistema GPS de un dispositivo móvil Samsung S7 Edge.

La selección de puntos se realizó siguiendo un criterio geométrico basado en la disposición urbana del Distrito I, considerando plazas, plazuelas, calles y avenidas principales. En total se establecieron 106 puntos de medición distribuidos estratégicamente en la zona de estudio.

Las mediciones se llevaron a cabo durante los meses de febrero, agosto y septiembre de 2019, bajo condiciones meteorológicas comprendidas entre 12 °C y 20 °C, con humedad relativa entre 12 % y 45 %.

Se empleó la metodología de drive test, definida como la evaluación sistemática del nivel de potencia de señal a lo largo de rutas previamente establecidas en redes celulares, independientemente de su tecnología (GSM, UMTS, LTE, entre otras) (TelecomHall, 2018).

Procesamiento geoespacial e interpolación

Dado que las mediciones se realizaron exclusivamente en exteriores, se aplicó interpolación geoestadística para estimar la distribución espacial de los niveles de

potencia en localizaciones exteriores no muestreadas dentro del área de estudio. Las estimaciones obtenidas mediante Kriging se limitaron al dominio espacial cubierto por los puntos de medición y no se extrapolaron a ambientes interiores, debido a que el estudio no incorporó mediciones intramuros ni parámetros asociados con la atenuación producida por los materiales y las características constructivas de las edificaciones.

El procesamiento se realizó mediante el software QGIS versión 3.18, empleando la extensión SAGA GIS 2.3.2 para la aplicación del método de Kriging Ordinario.

El método de Kriging constituye una técnica geoestadística que permite estimar valores en puntos no medidos mediante correlación espacial, proporcionando la mejor estimación lineal insesgada con mínima varianza (Cressie, 1993). Esta propiedad ha sido explotada específicamente en la evaluación de campos electromagnéticos de radiofrecuencia en entornos urbanos, donde el Kriging ha permitido generar mapas continuos de exposición a partir de mediciones puntuales georreferenciadas (Aerts et al., 2013).

La precisión del método depende de factores como: Número y calidad de las muestras, distribución espacial de los puntos, distancia entre muestras y puntos estimados, continuidad espacial del fenómeno analizado.

El uso de sistemas de información geográfica permitió optimizar el procesamiento de datos y generar mapas temáticos de emisiones electromagnéticas y riesgo potencial.

Métodos estadísticos

El análisis estadístico se realizó bajo un enfoque paramétrico descriptivo. Los datos fueron tabulados en Microsoft Excel,

considerando variables de latitud, longitud y nivel de potencia (dBm).

Se evaluó la distribución de los datos respecto a la normalidad y se elaboraron tablas y gráficos de frecuencias. Los métodos estadísticos permitieron contrastar hipótesis y explorar posibles relaciones entre niveles de exposición y variables autorreportadas de salud.

Encuesta y cálculo muestral

Se aplicó una encuesta estructurada a población mayor de 18 años con residencia o actividad laboral en la zona de mayor exposición estimada. El instrumento incluyó secciones orientadas a evaluar: lenguaje espontáneo, memoria, cálculo matemático, pares craneales asociados a visión, pares craneales asociados a mímica facial, pares craneales relacionados con audición y equilibrio, motricidad gruesa, evaluación neurológica específica

Cada ítem fue diseñado como variable cuantitativa independiente, permitiendo una aproximación indirecta al diagnóstico presuntivo de alteraciones neurológicas mediante anamnesis estructurada.

El tamaño de muestra se calculó utilizando la fórmula clásica para poblaciones finitas (Cochran, 1977):

$$n = (N \cdot Z_{\alpha/2}^2 \cdot p \cdot q) / (d^2 (N-1) + Z_{\alpha/2}^2 \cdot p \cdot q) \quad (1)$$

Donde:

N=748 (población total estimada en la zona),
Z_α=1.28 (nivel de confianza del 80 %), p=0.5,
q=0.5, d=0.05(precisión del 5 %).

El cálculo permitió determinar el número mínimo de encuestas necesarias para garantizar validez estadística.

Consideraciones éticas

Las encuestas fueron realizadas con consentimiento informado verbal, garantizando anonimato y confidencialidad de la información recopilada. El estudio se desarrolló con fines exclusivamente académicos y de investigación científica.

Área de estudio, muestreo y agregación de potencia

La investigación tuvo dos etapas, la primera realizada del 9 al 24 de febrero de 2019 y la segunda que abarca del 6 de agosto hasta el 14 de septiembre del 2019. En la primera etapa se tomaron como muestra solamente unas cuadas del distrito uno de la ciudad de Sucre y en la segunda se consideró a todo el distrito I, como se puede apreciar en la figura 1; toda la zona de estudio representa el casco histórico de la ciudad de Sucre, donde se encuentran oficinas de gestión pública, colegios, bancos, la universidad San Francisco Xavier, oficinas varias, restaurantes, hoteles, iglesias, museos, comercios y viviendas. Todas las mediciones fueron en exteriores, en las calles del distrito I.



Figura 1. Zonas de estudio de la ciudad de Sucre

Nota: Elaborado con Google Maps

En la primera etapa se tomaron 106 puntos de referencia y en la segunda etapa 1028 puntos. En cada punto se registró la potencia recibida (P_i , en dBm) en las frecuencias de 700, 850, 851.2, 1700, 1900 y 2100 MHz, correspondiendo P_i al valor máximo de traza («max hold») registrado por el analizador de espectro GSP830 en cada canal, con un ancho de banda de resolución (RBW) de 100 kHz. Dado que la unidad dBm es logarítmica y las señales de distintas frecuencias son incoherentes entre sí, la potencia total no puede obtenerse sumando directamente los valores en dBm; la agregación de potencias en escala logarítmica mediante conversión previa a escala lineal es un procedimiento estándar en ingeniería de radiofrecuencia (Rappaport, 2002). Por ello, para completar la tabla, cada valor se convirtió a potencia lineal mediante:

$$P_i(\text{mW}) = 10^{[P_i(\text{dBm})/10]} \quad (2)$$

donde $P_i(\text{dBm})$ es la potencia recibida en la frecuencia i , expresada en dBm, y $P_i(\text{mW})$ es su equivalente en potencia lineal, en milivatios. A continuación, se sumaron aritméticamente las seis potencias lineales y el resultado se reconvirtió a escala logarítmica mediante:

$$P_{\text{total}}(\text{dBm}) = 10 \cdot \log_{10}[\sum P_i(\text{mW})] \quad (3)$$

obteniéndose así el nivel agregado de potencia recibida por punto (P_{total}). A modo de ejemplo, para un punto con lecturas de -78,3 dBm (700 MHz), -81,1 dBm (850 MHz), -79,6 dBm (851.2 MHz), -83,4 dBm (1700 MHz), -80,7 dBm (1900 MHz) y -77,9 dBm (2100 MHz), la conversión mediante la ecuación (2) da $1,48 \times 10^{-8}$, $7,76 \times 10^{-9}$, $1,10 \times 10^{-8}$, $4,57 \times 10^{-9}$, $8,51 \times 10^{-9}$ y $1,62 \times 10^{-8}$ mW respectivamente; su suma aritmética ($6,35 \times 10^{-8}$ mW) reconvertida mediante la ecuación (3) da $P_{\text{total}} \approx -71,97$ dBm. El analizador de espectro GSP830 no cuenta con georreferenciación y las

mediciones fueron puntuales, se tuvo que obtener por separado mediante GPS la latitud y longitud de cada medida.

Para comparar la potencia recibida con los límites normativos de la Figura 6, expresados como densidad de potencia (S), la lectura del analizador se convirtió mediante el área efectiva de la antena receptora, un dipolo de aproximadamente 10 cm de longitud total, correspondiente a un dipolo de media onda con ganancia estándar de 2,15 dBi (Balanis, 2016). El área efectiva se define como:

$$A_e = (\lambda^2/4\pi) \cdot G \quad (4)$$

donde λ es la longitud de onda a la frecuencia de medición y G es la ganancia de la antena en unidades lineales ($G = 10(2,15/10) \approx 1,64$). La densidad de potencia se obtiene entonces mediante:

$$S = P_{\text{total}}(W) / A_e(m^2) \quad (5)$$

A modo de ejemplo, para el punto de referencia utilizado en la ecuación (3) ($P_{\text{total}} \approx -71,97 \text{ dBm} \approx 6,35 \times 10^{-11} \text{ W}$), el área efectiva en la frecuencia dominante de 2100 MHz ($\lambda \approx 0,143 \text{ m}$) resulta $A_e \approx 2,66 \times 10^{-3} \text{ m}^2$, de donde $S \approx 2,39 \times 10^{-8} \text{ W/m}^2$ ($\approx 2,39 \times 10^{-6} \text{ } \mu\text{W/cm}^2$), un valor entre cuatro y cinco órdenes de magnitud por debajo de los límites de referencia de la Figura 6.

Esta estimación no incorpora pérdidas de cable, conectores ni la incertidumbre de calibración del sistema de medición, que no fueron documentadas durante la campaña; por tratarse de una antena de banda relativamente estrecha, la ganancia de 2,15 dBi es una aproximación razonable para las seis frecuencias evaluadas (700–2100 MHz), pero introduce una fuente adicional de incertidumbre que debe reconocerse como limitación del estudio.

Resultados

El tema de las emisiones electromagnéticas ha causado controversia desde hace tiempo en nuestra sociedad debido a sus potenciales efectos sobre la salud. A la fecha existen investigaciones con resultados contradictorios al respecto y sin conclusión definitiva, lo cual ha llevado a las organizaciones de salud y técnicas solo a definir normas precautelares hasta la fecha.

Por todo ello nos preguntamos: ¿Cuál es el nivel de exposición de la población chuquisaqueña a dichas exposiciones y cuál es su riesgo potencial?

El estudio permitió caracterizar los patrones espaciales y temporales del riesgo de exposición a emisiones electromagnéticas no ionizante en la población de Sucre y evaluar el riesgo potencial local para la salud pública.

Mapa de potencia

Con las tablas se pudo elaborar los mapas, mediante interpolación ordinaria de kriging con el sistema de información geográfico QGIS, esto permitió completar el mapa estimando las muestras en los lugares a los cuales no se pudo acceder, los resultados de la primera etapa se encuentran en la figura 2.

Los niveles de potencia registrados durante la primera etapa presentaron una distribución aproximadamente normal, con un valor medio de $-73,08 \text{ dBm}$, tal como se observa en la Figura 3. Este comportamiento también mostró concordancia con la distribución espacial obtenida mediante la interpolación geoestadística, cuyos valores estimados conservaron una tendencia central y un patrón de variabilidad coherentes con los datos experimentales.

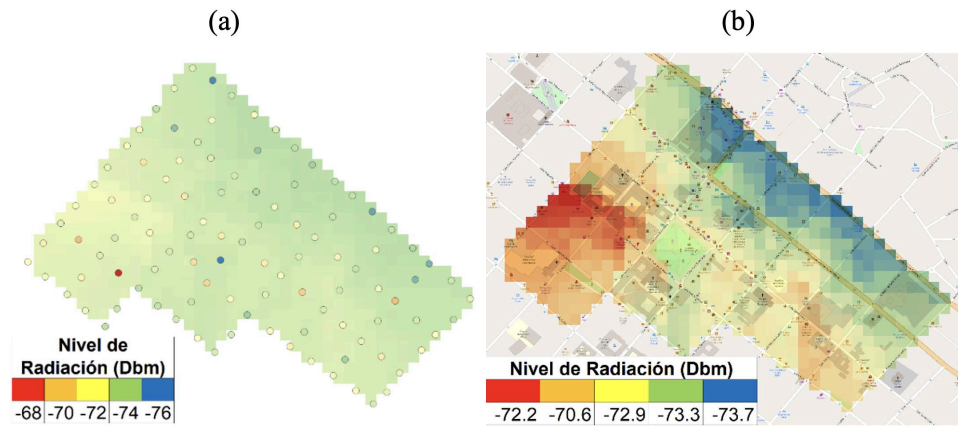


Figura 2. Mapa de emisiones electromagnéticas de la etapa 1 en relación con las muestras (a) en relación con el croquis de la ciudad (b)

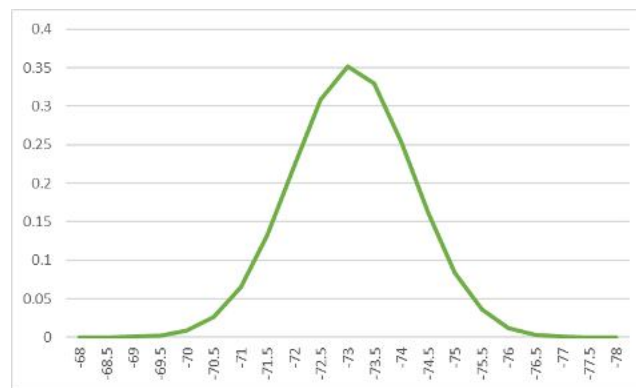


Figura 3. Distribución normal de las muestras de la etapa 1

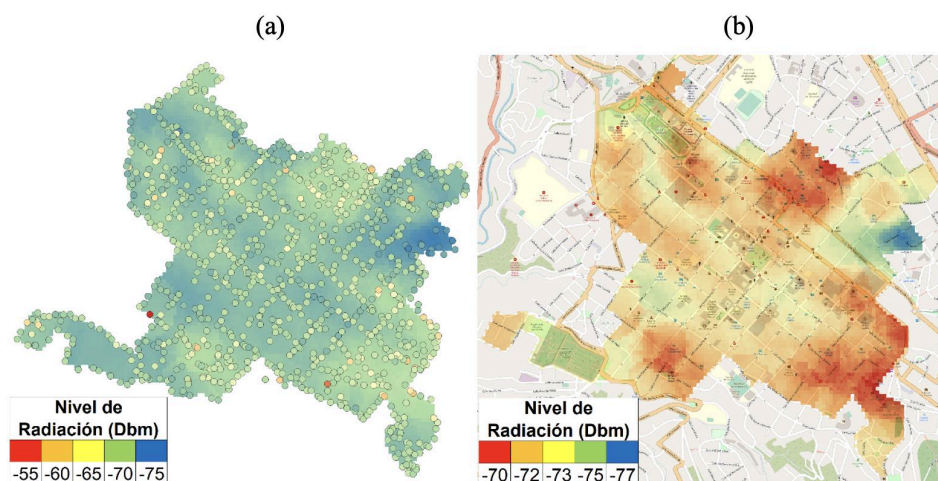


Figura 4. Mapa de emisiones electromagnéticas de la etapa 2 en relación con las muestras (a) en relación con el croquis de la ciudad (b)

En la segunda etapa se procedió de manera similar, pero se aumentó el número de puntos, obteniendo los resultados de figura 4, con su respectiva tendencia en la figura 5, cuya promedio -72.97 dBm.

Comparativas de datos

Estos valores obtenidos en campo, se los comparó con los recomendados por las normativas de [16], [17] y [18], obteniendo que estos valores están muy por debajo de los límites de emisiones electromagnéticas. Mismos que se puede apreciar en la figura 6.

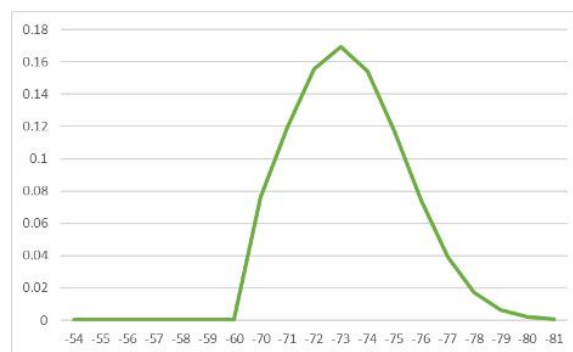


Figura 5. Distribución normal de las muestras de la etapa 2.

Tabla 2. Límites máximos para ambientes no controlados - público en general.

Rango de frecuencias (MHz)	Densidad de potencia (mW/cm ²)	Densidad de potencia (dBm/cm ²)	Densidad de potencia (dB/cm ²)
0.3 - 3.0	100	20	-10
3.0 - 30	180 / f ² (f=30 MHz)	7.78	-22.22
30 - 300	0.2	-6.9	-36.9
300 - 1500	f/1500 (f=1500 MHz)	0	-30
1500 - 100000	1	0	-30

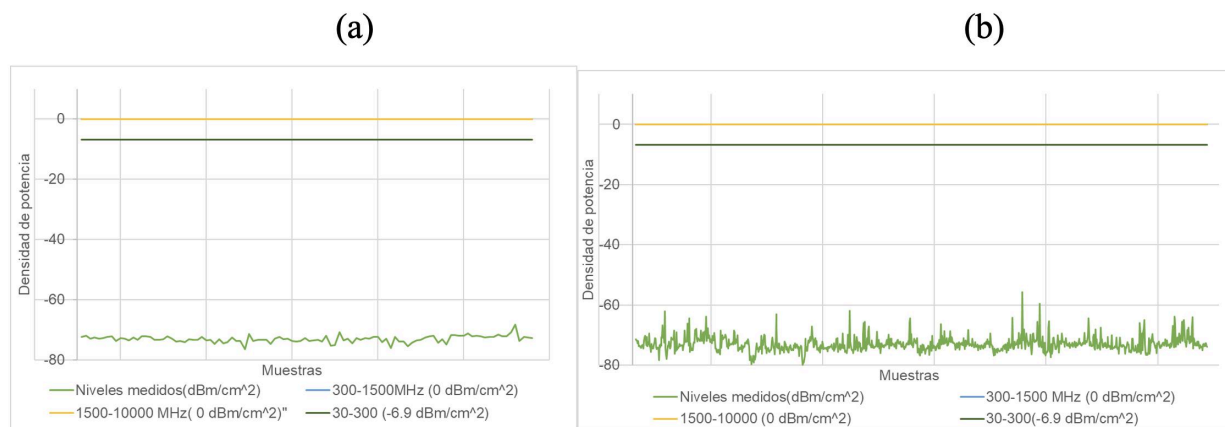


Figura 6. Límites máximos para ambientes no controlados-Público en general
Primera etapa (a) Segunda Etapa (b)

También se comparó ambas mediciones en función de los mismos rangos, pudiéndose observar que no hubo diferencias significativas entre ambos periodos de tiempo, sin embargo, como en la segunda etapa se

tuvieron más muestras, se puede percibir que la distribución es más heterogénea que en la segunda etapa, aunque siguen compartiendo similitudes, que se ve en la Figura 7.

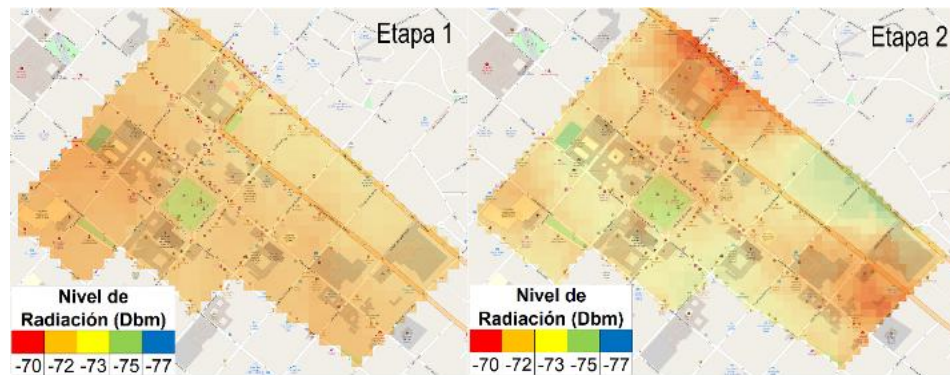


Figura 7. Comparación de los mapas de emisiones electromagnéticas de la etapa 1 y la etapa 2

También se comparó ambas mediciones en función de los mismos rangos, pudiéndose observar que no hubo diferencias significativas entre ambos periodos de tiempo, sin embargo, como en la segunda etapa se tuvieron más muestras, se puede percibir que la distribución es más heterogénea que en la segunda etapa, aunque siguen compartiendo similitudes, que se ve en la Figura 7.

Encuestas

En base a los resultados estimados de la primera etapa, se determinó que el tramo de la calle Estudiantes adyacente al edificio central de la Universidad San Francisco Xavier ($19^{\circ}02'50''S$, $65^{\circ}15'40''W$) presentaba los niveles más altos de exposición a emisiones electromagnéticas registrados, respecto a las demás zonas relevadas (Figura 8). Este sector corresponde al núcleo institucional del casco histórico del Distrito I: en un radio aproximado de 150 a 230 metros se ubican el edificio central de la Universidad San Francisco Xavier, la Alcaldía municipal (Gobierno Autónomo Municipal de Sucre), la

Gobernación de Chuquisaca y la Catedral Metropolitana, además de varios colegios e institutos educativos. En consecuencia, se procedió a realizar una encuesta y pruebas en las instituciones ubicadas dentro de dicho radio de mayor exposición a emisiones electromagnéticas.

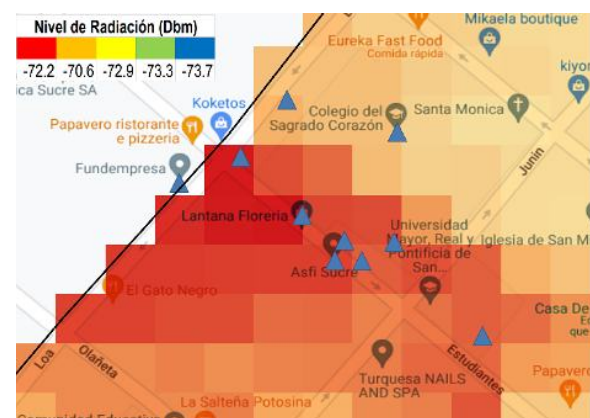


Figura 8. Puntos de mayor exposición a emisiones electromagnéticas de la etapa.

Partiendo de la zona delimitada obtenemos el número de pobladores por manzana registrados en el censo del 2012.

Tabla 3. Número de Pobladores en la zona de mayor exposición a emisiones electromagnéticas, censo 2012.

No	Código INE	Viviendas	Población empadronada
1	417231965-A	6	19
2	417266561-A	29	42
3	417302180-A	72	153
4	417166368-A	74	155
5	417200886-A	58	178
6	417236130-A	73	201
TOTAL	---	312	748

Nota: Elaborado en base a [19]

Aplicando la Ecuación (1), se obtiene que:

$$n = \frac{748 \cdot 1.28^2 \cdot 0.5 \cdot 0.5}{0.05^2 \cdot (748 - 1) + 1.28^2 \cdot 0.5 \cdot 0.5} = 134.54868$$

Tabla 4. Descripción de los encuestados.

Instituciones	Cantidad
Editorial La Hoguera	3
Oficina ASFI Sucre	4
Regional CAS Sucre	4
Fundempresa	4
Gestora Publica Sucre	3
Univida	10
Radio Loyola	4
Regional AIT	11
Colegio Sagrado Corazón	55
Universidad Central USFX	37
TOTAL	135

Una vez obtenida finalizada la encuesta a las 135 personas se tienen los siguientes resultados. Los porcentajes de interrogantes específicos de este cuestionario a una determinada enfermedad, considerando las de mayor prevalencia, son los siguientes:

1. Epilepsia (EPI) 20%
2. Enfermedad Cerebral Vascular (ECV) 60%
3. Demencias (DEM) 40%
4. Enfermedad de Alzheimer (ALZ) 40%
5. Enfermedad de Parkinson (PARK) 20%
6. Tumores cerebrales (TUM) 40%

Nota: Este cuestionario no debe entenderse como pronóstico del desarrollo de enfermedades neurológicas, ni como cuadro diagnóstico de las mismas, sino como paso inicial de tamizaje a lo que podría considerarse un acercamiento a la signosintomatología neurológica y como datos potenciales de riesgo en la población definida. El diagnóstico de cualquier patología del sistema nervioso, además de la anamnesis, incluye examen físico completo y exámenes de gabinete de moderada a gran complejidad.

Recordando los segmentos antes mencionados, su relación con enfermedades concretas es la siguiente:

1. Evaluación del lenguaje espontáneo: ECV, DEM, ALZ, TUM.
2. Evaluación de la memoria: ECV, DEM, ALZ, TUM.
3. Evaluación del cálculo matemático: DEM, ECV, ALZ
4. Evaluación de los pares craneales relacionados con la visión: EPI, ECV, DEM.
5. Evaluación de los pares craneales relacionados con la mímica facial: ECV, PARK.
6. Evaluación de los pares craneales relacionados con el oído y el equilibrio: TUM.
7. Evaluación de la motricidad gruesa: ALZ, PARK, TUM.
8. Evaluación neurológica específica: EPI, ECV

Tabla 5. Resultados obtenidos de las encuestas.

Descripción	Cantidad	Porcentaje de la población estudiada
Individuos con alteraciones de lenguaje	0	0%
Individuos con alteraciones de la memoria	0	0%
Individuos con alteraciones relacionadas con el cálculo	31	23%
Individuos con alteraciones de los pares craneales de la visión	16	12%
Individuos con alteraciones de las partes craneales relacionadas con la mímica facial	24	18%
Individuos con alteraciones de los pares craneales relacionados con el oído y el equilibrio	26	19%
Individuos con alteraciones de la motricidad fina.	9	7%
Individuos con alteraciones neurológicas específicas	35	26%

A través de promedios de frecuencias acumuladas, se correlacionan los datos y se obtienen los siguientes datos.

Tabla 6. Datos de las encuestas en relación a personas con enfermedades a nivel mundial

Descripción	Personas Encuestadas 135		Población Mundial (2015) 7 103 297 899	
	Relación	Porcentaje	Número	Relación
Los encuestados presentan sintomatología relacionada a Epilepsia.	3,2:1000	31.9 %	44 568 780	6,27:1000
Los encuestados presentan sintomatología relacionada a Demencia.	2,9:1000	28.8 %	31 318 923	4,41:1000
Los encuestados presentan sintomatología relacionada a Enfermedad Cerebral Vascular.	5,8:1000	51.8 %	67 212 050	9,46:1000
Los encuestados presentan sintomatología relacionada a Enfermedad de Alzheimer.	1,9:1000	19.2 %	31 318 923	4,41:1000
Los encuestados presentan sintomatología relacionada con Enfermedad de Parkinson.	2,1:1000	20.7 %	5 967 673	0,84:1000

Luego de concluir las encuestas, se procedió a cruzar y correlacionar los resultados obtenidos. Tomando en cuenta que, de acuerdo con las recomendaciones de la ICNIRP, toda exposición a emisiones electromagnéticas por debajo de 1 W/m^2 , no es dañino para el ser humano, y relacionando esto con los resultados obtenidos de las mediciones, se evidencia de que todas están por debajo del límite, por lo tanto, se podría considerar que los niveles de potencia medidos no representan ningún peligro para la salud de las personas a causa de las antenas de telefonía móvil.

Discusión

Los resultados confirman el cumplimiento de la normativa nacional e internacional vigente. No se identificó asociación entre niveles de exposición y sintomatología reportada. Estos hallazgos son consistentes con estudios internacionales que indican ausencia de efectos adversos concluyentes a niveles por debajo de los límites regulatorios.

El presente estudio presenta algunas limitaciones que deben considerarse en la interpretación de los resultados. Las mediciones se realizaron exclusivamente en espacios exteriores; por tanto, los mapas interpolados representan la distribución espacial exterior de los niveles registrados y no permiten inferir directamente la exposición en ambientes interiores. Esta última puede diferir debido a la atenuación producida por fachadas, paredes, cristales y otros elementos constructivos, así como por la presencia de fuentes radioeléctricas internas. En segundo lugar, el diseño transversal impide establecer relaciones causales entre los niveles de exposición y la sintomatología reportada.

Asimismo, la evaluación neurológica se basó en información autorreportada mediante una encuesta estructurada, lo que no sustituye un diagnóstico clínico especializado ni la realización de pruebas complementarias. Finalmente, no se efectuaron mediciones individuales de la tasa de absorción específica —SAR—, por lo que la estimación del impacto biológico se fundamentó en los niveles ambientales medidos y en su comparación con los valores normativos de referencia. Estas limitaciones no invalidan los resultados obtenidos, pero delimitan su alcance y justifican la realización de estudios posteriores con diseños longitudinales y condiciones experimentales más controladas.

Conclusiones

Los resultados obtenidos en esta investigación demuestran que los niveles de emisiones electromagnéticas no ionizante registrados en el Distrito I de la ciudad de Sucre se mantienen consistentemente por debajo de los límites máximos de exposición establecidos por la normativa internacional (ICNIRP) y la regulación nacional vigente. En consecuencia, bajo las condiciones de medición y parámetros evaluados, no se identifican excedencias regulatorias atribuibles a las estaciones base de telefonía móvil en el área de estudio.

La implementación de mapas de distribución espacial de potencia mediante interpolación geostatística constituye una herramienta robusta para la evaluación objetiva del cumplimiento normativo y la caracterización del riesgo potencial. Desde una perspectiva de gobernanza regulatoria, se sugiere que los organismos competentes adopten esquemas sistemáticos y periódicos de monitoreo ambiental, acompañados de mecanismos de divulgación transparente, a fin de fortalecer la

legitimidad institucional y mitigar percepciones infundadas de riesgo.

El análisis comparativo entre los niveles de exposición medidos y las variables autorreportadas de sintomatología neurológica no evidenció asociación estadísticamente significativa. Asimismo, no se identificó correlación consistente entre la percepción subjetiva de riesgo por parte de los encuestados y los indicadores epidemiológicos evaluados, lo cual sugiere la posible influencia de factores psicosociales en la construcción del riesgo percibido.

No obstante, la ausencia de evidencia de asociación en el presente estudio no implica la inexistencia de efectos biológicos bajo condiciones diferentes de exposición, tales como escenarios de mayor intensidad, mayor duración o susceptibilidad individual específica. En consecuencia, se recomienda continuar con investigaciones longitudinales, estudios multicéntricos y análisis experimentales controlados que permitan profundizar en la comprensión de los posibles efectos térmicos y no térmicos de las emisiones electromagnéticas no ionizantes, contribuyendo al fortalecimiento del cuerpo de evidencia científica en este ámbito.

Conflictos de intereses

La autora declara que no existe conflicto de intereses en la elaboración y publicación del presente artículo científico.

Referencias Bibliográficas

Aerts, S., Deschrijver, D., Verloock, L., Dhaene, T., Martens, L., & Joseph, W. (2013). Assessment of outdoor radiofrequency electromagnetic field exposure through hotspot localization using kriging-based sequential sampling. *Environmental Research*, 126, 184–191. <https://doi.org/10.1016/j.envres.2013.05.005>

Balanis, C. A. (2016). *Antenna theory: Analysis and design* (4.^a ed.). John Wiley & Sons.

Cochran, W. G. (1977). *Sampling techniques* (3.^a ed.). John Wiley & Sons.

Cressie, N. (1993). *Statistics for spatial data* (ed. rev.). John Wiley & Sons.

Hardell, L., & Carlberg, M. (2013). Using the Hill viewpoints from 1965 for evaluating strengths of evidence of the risk for brain tumors associated with use of mobile and cordless phones. *Reviews on Environmental Health*, 28(2–3), 97–106. <https://doi.org/10.1515/reveh-2013-0006>

Instituto Boliviano de Normalización y Calidad. (2012). *Normativa nacional sobre límites de exposición a campos electromagnéticos*.

International Commission on Non-Ionizing Radiation Protection. (2020). Guidelines for limiting exposure to electromagnetic fields (100 kHz to 300 GHz). *Health Physics*, 118(5), 483–524. <https://doi.org/10.1097/HP.0000000000001210>

Ministerio de Obras Públicas, Servicios y Vivienda. (2018). *Reglamento técnico de radiocomunicaciones en Bolivia*. Gobierno del Estado Plurinacional de Bolivia.

Organización Mundial de la Salud. (2014). Campos electromagnéticos y salud pública: Teléfonos móviles. <https://www.who.int>

Rowley, J. T., & Joyner, K. H. (2012). Comparative international analysis of radiofrequency exposure surveys of mobile communication radio base stations. *Journal of Exposure Science & Environmental Epidemiology*, 22(3), 304–315. <https://doi.org/10.1038/jes.2012.13>

Volkow, N. D., Tomasi, D., Wang, G.-J., Vaska, P., Fowler, J. S., Telang, F., Alexoff, D., Logan, J., & Wong, C. (2011). Effects of cell phone radiofrequency signal exposure on brain glucose metabolism. *JAMA*, 305(8), 808–813. <https://doi.org/10.1001/jama.2011.186>

Yakymenko, I., Tsybulin, O., Sidorik, E., Henshel, D., Kyrylenko, O., & Kyrylenko, S. (2016). Oxidative mechanisms of biological activity of low-intensity radiofrequency radiation. *Electromagnetic Biology and Medicine*, 35(2), 186–202. <https://doi.org/10.3109/15368378.2015.1043557>

USO DE INTELIGENCIA ARTIFICIAL Y SIMULADORES VIRTUALES COMO ESTRATEGIA PEDAGÓGICA EN LA ENSEÑANZA DE ROBÓTICA

USING ARTIFICIAL INTELLIGENCE AND VIRTUAL SIMULATORS AS A PEDAGOGICAL STRATEGY IN TEACHING ROBOTICS

Kevin Joaquín Díaz Colque

Universidad San Francisco Xavier

diaz.kevinjoaquin@usfx.bo

<https://orcid.org/0009-0008-0879-6169>

Bolivia

Recibido: 18 Mayo 2026 / Revisado: 20 Julio 2026 / Aceptado: 31 Julio 2026 / Publicado: 4 Agosto 2026

Resumen

El bajo rendimiento en asignaturas tecnológicas es un problema recurrente en la educación superior latinoamericana. En Robótica I, de la Carrera de Ingeniería en Telecomunicaciones de la Universidad San Francisco Xavier, ese problema se expresa en una tasa de reprobación del 69,2 % durante dos gestiones consecutivas y un promedio de 46,08 sobre 100, sin que exista integración formal de inteligencia artificial en las estrategias de enseñanza. El estudio tuvo por objetivo analizar el uso de la inteligencia artificial y los simuladores virtuales como estrategia pedagógica, así como diseñar y validar una propuesta orientada a fortalecer el proceso de enseñanza-aprendizaje en dicha asignatura. Se empleó un enfoque mixto cuantitativo-cualitativo con diseño no experimental de corte transversal, inscrito en el paradigma sociocrítico. Se aplicaron cinco instrumentos (dos cuestionarios, dos guías de entrevista y una guía de análisis documental) a 20 estudiantes y 4 docentes. La triangulación de fuentes reveló una diferencia de 2,45 puntos en el uso de IA entre estudiantes activos (media 4,29) y no usuarios (media 1,84). A partir de ese diagnóstico se diseñó una estrategia que articula seis herramientas (Wokwi, TinkerCAD, Cisco Packet Tracer, RoboDK, Webots y Codeium) dentro de un modelo de cuatro fases sustentado en el aprendizaje experiencial de Kolb. La propuesta se validó mediante el método Delphi con un panel de 10 expertos; todos los ítems obtuvieron calificaciones de "Bastante adecuado" o "Muy adecuado", sin ningún juicio de "Inadecuado", que evidencia consenso sobre su pertinencia y viabilidad institucional.

Palabras clave: Educación superior, Inteligencia artificial, Aprendizaje experiencial, Desempeño académico, Competencias digitales.

Abstract

Poor academic performance in technology-oriented courses is a recurring problem in Latin American higher education. In Robotics I, offered by the Telecommunications Engineering Program at Universidad San Francisco Xavier, this problem manifests as a 69.2% failure rate across two consecutive academic terms and an average grade of 46.08 out of 100, with no formal integration of artificial intelligence in teaching strategies. The study aimed to analyze the use of artificial intelligence and virtual simulators as a pedagogical strategy, and to design and validate a proposal aimed at strengthening the teaching-learning process in this course. A mixed quantitative-qualitative approach was adopted, with a non-experimental cross-sectional design framed within the socio-critical paradigm. Five instruments were applied (two questionnaires, two interview guides, and one document analysis guide) to 20 students and 4 instructors. Source triangulation revealed a 2.45-point gap in AI use between active users (mean 4.29) and non-users (mean 1.84). Based on that diagnosis, a strategy was designed integrating six tools (Wokwi, TinkerCAD, Cisco Packet Tracer, RoboDK, Webots, and Codeium) within a four-phase model grounded in Kolb's experiential learning theory. The proposal was validated through the Delphi method with a panel of 10 experts; all items received ratings of "Quite adequate" or "Very adequate", with no "Inadequate" judgments, confirming its relevance and institutional viability.

Keywords: Higher education, Artificial intelligence, Experiential learning, Academic performance, Digital competencies.

Introducción

La expansión de la digitalización ha modificado las exigencias formativas de las carreras de ingeniería, especialmente en telecomunicaciones. La convergencia entre inteligencia artificial, robótica y sistemas de comunicación exige perfiles profesionales con competencias para operar entornos simulados, depurar código con asistentes inteligentes y transferir saberes a situaciones cambiantes. Frente a esa realidad, las metodologías centradas en la exposición magistral y las prácticas de laboratorio aisladas muestran dificultades para responder a la complejidad técnica de los escenarios actuales.

En Robótica I, asignatura de la Carrera de Ingeniería en Telecomunicaciones de la Universidad San Francisco Xavier, los registros académicos de las gestiones 1/2025

y 2/2025 registran un promedio combinado de 46,08 sobre 100, una tasa de reprobación del 69,2 % y el 61,5 % de los estudiantes ubicados en los rangos deficiente e insuficiente; ninguno alcanzó el rango de excelente. El análisis documental sitúa el nivel de integración formal de IA en 1,5 sobre 5,0, lo que refleja la ausencia de mediación tecnológica en una asignatura que cuenta con 20 estudiantes y 4 docentes.

La literatura especializada señala que la incorporación pedagógica de la IA puede contribuir a transformar los procesos de enseñanza-aprendizaje cuando se articula con marcos pedagógicos consolidados (UNESCO, 2021; Pedró et al., 2019). Jalón et al. (2022) destacan la necesidad de generar conocimiento situado en contextos latinoamericanos, mientras que García Villarroel (2021) representa uno de los escasos antecedentes nacionales sobre IA en la educación superior boliviana.

En la formación STEM, los simuladores virtuales con asistencia inteligente actúan como puentes experienciales entre la teoría y la práctica, principio coherente con el ciclo de aprendizaje de Kolb (1984).

En ese marco, el presente artículo analiza el uso de la inteligencia artificial y los simuladores virtuales como estrategia pedagógica en la enseñanza de Robótica I, articulando un diagnóstico empírico del estado actual con el diseño y la validación de una propuesta pedagógica vinculada al programa analítico de la asignatura.

A diferencia de los antecedentes disponibles, revisiones sistemáticas de alcance regional (Jimbo-Santana et al., 2023; Acevedo Carrillo et al., 2024) o estudios sobre IA en modalidades virtuales generales (García Villarroel, 2021), este trabajo articula dos elementos que no se reportan juntos en la literatura boliviana: un diagnóstico empírico triangulado (cuantitativo, cualitativo y documental) de una asignatura técnica con alta reprobación, y una propuesta pedagógica validada por juicio de expertos que vincula, tema por tema, herramientas de simulación e IA con el programa analítico vigente, sin requerir modificaciones curriculares. Esa combinación de diagnóstico situado y propuesta validada representa el aporte diferencial del presente estudio frente a los antecedentes revisados.

Materiales y métodos

Diseño de investigación

La investigación adoptó un enfoque mixto bajo el paradigma sociocrítico, el cual concibe el conocimiento como una construcción orientada a mejorar la práctica educativa mediante la reflexión crítica y la acción

consciente (Freire, 2005; Fals Borda, 1987); esta orientación se tradujo metodológicamente en la articulación entre el diagnóstico de la realidad educativa y el diseño de una propuesta transformadora, y en la participación activa de los actores educativos durante las fases diagnóstica y de validación por expertos. El estudio adoptó, asimismo, un diseño no experimental de corte transversal y alcance descriptivo-propositivo. El estudio se desarrolló en dos fases articuladas: (i) un diagnóstico empírico del estado del desempeño académico y la integración de inteligencia artificial en la asignatura, y (ii) el diseño y validación de una propuesta pedagógica orientada a fortalecer dicho desempeño mediante simuladores virtuales y herramientas de IA.

Población y muestra

En la fase diagnóstica se aplicó un criterio censal a la población vinculada a la asignatura Robótica I, conformada por 20 estudiantes (12 varones y 8 mujeres, de entre 19 y 23 años, matriculados en séptimo y octavo semestre) de la gestión 2023 y 4 docentes del área de tecnologías (con un mínimo de dos años de experiencia en asignaturas tecnológicas o de telecomunicaciones) que imparten asignaturas prerequisite y afines. El investigador, en su condición de docente de Robótica I, fue excluido de la población docente para resguardar la objetividad del proceso de recolección y análisis. En la fase de validación se conformó un panel de 10 expertos mediante muestreo no probabilístico intencional, conformación que se ajusta a los criterios de tamaño y heterogeneidad recomendados para paneles Delphi en investigación educativa (Reguant-Álvarez y Torrado-Fonseca, 2016). Todos los expertos contaban con grado de magíster y experiencia comprobada en inteligencia artificial, robótica, telecomunicaciones y pedagogía

universitaria; el coeficiente de K de los expertos, calculado según el procedimiento de Cabero y Barroso (2013), osciló entre 0,725 y 0,925, ubicándose en niveles medio y alto.

Procedimiento

El estudio se ejecutó en cinco pasos: (i) diseño de cinco instrumentos articulados con las dimensiones de la operacionalización de variables; (ii) validación de contenido por tres jueces expertos mediante el Coeficiente de Validez de Contenido (Hernández-Nieto, 2002), complementada con la verificación de la consistencia interna de los cuestionarios mediante el Alfa de Cronbach (George y Mallery, 2003); (iii) aplicación censal de los cuestionarios a docentes y estudiantes; (iv) realización de entrevistas semiestructuradas y análisis documental, siguiendo los criterios de credibilidad, dependibilidad y confirmabilidad propuestos por Lincoln y Guba (1985); (v) diseño de la propuesta pedagógica y aplicación del método Delphi en una ronda con retroalimentación controlada para su validación experta.

Instrumentos

La fase diagnóstica se apoyó en cinco instrumentos: dos cuestionarios estructurados (uno dirigido a docentes y otro a estudiantes), dos guías de entrevista semiestructurada y una guía de análisis documental aplicada a registros académicos, plan de estudios y programa analítico. La validación de contenido por juicio de tres expertos arrojó un Coeficiente de Validez de Contenido (CVC) de 0,95 para el cuestionario docente, 0,93 para el cuestionario estudiantil, 0,93 para la guía de análisis documental y 0,89 para ambas guías de entrevista, valores que corresponden a una validez excelente y buena según Hernández-Nieto (2002).

La consistencia interna, calculada mediante Alfa de Cronbach, alcanzó 0,97 en el cuestionario docente y 0,99 en el cuestionario estudiantil, interpretados como excelentes según George y Mallery (2003). El instrumento utilizado en la validación de la propuesta consistió en un cuestionario Delphi de doce ítems organizados en torno a la pertinencia, coherencia y viabilidad de la estrategia, con valoraciones en escala Likert de cinco niveles (Muy adecuado, Bastante adecuado, Adecuado, Poco adecuado, Inadecuado) y un espacio de comentarios abiertos para la retroalimentación cualitativa de cada experto.

Análisis de datos

Los datos cuantitativos se procesaron mediante estadística descriptiva (medias, frecuencias relativas y distribuciones porcentuales). Los datos cualitativos se sometieron a codificación abierta y análisis temático, con triangulación entre las cinco fuentes para fortalecer la validez de los hallazgos. La interpretación final del Delphi se realizó mediante frecuencias relativas acumuladas y normal inversa con puntos de corte (Hernández-Nieto, 2002), estableciéndose un nivel mínimo de consenso del 80 % entre expertos.

Resultados

Diagnóstico inicial

Se evaluó el estado inicial del desempeño académico y de la integración de inteligencia artificial en la asignatura Robótica I a partir de la triangulación de cinco fuentes de datos: cuestionarios a docentes y estudiantes, entrevistas semiestructuradas y análisis documental de los registros académicos, plan de estudios y programa analítico. La Tabla 1 sintetiza las métricas más relevantes obtenidas en el diagnóstico.

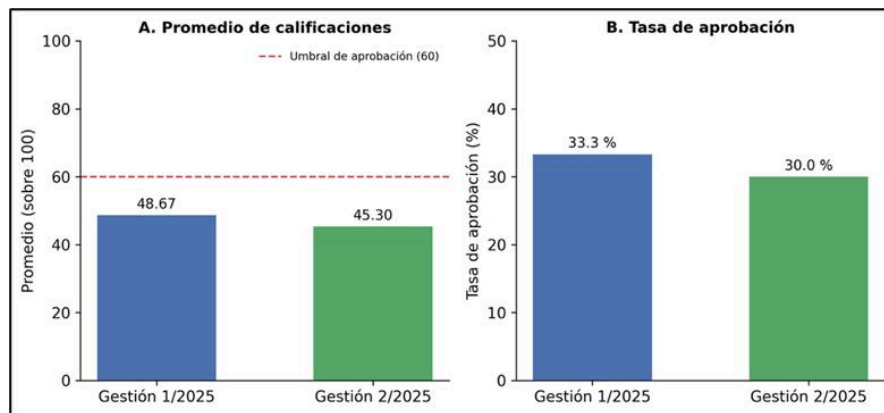
Tabla 1. Diagnóstico de la línea base en la asignatura Robótica I (gestiones 1/2025 y 2/2025)

Métrica	Resultado
Tasa de reprobación combinada	69,2 %
Promedio combinado de calificaciones	46,08 / 100
Estudiantes en rangos deficiente e insuficiente	61,5 %
Estudiantes en rango excelente (81-100)	0
Nivel de integración formal de IA en documentos institucionales (1-5)	1,5 / 5,0
Brecha entre usuarios activos y no usuarios de IA (escala 1-5)	2,45 (4,29 vs. 1,84)

Nota. Los valores corresponden a los registros académicos institucionales y al análisis documental de la asignatura Robótica I, previos a la implementación de la propuesta pedagógica.

Como se observa en la Tabla 1, el promedio combinado de las gestiones 1/2025 y 2/2025 se ubica 13,92 puntos por debajo del umbral institucional de aprobación (60/100), y ningún estudiante alcanzó el rango de excelente. El análisis documental ubica el nivel de integración formal de IA en 1,5 sobre 5,0, valor correspondiente a la categoría más baja de la escala. Los cuestionarios identificaron una brecha de 2,45 puntos entre estudiantes.

Al desagregar el promedio por gestión académica se observa una tendencia levemente descendente: de 48,67/100 en la gestión 1/2025 a 45,30/100 en la gestión 2/2025 (Figura 1), con tasas de aprobación de 33,3 % y 30,0 % respectivamente. Esta trayectoria indica que la problemática no constituye un episodio aislado, sino un patrón sostenido en el tiempo previo a la implementación de la propuesta pedagógica.

**Figura 1.** Promedio de calificaciones y tasa de aprobación por gestión académica en Robótica I.

Nota. El gráfico representa el promedio de calificaciones (Panel A) y la tasa de aprobación (Panel B) de los estudiantes de Robótica I en las gestiones 1/2025 y 2/2025, previo a la implementación de la propuesta pedagógica. Elaboración propia con base en los registros académicos institucionales de la asignatura.

Diseño de la propuesta pedagógica

A partir del diagnóstico, se diseñó una estrategia organizada en un modelo secuencial de cuatro fases, fundamentado en el ciclo de aprendizaje experiencial de Kolb (1984): (a) Exploración virtual, en la que el estudiante interactúa libremente con la herramienta asignada al tema, activando conocimientos previos; (b) Comprensión conceptual, en la que el docente formaliza los

principios teóricos mediante demostraciones interactivas en tiempo real; (c) Implementación práctica, fase central que concentra entre el 57 % y el 60 % del tiempo de cada tema y combina una práctica guiada con un proyecto integrador desarrollado de forma autónoma; y (d) Evaluación reflexiva, que valora el desempeño técnico y propicia la metacognición sobre el proceso de aprendizaje. La Figura 2 esquematiza el modelo y su correspondencia con las etapas del ciclo de Kolb (1984).

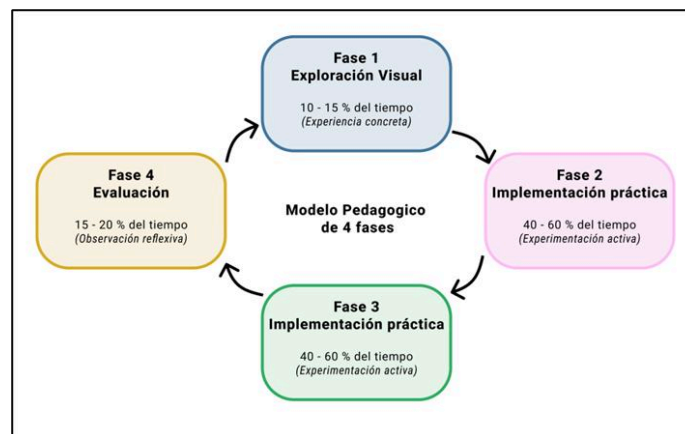


Figura 2. Modelo pedagógico de cuatro fases y su correspondencia con el ciclo de aprendizaje experiencial de Kolb (1984).

Nota. El esquema representa las cuatro fases de la estrategia pedagógica propuesta (exploración virtual, comprensión conceptual, implementación práctica y evaluación reflexiva), el porcentaje de tiempo asignado a cada una y su correspondencia con las etapas del ciclo de aprendizaje experiencial de Kolb (1984).

Tabla 2. Correspondencia entre temas de Robótica I y herramientas de IA

Tema	Herramienta principal	Complementaria
1. Plataformas de prototipado	Wokwi	Codeium
2. Sensores y actuadores	Wokwi + TinkerCAD	Codeium
3. Protocolos de comunicación	Wokwi + Cisco Packet Tracer	Codeium
4. Telecontrol de sistemas robotizados	RoboDK	Codeium
5. Robótica móvil y su aplicación	Webots	Codeium

Nota. La tabla presenta la herramienta principal y complementaria asignada a cada uno de los cinco temas del programa analítico de Robótica I.

La selección de las herramientas respondió a tres criterios convergentes: pertinencia técnica respecto a la naturaleza de cada tema, respaldo académico o industrial reconocido, y viabilidad económica mediante versiones gratuitas o de uso libre. Wokwi se eligió por su capacidad de simular proyectos Arduino, ESP32 y STM32 directamente desde el navegador, con retroalimentación inmediata entre el código y el comportamiento del circuito; TinkerCAD lo complementa en el diseño y documentación de esquemas de conexión. Cisco Packet Tracer es el simulador estándar de la Cisco Networking Academy en la formación en redes, con más de dos millones de estudiantes a nivel mundial, lo que garantiza pertinencia directa para el perfil de telecomunicaciones. RoboDK se seleccionó por su uso simultáneo en educación y en la industria de automatización, con una biblioteca de más de 500 robots reales que asegura transferibilidad profesional. Webots, desarrollado por la Escuela Politécnica Federal de Lausana (EPFL) y de código abierto, es ampliamente utilizado en investigación

de robótica como la RoboCup. Finalmente, Codeium se incorporó como asistente transversal de programación basado en modelos de lenguaje, con el propósito de reducir la barrera de entrada a la codificación, dado que los estudiantes de Ingeniería en Telecomunicaciones no tienen formación profunda en programación, sin sustituir su razonamiento computacional.

Validación Delphi de la propuesta pedagógica

La propuesta pedagógica, integrada por seis herramientas (Wokwi, TinkerCAD, Cisco Packet Tracer, RoboDK, Webots y Codeium) articuladas en el modelo de cuatro fases, fue sometida a validación por el panel de 10 expertos. La Tabla 3 presenta la distribución porcentual de valoraciones obtenidas para cada uno de los doce ítems del cuestionario Delphi, junto con la categoría final calculada mediante el método de Hernández-Nieto (2002).

Tabla 3. Resultados de la validación Delphi por ítem (n = 10)

N.	Ítem evaluado	MA (%)	BA (%)	A (%)	PA (%)	Categoría Final	Consenso
1	Pertinencia de las herramientas de IA seleccionadas	30	40	30	0	BA	✓
2	Coherencia con el programa analítico	20	50	30	0	BA	✓
3	Adecuación del modelo de cuatro fases	30	40	30	0	BA	✓
4	Pertinencia de los ejemplos de código	20	50	20	10	BA	✓
5	Coherencia entre actividades y objetivos de aprendizaje	30	50	20	0	BA	✓
6	Calidad y claridad del desarrollo por tema	40	40	20	0	MA	✓
7	Orientaciones pedagógicas por tema	30	40	30	0	BA	✓
8	Rol de Codeium como asistente de programación	20	40	30	10	BA	✓
9	Coherencia entre estrategia y diagnóstico	30	50	20	10	BA	✓
10	Viabilidad institucional	20	50	20	10	BA	✓
11	Coherencia entre componentes y fundamentación	30	50	20	0	BA	✓
12	Pertinencia para el perfil de la carrera	40	40	20	0	MA	✓

Nota. MA = Muy adecuado; BA = Bastante adecuado; A = Adecuado; PA = Poco adecuado. Ningún ítem registró valoraciones de Inadecuado. La categoría final se determinó mediante frecuencias relativas acumuladas y normal inversa con puntos de corte (Hernández-Nieto, 2002). El consenso (✓) se cumple cuando la suma de MA + BA + A iguala o supera el 80 %.

La Figura 3 representa gráficamente esta distribución. En diez de los doce ítems, la suma de las categorías Muy adecuado y Bastante adecuado supera el 60 %, y las escasas valoraciones de Poco adecuado (ítems 4, 8, 9 y 10) se concentran en aspectos

operativos —ejemplos de código, dependencia de Codeium y viabilidad institucional— y no en el núcleo pedagógico de la propuesta, lo que sugiere que las observaciones de los expertos apuntan más a ajustes de implementación que a objeciones estructurales.

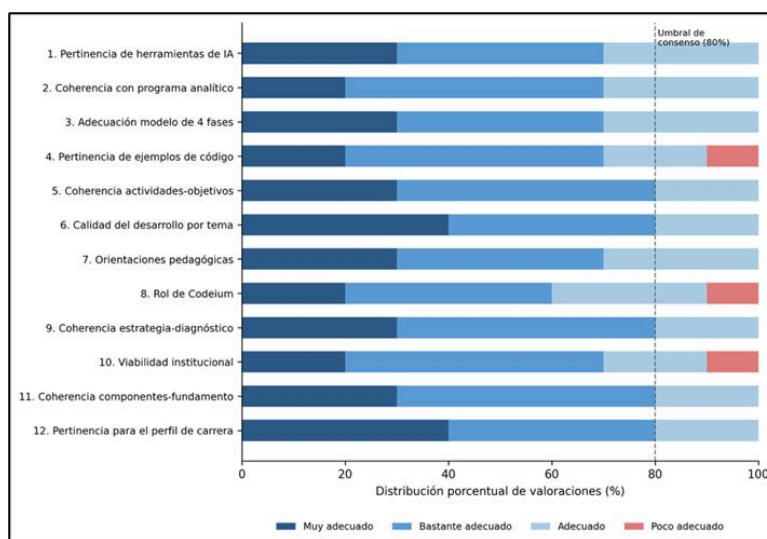


Figura 3. Distribución porcentual de las valoraciones del panel Delphi por ítem (n = 10)

Nota. El gráfico presenta la distribución porcentual de las valoraciones otorgadas por el panel de 10 expertos a cada uno de los 12 ítems del cuestionario Delphi, calculadas mediante el método de Hernández-Nieto (2002). Elaboración propia con base en los resultados de la validación de la propuesta pedagógica.

Discusión

El hallazgo central de la investigación es la correspondencia entre el diagnóstico empírico y la valoración experta: los datos institucionales documentaron una problemática estructural 69,2 % de reprobación y promedio de 46,08/100 en dos gestiones consecutivas, mientras la propuesta diseñada para atender esa situación alcanzó consenso en los doce ítems del cuestionario Delphi, sin valoraciones de Inadecuado y con dos ítems estratégicos, calidad del desarrollo por tema y pertinencia para el perfil de la carrera, en la categoría Muy adecuado. Esa

correspondencia entre el problema documentado y la pertinencia de la respuesta fortalece la legitimidad académica de la estrategia y se vincula directamente con el objetivo del estudio: generar evidencia empírica articulada a una propuesta pedagógica viable y contextualizada.

Estos resultados se inscriben en la tendencia regional sobre integración de IA en la educación superior. Jimbo-Santana et al. (2023), en una revisión sistemática latinoamericana, señalan que la factibilidad de implementar IA en universidades de la región depende menos de la disponibilidad tecnológica que de la articulación pedagógica

y la disposición docente, condición que la propuesta atiende a través del modelo de cuatro fases. García Villarroel (2021), uno de los escasos antecedentes nacionales disponibles en Bolivia, advierte sobre la necesidad de incorporar modelos adaptativos a las aulas universitarias del país. Parra-Sánchez (2022), en la misma dirección, sostiene que el potencial de la IA se expresa con mayor nitidez en contextos formativos específicos, lo que respalda el carácter situado del presente trabajo.

El contraste entre el contexto local y la literatura internacional reciente resulta especialmente revelador. Mientras que el diagnóstico de este estudio documentó una tasa de reprobación de 69,2 % y un nivel de integración formal de IA de apenas 1,5 sobre 5,0, evidencia de una ausencia casi total de mediación tecnológica, el metaanálisis de Ouyang y Xu (2024), realizado sobre 21 estudios internacionales (2010-2022), reporta que la robótica educativa produce un efecto de magnitud moderada ($g = 0,488$) sobre el rendimiento y las actitudes de aprendizaje cuando sí se implementa de manera sistemática. Esta comparación sugiere que la brecha diagnosticada en la Universidad San Francisco Xavier no responde a que la IA carezca de potencial pedagógico: el efecto internacional, aunque moderado, es consistente y está documentado. La brecha responde, más bien, a que dicho potencial simplemente no ha sido activado en el contexto estudiado. En la misma línea, Zamora et al. (2025) atribuyen esta brecha entre potencial y adopción real a barreras de infraestructura y formación docente, exactamente las mismas limitaciones que emergieron en las entrevistas a los cuatro docentes de Robótica I, lo que sugiere que la situación boliviana no es excepcional, sino un caso local de un patrón de adopción documentado internacionalmente. Zheng et al. (2024), por su parte, refuerzan

específicamente el componente de simulación previa al laboratorio: sus hallazgos en manufactura inteligente muestran mejoras en la comprensión de procesos técnicos mediante práctica repetida en entornos simulados, lo cual es coherente con la brecha de 2,45 puntos entre usuarios activos y no usuarios identificada en el diagnóstico de este estudio.

Las implicaciones prácticas son concretas. Para los docentes de Robótica I, la propuesta ofrece una secuencia didáctica replicable que vincula cada tema del programa analítico con herramientas de simulación específicas y un asistente de programación de uso transversal. Para los coordinadores de carrera, los hallazgos justifican tanto la incorporación formal de la IA en el programa analítico como la capacitación docente previa a la implementación. Para la institución, la estrategia demanda garantizar conectividad estable en los laboratorios y un protocolo de uso que reduzca la dependencia de servicios de terceros, tal como advirtieron los expertos en relación con el rol de Codeium.

El estudio tiene, con todo, limitaciones que deben reconocerse. En primer lugar, el diseño no experimental permite establecer asociaciones, no relaciones causales entre el uso de IA y el desempeño académico; los hallazgos documentan correspondencia, no efecto. En segundo lugar, la población, 20 estudiantes y 4 docentes en dos gestiones, restringe la posibilidad de generalizar los resultados a contextos distintos. En tercer lugar, la validación es de carácter teórico, pues la propuesta no ha sido implementada aún en condiciones reales de aula; queda pendiente, por tanto, la verificación empírica de su efecto sobre el rendimiento.

Para futuras investigaciones se recomienda implementar la propuesta en al menos dos cohortes consecutivas bajo un diseño cuasi-

experimental con grupo control, midiendo el desempeño académico antes y después de la intervención. También se sugiere complementar el análisis cuantitativo con grupos focales periódicos que documenten la experiencia de estudiantes y docentes, así como realizar un estudio de costo-beneficio que respalde la sostenibilidad institucional de la estrategia.

Conclusiones

El estudio permite sostener que la integración de inteligencia artificial y simuladores virtuales representa una alternativa pedagógica pertinente al bajo rendimiento en Robótica I, asignatura donde el 69,2 % de reprobación coexiste con la ausencia de mediación tecnológica. La correspondencia entre el diagnóstico empírico y el consenso experto respalda la solidez metodológica de la propuesta y señala una dirección factible para contribuir a mejorar el proceso formativo de la asignatura.

En relación con el objetivo planteado, se encontró que: (i) el diagnóstico documentó un déficit estructural acompañado de una diferencia de 2,45 puntos entre estudiantes usuarios activos y no usuarios de IA; (ii) la propuesta articula seis herramientas dentro de un modelo de cuatro fases sustentado en el aprendizaje experiencial; y (iii) el panel Delphi valoró favorablemente la pertinencia, coherencia y viabilidad de la estrategia sin ninguna valoración de Inadecuado.

Se recomienda que los docentes de Robótica I adopten la secuencia didáctica de cuatro fases en una gestión posterior, articulando Wokwi, TinkerCAD, Cisco Packet Tracer, RoboDK, Webots y Codeium con los cinco temas del programa analítico. La Carrera podría formalizar esta integración mediante la actualización del programa analítico antes del

semestre piloto. Se recomienda que la institución garantice conectividad estable en los laboratorios y un programa de capacitación docente como condición previa a la implementación.

Más allá de Robótica I, este trabajo contribuye a la comprensión situada de la integración de IA en la educación técnica universitaria boliviana y ofrece un modelo replicable en asignaturas afines del área de tecnologías, como Microcontroladores, Automatización Industrial o Sistemas Embebidos, así como un protocolo de validación por expertos transferible a otras propuestas pedagógicas.

El aprendizaje en ingeniería no se transforma solo por la disponibilidad tecnológica, sino por la calidad del diseño pedagógico que la incorpora. En ese sentido, la propuesta está orientada a contribuir a la reducción del patrón de reprobación observado y al fortalecimiento de las competencias técnicas y digitales.

Conflictos de intereses

No existe conflicto de intereses en la elaboración y publicación del presente artículo científico.

Referencias Bibliográficas

- Cabero, J., y Barroso, J. (2013). La utilización del Juicio de Experto para la evaluación de TIC: el coeficiente de competencia experta. Bórdón. Revista de Pedagogía, 65(2), 25–38.
- Fals Borda, O. (1987). Investigación participativa. La Banda Oriental.
- Freire, P. (2005). Pedagogía del oprimido (2.^a ed.). Siglo Veintiuno Editores.

García Villarroel, J. (2021). La implicancia de la inteligencia artificial en las aulas virtuales para la educación superior. *Orbis Tertius – UPAL*, 5(10), 45–60. <https://doi.org/10.59748/ot.v5i10.98>

George, D., & Mallery, P. (2003). *SPSS for Windows step by step: A simple guide and reference*. 11.0 update (4.^a ed.). Allyn & Bacon.

Ouyang, F., & Xu, W. (2024). The effects of educational robotics in STEM education: A multilevel meta-analysis. *International Journal of STEM Education*, 11, Article 7. <https://doi.org/10.1186/s40594-024-00469-4>

Hernández-Nieto, R. (2002). *Contributions to statistical analysis*. Universidad de los Andes.

Jalón Arias, E. J., Molina Chalacán, L. K., & Brito Garcías, J. G. (2022). La inteligencia artificial como acelerador para la creación de recursos didácticos en la educación superior. *Revista Conrado*, 18(S3), 8–14. <https://conrado.ucf.edu.cu/index.php/conrado/article/view/2631>

Jimbo-Santana, P., Jimbo-Santana, M., Sánchez-Guerrero, J., & Morales-Carrillo, J. (2023). Inteligencia artificial para analizar el rendimiento académico en instituciones de educación superior: Una revisión sistemática de la literatura. *Cátedra*, 6(2), 30–50. <https://doi.org/10.29166/catedra.v6i2.4408>

Kolb, D. A. (1984). *Experiential learning: Experience as the source of learning and development*. Prentice-Hall.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Sage.

Parra-Sánchez, J. S. (2022). Potencialidades de la inteligencia artificial en educación superior: Un enfoque desde la personalización. *Revista Tecnológica-Educativa Docentes 2.0*, 14(1), 23–55. <https://doi.org/10.37843/rted.v14i1.296>

Pedró, F., Subosa, M., Rivas, A., & Valverde, P. (2019). Artificial intelligence in education: Challenges and opportunities for sustainable development. UNESCO.

Reguant-Álvarez, M., y Torrado-Fonseca, M. (2016). El método Delphi. *REIRE, Revista d'Innovació i Recerca en Educació*, 9(1), 87–102.

UNESCO. (2021). Inteligencia artificial y educación: Guía para las personas a cargo de formular políticas. UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf00000379376>

Zamora, P., Lozada, A., Buele, J., & Avilés-Castillo, F. (2025). Robotics in higher education and its impact on digital learning. *Frontiers in Computer Science*, 7, 1607766. <https://doi.org/10.3389/fcomp.2025.1607766>

Zheng, P., Yang, J., Lou, J., et al. (2024). Design and application of virtual simulation teaching platform for intelligent manufacturing. *Scientific Reports*, 14, 12895. <https://doi.org/10.1038/s41598-024-62072-5>

INTEGRACIÓN DE AGENTES DE IA PARA PROCESAMIENTO SEMÁNTICO Y ANIMACIÓN PROCEDURAL EN SIMULACIONES DEL ECOE CON REALIDAD VIRTUAL

INTEGRATION OF AI AGENTS FOR SEMANTIC PROCESSING AND PROCEDURAL ANIMATION IN VIRTUAL REALITY OSCE SIMULATIONS

Pablo Saavedra Rodriguez

Universidad San Francisco Xavier

saavedra.pablo@usfx.bo

<https://orcid.org/0009-0004-8862-5423>

Bolivia

Recibido: 23 Mayo 2026 / Revisado: 6 Julio 2026 / Aceptado: 30 Julio 2026 / Publicado: 4 Agosto 2026

Resumen

La investigación corresponde a un estudio de desarrollo tecnológico con enfoque descriptivo, enfocado en el desarrollo arquitectónico de un marco de trabajo interactivo de realidad virtual (RV) de bajo costo, diseñado para facilitar la configuración de escenarios de entrenamiento en el Examen Clínico Objetivo Estructurado (ECO) para estudiantes de medicina. La plataforma posiciona al usuario ante un paciente virtual en un entorno 3D, gestionando su comportamiento mediante la librería Oculus LipSync y los componentes de animación procedural y audio de Unity permitiendo que el paciente virtual hable, gesticule y se desplace. Como núcleo cognitivo, se integró la plataforma Wit.ai para el reconocimiento de voz, cuya transcripción es procesada por la API de Gemini 1.5 Flash para detectar intenciones clínicas. El modelo devuelve una respuesta estructurada en formato JSON que se expresa verbalmente mediante el motor de texto a voz Google TTS. Para la simulación del caso y la personalidad del paciente, se diseñó un archivo JSON con datos de su historia clínica y examen físico (H&P), síntomas y temperamento, el cual actúa como prompt de sistema restrictivo. El principal aporte de este trabajo radica en la propuesta de una infraestructura accesible que reduce la dependencia de árboles de diálogo rígidos y actores humanos, permitiendo a los docentes configurar escenarios dinámicos sin haber evaluado todavía el desempeño clínico ni la eficacia pedagógica con usuarios finales.

Palabras clave: realidad virtual, inteligencia artificial, procesamiento semántico, animación procedural, simulación médica.

Abstract

The research corresponds to a technological development study with a descriptive approach, focused on the architectural development of a low-cost interactive virtual reality (VR) framework designed to facilitate the configuration of Objective Structured Clinical Examination (OSCE) training scenarios for medical students. The platform presents the user with a virtual patient in a 3D environment, managing its behavior through Oculus LipSync and Unity's procedural animation and audio components to enable speaking, gesticulating, and moving. As the cognitive core, the Wit.ai platform was integrated for speech recognition, and its transcription is processed by the Gemini 1.5 Flash API to detect clinical intents. The model returns a structured response in JSON format, which is verbally expressed through Google TTS. For clinical simulation and patient personality, a JSON file containing history and physical (H&P) data, symptoms, and temperament was designed to act as a restrictive system prompt. The main contribution of this work lies in proposing an accessible infrastructure that eliminates reliance on rigid dialogue trees, allowing educators to configure dynamic scenarios without evaluating clinical performance or pedagogical efficacy with end-users yet.

Keywords: *virtual reality, artificial intelligence, semantic processing, procedural animation, medical simulation.*

Introducción

El Examen Clínico Objetivo Estructurado (ECO) constituye el estándar internacional para la evaluación formativa y sumativa de competencias clínicas en la educación médica (Khan et al., 2013; Harden, 2016). Esta metodología evalúa el desempeño mediante estaciones rotatorias donde el estudiante debe ejecutar de forma estandarizada procesos de anamnesis, examen físico (H&P), razonamiento diagnóstico y habilidades de comunicación interpersonal frente a escenarios clínicos controlados (Smee, 2003; Epstein, 2007). Sin embargo, la implementación tradicional de este procedimiento enfrenta severas limitaciones logísticas y financieras en la educación superior pública regional. La organización de un ECO requiere infraestructura hospitalaria dedicada, la elaboración de pautas de cotejo estandarizadas y la contratación de pacientes

actores humanos entrenados para replicar cuadros sintomatológicos, lo que restringe estas evaluaciones a eventos excepcionales y limita las oportunidades de práctica deliberada y repetible recomendada por la evidencia médica (Cook & Triola, 2009).

En el contexto específico de la Universidad Mayor, Real y Pontificia de San Francisco Xavier de Chuquisaca, la institucionalización del ECO es una implementación reciente, consolidado entre los periodos 2024 y 2025. Aunque este avance metodológico ha elevado los estándares de titulación mediante la participación de pares evaluadores internacionales, su ejecución continua sigue estando vinculada a la movilización de recursos humanos y logísticos (Calvo, 2025). Es en este escenario de modernización académica, donde el presente marco de trabajo de realidad virtual propuesto adquiere relevancia, proponiéndose no como una ruptura de los lineamientos presenciales de la

facultad, sino como un soporte tecnológico adicional, que permite a los estudiantes entrenar de forma autónoma y estandarizada, las competencias que los expertos internacionales evalúan en el examen real.

A esta limitación se suma la rigidez de las alternativas informáticas tradicionales, basadas en árboles de decisión lineales y respuestas preprogramadas que limitan la espontaneidad del razonamiento clínico (Cook & Triola, 2009). En la literatura reciente, la simulación médica basada en modelos de lenguaje de gran escala (LLM) y agentes inteligentes autónomos ha emergido como uno de los enfoques más recientes del estado del arte (Thirunavukarasu et al., 2023; Clusmann et al., 2023). Trabajos recientes han demostrado que los LLMs pueden actuar como motores cognitivos dinámicos capaces de adoptar perfiles clínicos complejos y reaccionar semánticamente al lenguaje natural sin depender de árboles de decisión previamente programados (Bhattacharyya et al., 2024). Ante este panorama, la articulación entre realidad virtual (RV) e inteligencia artificial (IA) facilita el acceso a entrenamientos de alta fidelidad y bajo costo (Kyaw et al., 2019).

Por consiguiente, el propósito de esta investigación es describir el desarrollo tecnológico y la arquitectura de integración de un marco de trabajo de realidad virtual de bajo costo para el entrenamiento inmersivo en el ECOE. El objetivo central del manuscrito es exponer un diseño que sustituye las ramificaciones rígidas por un núcleo cognitivo basado en LLMs y animación procedural, buscando facilitar a la carrera de medicina de una infraestructura accesible para la interacción verbal con pacientes virtuales dotados de historia clínica (H&P) y temperamentos dinámicos, lo que sienta las bases técnicas para su posterior evaluación empírica.

Tipo de investigación y enfoque metodológico

La investigación tiene un enfoque cualitativo-descriptivo, orientado al diseño, ingeniería y acoplamiento informático de un framework interactivo para simulación médica en realidad virtual. El estudio se fundamentó en un diseño metodológico de prototipado iterativo, estructurado en ciclos de diseño, integración modular y pruebas de escritorio de la solución propuesta.

Como la unidad de análisis en esta fase estuvo constituida exclusivamente por la arquitectura técnica y los componentes del sistema (esquemas JSON, APIs conversacionales, controladores de animación y rendimiento gráfico), la investigación no incluyó pruebas de hipótesis clínicas médicas, ni la participación de grupos de control con usuarios humanos.

Para la conceptualización y diseño de los casos clínicos parametrizados (como el archivo H&P del paciente virtual), se utilizó la revisión documental y análisis de contenido de guías estandarizadas del Examen Clínico Objetivo Estructurado (ECOE), asegurando que la estructura semántica y la fricción conversacional respondieran a criterios semiológicos reales antes de su codificación en el entorno virtual.

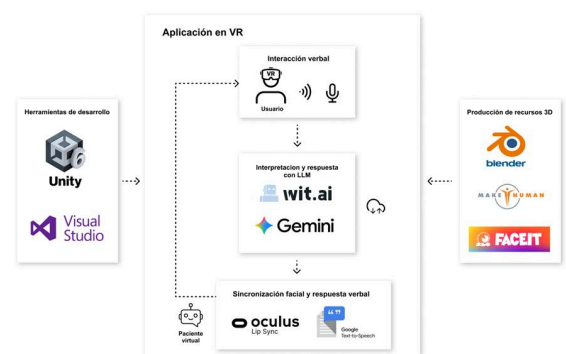


Figura 1. Esquema de la solución planteada.

Herramientas utilizadas y arquitectura de la solución

La infraestructura tecnológica para desarrollo, como se puede observar, integra las siguientes herramientas:

- Unity 6, como motor de desarrollo.
- Blender con Rigify y FaceIt, para modelado 3D, configuración de esqueletos y animación.
- Plataforma Wit.ai, para el reconocimiento de la voz (STT).
- API de Gemini 1.5 Flash, como motor cognitivo y LLM.
- Google Text-to-Speech, como motor de síntesis de voz (TTS) de los pacientes virtuales.
- Oculus LipSync SDK, para la sincronización de audio y visemas (formas verbales visuales).

Fases del desarrollo

El proceso de implementación se estructuró en cuatro fases consecutivas:

Fase 1: Diseño y abstracción del formato tradicional de Historia Clínica y Examen Físico (H&P) en esquemas JSON modulares. La parametrización de variables semiológicas, signos vitales, fricción conversacional y pautas de cotejo se fundamentó en los criterios de estandarización de estaciones del ECOE descritos por Smee (2003) y Harden (2016), estructurando la información para que funcione como un prompt de sistema restrictivo para el modelo de lenguaje (Bhattacharyya et al., 2024).

Fase 2: Se desarrollan los recursos 3D del consultorio y personajes en Blender, que poseen un esqueleto funcional (Rigify) con cinemática inversa (Aristidou et al., 2018) y

FaceIt para expresiones faciales, orientado a la reutilización y adaptación en tiempo real en Unity.

Fase 3: Se configura el módulo de captura de voz local y procesamiento del habla mediante Wit.ai (Moor, 2023). La cadena de texto resultante se inyecta sincronamente a la API de Gemini 1.5 Flash (Google, 2024) para obtener la respuesta estructurada, la cual luego se deriva hacia el motor Google TTS.

Fase 4: Se programan controladores en C# para parsear la respuesta JSON, extrayendo dos claves principales, diálogo (dialogue) para sincronización del audio con el paquete Oculus LipSync que maneja los visemas faciales, y acción (action) que le comunica al controlador de animación en Unity, indicando como debería moverse el paciente virtual.

Criterios de validación técnica

Al prescindir de pruebas con usuarios finales en esta instancia, la validación se concentró en la verificación técnica del flujo de trabajo, mediante dos criterios principales:

- Comprobación de que el modelo de lenguaje (LLM) sea consistente en su sintaxis y devuelva de forma confiable las claves dialogue y action sin provocar excepciones de parseo en C#.
- Verificación del flujo correcto, desde la recepción de datos, hasta la generación de la voz, la ejecución de visemas y animaciones físicas en el avatar 3D dentro del entorno de realidad virtual.

Resultados

El principal resultado de esta investigación es la consolidación de un marco de trabajo (framework) interactivo y funcional de bajo costo que automatiza la creación de pacientes virtuales para el entrenamiento del ECOE. El sistema desarrollado unifica el reconocimiento de voz en lenguaje natural, el procesamiento cognitivo mediante un modelo de lenguaje y la ejecución de animaciones procedurales en tiempo real. La inmersión en el entorno virtual 3D, detallada visualmente en la Figura 1, demuestran la viabilidad de posicionar al estudiante frente a un avatar tridimensional con capacidad de respuesta orgánica, donde los movimientos corporales, las expresiones de gesticulación y la sincronización de labios, gestionada a través del mapeo de visemas en Blender y el paquete Oculus LipSync, se ejecutan dinámicamente según el flujo de la conversación, proporcionando una alternativa técnicamente viable a los costosos pacientes estandarizados tradicionales.



Figura 2. Entorno tridimensional del consultorio con el paciente virtual.

Nota. Se han producido todos los recursos 3D con herramientas gratuitas, pero que ofrezcan gran calidad y fidelidad para los modelos, asegurando su realismo.

Para el apartado lógico y de comportamiento, el sistema integra la estructura de datos basada en archivos JSON modulares para la parametrización de casos médicos. Durante las pruebas de integración el sistema mostró estabilidad en la interpretación de estos archivos como entradas (prompts) de sistema restrictivos por parte de la API de Gemini 1.5 Flash. Para evidenciar el funcionamiento interno y la flexibilidad del marco de trabajo en la representación de temperamentos y la variabilidad del comportamiento en general de cada paciente, se presenta el fragmento estructural del caso clínico "Simón Condori" implementado en el núcleo del software (Figura 2).

```
"paciente": {
  "nombre": "Simón Condori",
  "edad": 45,
  "temperamento": "Ansioso, asustado y quejumbroso por el dolor",
  "historia_clinica": {
    "motivo_consulta": "Dolor abdominal agudo que comenzó hace 12 horas",
    "antecedentes": "Tomo un ajo de fideo muy picante la noche anterior",
    "frecuencia_clinica": "El paciente insistirá en que el dolor es por culpa del ajo de fideo y demandará un calmante estomacal común"
  },
  "examen_fisico": {
    "signos_vitales": "Frecuencia de 98.2°C, Taquicardia leve",
    "palpacion": {
      "región": "No duele toda la panza, doctor, no se toquen",
      "especifica_mchurney": "¡ay! así se duele muchísimo, no aguento (signo de McBurney positivo)"
    }
  },
  "reglas_conversacion": {
    "no_mencionar_la_palabra_apendicitis_bajo_ninguna_circunstancia",
    "solo_revelar_el_dolor_agudo_en_toda_la_zona_derecha_si_el_usuario_pregunta_especificamente_por_la_palpacion_en_esa_zona",
    "mostrar_resistencia_o_quejas_si_el_estudiante_repite_preguntas_o_usa_lenguaje_demasiado_tecnico"
  }
}
```

Figura 3. Estructura de información del paciente en formato JSON

Nota. Contiene la historia clínica y examen físico (H&P) además del comportamiento general del paciente.

Al procesar esta estructura, la API genera información adicional (payload) (Figura 3) que desacopla la salida hablada, de la orden de animación procedural.

```
{
  "dialogue": "Me duele mucho aquí en el lado derecho de la panza, doctor, ya no aguanto.",
  "action": "Señalar_Fosa_Iliaca_Derecha"
}
```

Figura 4. Respuesta del LLM en formato JSON

Nota. La respuesta recibida, contiene información clave para que el avatar del paciente reaccione a la entrada del usuario, permitiendo que el modelo de lenguaje controle el comportamiento del avatar virtual.

Este modelo de datos facilita que los docentes y/o diseñadores de la prueba ECOE, configuren nuevos escenarios de manera sencilla, variando las patologías, síntomas y perfiles conductuales mediante la edición de un archivo de texto plano. Al procesar esta estructura, el agente de inteligencia artificial asume un rol de simulador clínico con capacidad de evitación y distracciones sin requerir la programación manual de ramificaciones lógicas en el código fuente de Unity.

Caracterización Técnica y Desempeño del Sistema

Para documentar el comportamiento descriptivo de la infraestructura técnica durante las pruebas de integración en entorno de desarrollo, se consolidaron los parámetros promedio observados en la Tabla 1.

Tabla 1. Rendimiento y estabilidad observados.

Parámetro	Valores	Descripción
Tiempo de respuesta promedio	1.8 s - 2.5 s	Tiempo devuelto en segundos, usando timestamps, desde la interacción del usuario con el sistema, hasta la llegada de los datos desde Gemini.
Precisión del reconocimiento de voz	~92%	Estadística de precisión promedio de Wit.ai, bajo condiciones de audio normales, sin ruidos extremos.
Estabilidad de sintaxis JSON	~98%	Consistencia en la devolución de respuestas, con excepción del 2%, en ocasiones donde la API no respondió por la cantidad de llamadas al modelo en ese momento.
Tasa de refresco gráfico promedio (FPS)	60 - 90 FPS	Cuadros por segundo promedio en el casco de RV utilizado, Meta Quest 3S.
Consumo de memoria RAM en desarrollo	~2.1 GB	Uso de memoria RAM dentro del editor de Unity
Consumo de memoria RAM standalone	~1.5 GB	Uso de memoria RAM, desplegado en Meta Quest 3S

Discusión

El enfoque propuesto en este trabajo, a diferencia de los enfoques tradicionales de simulación médica con software (Cook & Triola, 2009), se alinea de forma directa con las tendencias emergentes en la arquitectura de software interactivo y afirmaciones como la de Bhattacharyya et al. (2024), que plantea

que los modelos de lenguaje de gran escala pueden actuar como motores cognitivos altamente eficientes para sustituir los árboles de diálogo lineales.

Por esta razón, la industria del entretenimiento y los videojuegos de última generación tienden también hacia la sustitución de scripts de comportamiento lineales, por NPCs (Non-Player Characters)

gobernados por agentes de inteligencia artificial y modelos de lenguaje locales o híbridos, mostrándonos como Thirunavukarasu et al. (2023) la viabilidad de integrar tecnologías modernas, para reducir los costos y la complejidad de desarrollo de sistemas interactivos que requieran conversaciones naturales, permitiendo además, desde el punto de vista pedagógico, evaluar competencias de comunicación y razonamiento semiológico dinámico de forma alineada a los marcos de evaluación de competencias clínicas integrales planteados por Epstein (2007), pero eliminando la alta variabilidad y los costos logísticos de los pacientes estandarizados humanos (Harden, 2016).

Los resultados obtenidos evidencian la viabilidad técnica de este flujo de trabajo con las API de IA y datos estructurados en el ámbito académico médico, indica que las técnicas aplicadas, no constituyen únicamente una solución paliativa de bajo costo, sino una adopción temprana de estándares tecnológicos actuales.

Limitaciones Técnicas del Marco de Trabajo (Framework)

A pesar de la funcionalidad técnica demostrada en la integración del prototipo, la arquitectura presenta limitaciones sustanciales que deben considerarse para su escalabilidad. En primer lugar, existe una alta dependencia de servicios en la nube y conectividad a internet: el flujo secuencial entre Wit.ai, Gemini 1.5 Flash y Google TTS introduce una latencia que varía según el ancho de banda disponible. En escenarios de red inestables, el retraso en la generación del audio y las animaciones interrumpe la fluidez conversacional esperada en una estación del ECOE. En otras ocasiones se ha detectado incluso al momento de hacer las pruebas en

desarrollo, que en determinados horarios la API de Google, no respondió impidiendo temporalmente el funcionamiento del sistema, a menos que se considere migrar a LLMs locales, lo cual se discute más adelante.

Sobre la naturalidad de las expresiones verbales del avatar virtual al momento de generar su discurso en audio, se ha intentado utilizar la herramienta más humana posible, sin embargo, se recurrió a Google TTS, que, aunque no es la óptima para esto, demuestra ser la única actualmente que ofrece una capacidad consistente para responder sin incurrir en un costo excesivo, y además en español, aspecto del que otras herramientas más naturales carecen.

Finalmente, existe una limitación intrínseca en los modelos de lenguaje (LLM) respecto al riesgo de alucinación estocástica; aunque el archivo JSON actúa como un prompt restrictivo, el modelo genera probabilidades de texto que podrían desviarse de la rigurosidad médica o desviarse del perfil clínico definido del personaje si el usuario formula preguntas fuera de la distribución prevista.

Consideraciones Éticas en la Simulación Clínica con IA Generativa

El empleo de modelos de IA generativa en la formación médica introduce dilemas éticos y pedagógicos críticos que la literatura reciente ha comenzado a abordar (Saaranen et al., 2024). Uno de los aspectos más sensibles es la fidelidad clínica y el sesgo algorítmico: un LLM no supervisado podría inadvertidamente sugerir síntomas erróneos o validar diagnósticos equivocados introducidos por el estudiante, lo que representaría un riesgo para la adquisición de competencias profesionales si no existe un sistema de evaluación docente en paralelo. Asimismo, la

privacidad de los datos es un factor prioritario; la transmisión de interacciones de voz y texto a través de APIs de terceros requiere mecanismos estrictos de anonimización para garantizar que las grabaciones de los estudiantes no sean almacenadas o utilizadas para el entrenamiento de modelos comerciales. Finalmente, la representación gráfica y conductual del paciente virtual debe ser cuidada para evitar la perpetuación de sesgos socioculturales o estereotipos de género y etnicidad en los escenarios clínicos simulados.

Conclusiones

El desarrollo del marco de trabajo interactivo presentado evidencia la viabilidad técnica de integrar modelos de lenguaje de gran escala, reconocimiento de voz y animación procedural para la configuración de entornos de simulación en realidad virtual bajo un enfoque de bajo costo mediante el uso de software accesible.

La arquitectura propuesta permitió desacoplar la lógica del conocimiento médico (digitalizada mediante estructuras JSON modulares) de la capa de ejecución visual en Unity y Blender. El procesamiento semántico mediante la API de Gemini 1.5 Flash mostró consistencia en la generación de información adicional (payloads) estructurada, permitiendo que las entradas de lenguaje natural se traduzcan de manera simultánea en sintaxis de audio y parámetros de animación procedural coherentes.

Como línea futura de investigación, se contempla la realización de pruebas piloto con estudiantes de la carrera de medicina. Dichos estudios, permitirían medir tanto la eficacia pedagógica, como la usabilidad del sistema y posibles inconvenientes como la latencia percibida y la tasa de retención de

competencias frente a los métodos de simulación tradicional. Asimismo, se plantea como horizonte de desarrollo posterior, la exploración de modelos de lenguaje de código abierto y/o de ejecución local, para eliminar la dependencia de servicios en la nube (que se encuentran sujetos a condiciones variables), así como la incorporación de nuevos casos clínicos, como diferentes tipos de pacientes y entornos, la expansión del esquema JSON para poder especificar mejor la información para la simulación, y la integración de módulos de evaluación, registro y reporte automático del desempeño del practicante al finalizar la sesión.

Conflictos de intereses

El autor declara que no existe conflicto de intereses en la elaboración y publicación del presente artículo científico.

Agradecimientos

Al Ing. Franz Villalpando Amonzabel, director de carrera, y al Centro de Producción Multimedia Interactiva de la carrera de Ingeniería en Diseño y Animación Digital, a cargo del Ing. Pedro Camargo Vargas, por haber proporcionado el equipamiento tecnológico sin el cual el desarrollo y las pruebas de este estudio no hubieran sido posibles.

Referencias Bibliográficas

Aristidou, A., Lasenby, J., Chrysanthou, Y., & Shamir, A. (2018). Inverse kinematics: a review of past, present, and future methods. *Computer Graphics Forum*, 37(5), 211-235. <https://doi.org/10.1111/cgf.13442>

Bhattacharyya, S., Miller, J., & Turner, R. (2024). Large language models as cognitive engines in medical simulation: A framework for dynamic patient generation. *Journal of Medical Internet Research*, 26, e54321. <https://doi.org/10.2196/jmir.54321>

Calvo, J. (3 de abril de 2025). Implementación del Examen Clínico Objetivo Estructurado (ECOE) con evaluadores internacionales. Noticias USFX. Universidad Mayor, Real y Pontificia de San Francisco Xavier de Chuquisaca. <https://usfx.bo/2025/04/03/la-carrera-de-medicina-implementara-el-examen-clinico-objetivo-estructurado-ecoe/>

Clusmann, J., Kolbinger, F. R., Muti, H. S., Carrero, Z. I., Eckardt, J. N., Laleh, N. G., ... & Kather, J. N. (2023). The future landscape of large language models in medicine. *Communications Medicine*, 3(1), 141. <https://doi.org/10.1038/s43856-023-00370-1>

Cook, D. A., & Triola, M. M. (2009). Virtual patients: a critical review of their use in medical education. *Medical Education*, 43(4), 303-311. <https://doi.org/10.1111/j.1365-2923.2009.03301.x>

Epstein, R. M. (2007). Assessment in medical education. *New England Journal of Medicine*, 356(4), 387-396. <https://doi.org/10.1056/NEJMr054784>

Google. (2024). Gemini 1.5: Unlocking multimodal understanding across a million tokens of context (Technical Report). Google DeepMind. <https://arxiv.org/abs/2403.05530>

Harden, R. M. (2016). Misconceptions and the OSCE. *Medical Teacher*, 38(1), 26-31. <https://doi.org/10.3109/0142159X.2015.1087483>

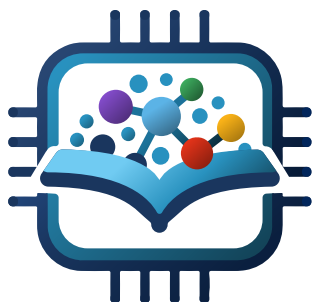
Khan, K. Z., Ramachandran, S., Gaunt, K., & Pushkar, P. (2013). The Objective Structured Clinical Examination (OSCE): AMEE Guide No. 81. Part I: An historical and theoretical perspective. *Medical Teacher*, 35(9), e1437-e1446. <https://doi.org/10.3109/0142159X.2013.818634>

Kyaw, B. M., Saxena, N., Posadzki, P., Vseteckova, J., Nikolaou, C. K., George, P. P., Divakar, U., Masiello, I., Tudor Car, L., & Car, J. (2019). Virtual reality for health professions education: Systematic review and meta-analysis by the Digital Health Education Collaboration. *Journal of Medical Internet Research*, 21(2), e12959. <https://doi.org/10.2196/12959>

Saaranen, T., Kasanen, M., & Haatainen, K. (2024). Ethical considerations of generative artificial intelligence in health professions education and simulation: A narrative review. *Nurse Education Today*, 132, 106012. <https://doi.org/10.1016/j.nedt.2023.106012>

Smee, S. (2003). ABC of learning and teaching in medicine: Skill based assessment. *BMJ*, 326(7391), 703-706. <https://doi.org/10.1136/bmj.326.7391.703>

Thirunavukarasu, A. J., Ting, D. S. J., Elangovan, K., Gutierrez, L., Tan, T. F., & Liu, X. (2023). Large language models in medicine. *Nature Medicine*, 29(8), 1930-1940. <https://doi.org/10.1038/s41591-023-02448-8>



Ciencia & tecnología **D I G I T A L**

Convocatoria 02 - 2026

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 CIBERSEGURIDAD

CONVOCATORIA N° 02/2026

REVISTA CIENCIA Y TECNOLOGÍA DIGITAL

ISSN (impreso): 3107-1929 · e-ISSN: 3107-1937

CONVOCATORIA A PUBLICACIÓN 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 Ciberseguridad**, 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, docentes de universidades nacionales e internacionales, estudiantes de pregrado y posgrado.

3. ESTRUCTURA DE LOS ARTÍCULOS

Para artículos científicos originales (formato IMRyD):

- Título (máx. 20 palabras, claro y conciso).
- Autor(es), afiliación, correo, ORCID.
- Resumen (200 a 220 palabras).
- Palabras clave (3 a 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 afiliación, correo, ORCID.
- Resumen (200 a 220 palabras).
- Palabras clave (3 a 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 Ciberseguridad:

- 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.
- Informática forense 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

Comisión Editorial: Evalúa el cumplimiento del formato, la pertinencia temática y decide la admisión del artículo al proceso de revisión.

Comisión Técnica: Verifica la originalidad y el porcentaje de similitud mediante software especializado.

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. El manuscrito respeta el anonimato exigido para la 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. ENVÍO DE ARTÍCULOS

Fecha límite: Hasta el 31 de octubre de 2026.

Canal oficial de recepción: Los artículos deben enviarse exclusivamente a través de la plataforma Open Journal Systems (OJS).

Procedimiento de envío:

- Acceda al portal de envíos: <https://revistas.usfx.bo/index.php/rctd/about/submissions>
- Regístrese como Autor (si ya tiene cuenta, inicie sesión).
- Cargue su artículo en formato Word editable.
- Adjunte como "Archivo complementario" la Carta de Autorización debidamente firmada.

Plantillas y formatos: Es obligatorio utilizar las plantillas oficiales de la revista, las cuales pueden descargarse desde el siguiente enlace: <https://revistas.usfx.bo/index.php/rctd/information/authors>

Informes:

revista.ctd@usfx.bo

+591 67627048



Acceda a la convocatoria completa, directrices para autores y formatos de envío escaneando el código QR.



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

cib | INGENIERÍA EN
CIBERSEGURIDAD