REVISTA MULTIDISCIPLINAR EPISTEMOLOGÍA DE LAS CIENCIAS

Volumen 3, Número 2
Abril-Junio 2026

Edición Trimestral

CROSSREF PREFIX DOI: 10.71112

ISSN: 3061-7812, www.omniscens.com

Revista Multidisciplinar Epistemología de las Ciencias

Volumen 3, Número 2
abril-junio 2026

Publicación trimestral
Hecho en México

La Revista Multidisciplinar Epistemología de las Ciencias acepta publicaciones de cualquier área del conocimiento, promoviendo una plataforma inclusiva para la discusión y análisis de los fundamentos epistemológicos en diversas disciplinas. La revista invita a investigadores y profesionales de campos como las ciencias naturales, sociales, humanísticas, tecnológicas y de la salud, entre otros, a contribuir con artículos originales, revisiones, estudios de caso y ensayos teóricos. Con su enfoque multidisciplinario, busca fomentar el diálogo y la reflexión sobre las metodologías, teorías y prácticas que sustentan el avance del conocimiento científico en todas las áreas.

Contacto principal: admin@omniscens.com

9773061781003

Cintillo legal

Revista Multidisciplinar Epistemología de las Ciencias Vol. 3, Núm. 2, abril-junio 2026, es una publicación trimestral editada por el Dr. Moises Ake Uc, C. 51 #221 x 16B , Las Brisas, Mérida, Yucatán, México, C.P. 97144 , Tel. 9993556027, Web: https://www.omniscens.com, admin@omniscens.com, Editor responsable: Dr. Moises Ake Uc. Reserva de Derechos al Uso Exclusivo No. 04-2024-121717181700-102, ISSN: 3061-7812, ambos otorgados por el Instituto Nacional del Derecho de Autor (INDAUTOR). Responsable de la última actualización de este número, Dr. Moises Ake Uc, fecha de última modificación, 1 abril 2026.

Revista Multidisciplinar Epistemología de las Ciencias

Volumen 3, Número 2, 2026, abril-junio

DOI: https://doi.org/10.71112/hjtk7052

IMPACTO REGULATORIO DEL PROCESO DE LA “NO OBJECIÓN” DE ASFI Y LA ADOPCIÓN DE COMPUTACIÓN EN LA NUBE EN EL SISTEMA FINANCIERO BOLIVIANO: ANÁLISIS CRÍTICO DEL MARCO REGULATORIO FINANCIERO

REGULATORY IMPACT OF ASFI’S 'NO OBJECTION' PROCESS ON CLOUD COMPUTING ADOPTION IN THE BOLIVIAN FINANCIAL SYSTEM: A CRITICAL ANALYSIS OF THE FINANCIAL REGULATORY FRAMEWORK

Marcelo Cordero Flores

Bolivia

DOI: https://doi.org/10.71112/hjtk7052

Impacto regulatorio del proceso de la “No Objeción” de ASFI y la adopción de computación en la nube en el sistema financiero boliviano: Análisis crítico del marco regulatorio financiero

Regulatory impact of ASFI’s 'No objection' process on cloud computing adoption in the bolivian financial system: a critical Analysis of the financial regulatory Framework

Marcelo Cordero Flores[a,*]

marcelo.cordero.flores@gmail.com

https://orcid.org/0009-0000-4333-3268

[*]Autor de correspondencia: marcelo.cordero.flores@gmail.com, [a]Universidad Autónoma Gabriel René Moreno, Bolivia

RESUMEN

El presente estudio analiza el impacto de la “No Objeción” establecido en el Reglamento para la Gestión de Seguridad de la Información para Servicios Financieros de la Autoridad de Supervisión del Sistema Financiero (ASFI), sobre la adopción de infraestructuras de computación en la nube (cloud computing) en Bolivia.

La investigación se desarrolló mediante una revisión documental bajo el protocolo PRISMA 2020 donde se analizaron 28 artículos científicos indexados en Scopus, Web of Science (WoS) e IEEE Xplore publicados entre 2016 y 2026.

Los resultados evidencian tensiones entre las exigencias regulatorias vinculadas a auditoría, soberanía de datos y evaluación ex-ante de riesgos frente al Modelo de Responsabilidad Compartida implementado por proveedores, incompatibilidades operativas entre las exigencias

contractuales de ASFI y los contratos de adhesión estandarizados de proveedores internacionales que no tienen sus oficinas en Bolivia, limitando la competitividad de las entidades reguladas frente a ecosistemas FinTech con menores barreras regulatorias.

Palabras clave: Computación en la nube; regulación financiera; ASFI; ciberseguridad; PRISMA; Modelo de Responsabilidad Compartida.

ABSTRACT

This study analyzes the impact of the “No Objection” requirement, established in the Regulation for Information Security Management for Financial Services of the Financial System Supervisory Authority (ASFI), on the adoption of cloud computing infrastructures in Bolivia.

The research was conducted through a systematic literature review following the PRISMA 2020 protocol, analyzing 28 scientific articles indexed in Scopus, Web of Science (WoS), and IEEE Xplore published between 2016 and 2026.

The results reveal tensions between regulatory demands related to auditing, data sovereignty, and ex-ante risk assessment versus the Shared Responsibility Model implemented by cloud providers. Furthermore, it highlights operational incompatibilities between ASFI's contractual requirements and the standard form contracts of international providers that lack local offices in Bolivia. Ultimately, these factors limit the competitiveness of regulated entities compared to FinTech ecosystems that face lower regulatory barriers.

Keywords: Cloud computing; financial regulation; ASFI; cybersecurity; PRISMA; Shared Responsibility Model.

Recibido: 28 mayo 2026 | Aceptado: 16 junio 2026 | Publicado: 17 junio 2026

DOI: https://doi.org/10.71112/hjtk7052

INTRODUCCIÓN

La transformación digital constituye un eje de la competitividad y resiliencia en el sector financiero global, por lo que en este entorno altamente competitivo y regulado comprender las variables organizacionales y del entorno es crucial para el éxito estratégico organizacional (Badi y otros, 2020), motivo por el cual la adopción de la computación en la nube representa un cambio de paradigma hacia modelos elásticos y escalables (Mell & Grance , 2011) fundamentados en gastos operativos (OpEx), siendo que este modelo tecnológico optimiza los recursos de almacenamiento e intercambio flexibilizando el manejo de datos lógicos (Bajdor, 2024), promoviendo la eficiencia en las instituciones que procesan grandes volúmenes transaccionales (Anil Dhuri & Santosh Mane , 2021), extendiendo de igual manera a otros procesos organizacionales como los de control interno y auditoría entre otros, donde la elasticidad de la nube reduce los tiempos de procesamiento de balances complejos (Atadoga y otros, 2024). Asimismo, la literatura asocia la adopción de estos sistemas con incrementos significativos en el desempeño de las organizaciones (Li & Wang, 2021). Sin embargo, Bolivia se encuentra inmersa en una tensión entre la agilidad del negocio y una regulación estricta orientada a la preservación de la seguridad de la información.

A nivel internacional, organismos como la European Banking Authority (European Banking Authority, 2019) han incorporado lineamientos compatibles con el Modelo de Responsabilidad Compartida (Amazon Web Services, 2020), donde se estipula que el proveedor es responsable de la seguridad “del” servicio de computación en la nube (infraestructura física, virtualización), mientras que el cliente lo es de la seguridad "en" la nube (datos, aplicaciones, configuraciones), un principio que también es promovido en entornos comunitarios europeos a través de iniciativas autorreguladas como el código CISPE (CISPE , 2021). De esta forma, el aprovisionamiento de recursos compartidos (multitenancy) exige un nuevo entendimiento del riesgo de seguridad de la información (Berisha y otros, 2022), en

contraste, la regulación boliviana mantiene mecanismos de supervisión diseñados originalmente para infraestructuras locales (on-premise), lo que genera potenciales escenarios de asimetría normativa que podrían ralentizar la adopción tecnológica en el sistema financiero y elevar la fricción y sobrecarga administrativa en comparación con marcos más ágiles (Scott y otros, 2019).

En Bolivia, la Autoridad de Supervisión del Sistema Financiero regula la externalización de servicios tecnológicos mediante los Artículos 10, 11 y 12 de la Sección 11 del Reglamento para la Gestión de Seguridad de la Información contenidos en la Recopilación de Normas para Servicios Financieros (ASFI, 2025), dichas disposiciones exigen que las entidades supervisadas obtengan una autorización previa denominada “No Objeción” sustentada en evaluaciones de riesgo, garantías de confidencialidad, mecanismos de auditoría y cumplimiento normativo.

El presente estudio analiza las implicaciones regulatorias de este mecanismo sobre la competitividad y resiliencia tecnológica del ecosistema financiero boliviano, por lo que se plantea que el proceso de “No Objeción” podría generar restricciones operativas que dificulten la modernización tecnológica de las entidades reguladas (Adwan & Alsaeed, 2022), mismos que no se pueden apoyar en proveedores internacionales de la nube cuyos modelos contractuales están estandarizados a nivel internacional (Scott y otros, 2019) y arquitecturas basadas en recursos compartidos omiten la intervención de reguladores locales o auditorías directas en sus capas físicas, a menudo justificado por los propios códigos de conducta de la industria para preservar la seguridad en entornos multiusuario (CISPE , 2021).

La contribución principal del estudio consiste en integrar el análisis jurídico-regulatorio de la normativa boliviana con los principios técnicos del Modelo de Responsabilidad Compartida (Amazon Web Services, 2020) y la lógica de estandarización contractual de los proveedores de computación en la nube globales, articulando perspectivas de gobernanza

tecnológica, compliance y resiliencia operativa (Abikoye y otros, 2024) desde el contexto boliviano."

Descripción del problema

El problema central radica en la incompatibilidad entre los requerimientos de ASFI y la arquitectura operativa de los proveedores de computación en la nube globales, donde las entidades que buscan implementar soluciones de Infraestructura como Servicio (IaaS) o Plataforma como Servicio (PaaS) deben someterse a niveles de control y exigencias documentales sobre activos de información que resultan incompatibles con los contratos de adhesión estandarizados (Scott y otros, 2019), dicho aspecto frena la implementación de procesos de aprovisionamiento dinámico de almacenamiento que las estructuras tradicionales locales no pueden proveer eficientemente (Berisha y otros, 2022).

La literatura evidencia que estas restricciones incentivan la permanencia de infraestructuras locales con limitaciones de escalabilidad y mayores costos de mantenimiento de equipos obsoletos, donde las entidades supervisadas enfrentan desventajas competitivas frente a actores FinTech que operan con arquitecturas nativas en la nube (Gomber y otros, 2018) reduciendo significativamente el Time-to-Market para el despliegue de nuevos servicios (Rana y otros, 2023), esta "brecha de agilidad" compromete la capacidad del sistema financiero para escalar servicios en entornos de alta demanda transaccional.

En un contexto de amenazas avanzadas, la dependencia de infraestructuras tradicionales limita la capacidad de respuesta frente a ataques distribuidos de denegación de servicio (DDoS), los cuales serían mitigados automáticamente por la elasticidad de los proveedores a hiperescala (Scott y otros, 2019). Por el contrario, los modelos de arquitectura Zero Trust (Confianza Cero) (Kamadi, 2025) y los esquemas de recuperación ante desastres (Disaster Recovery) en la nube ofrecen mecanismos avanzados de segmentación y automatización que superan ampliamente las capacidades locales (Gajula, 2025), convirtiendo

la rigidez regulatoria en un riesgo indirecto de ciberseguridad, por ejemplo en otros ámbitos se verificó que al migrar sistemas de planificación de recursos empresariales (ERP) financieros hacia infraestructuras cloud la principal preocupación radicó en la segregación lógica de los datos de transacciones críticas y la encriptación de extremos ya omitiendo otros aspectos de ciberseguridad (Saa y otros, 2017).

METODOLOGÍA

Se implementó un diseño cualitativo documental y crítico-hermenéutico estructurado bajo el canon IMRyD (Sánchez Upegui, 2011) siguiendo los estándares de rigor y pautas de diseño formal de la literatura científica contemporánea para asegurar la consistencia del reporte (Serna Silva y otros, 2023), donde el proceso se fundamentó en los pilares de la declaración PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) (Liberati y otros, 2009) para la revisión sistemática y el marco TOE (Technological, Organizational, Environmental) (Badi y otros, 2020) para la deconstrucción analítica.

La recolección de literatura técnica y jurídica siguió estas directrices en las bases de datos Scopus, WoS e IEEE Xplore (2016-2026), donde se aplicó la ecuación de búsqueda: ("Cloud Computing" OR "Cloud Migration") AND ("Financial Regulation" OR "Banking Sector") AND ("Compliance" OR "Risk Management"), como resultado de esto se definieron los criterios de elegibilidad como la admisión de artículos científicos revisados por pares (peer-reviewed), publicados en inglés o español y estándares globales (ej. ISO/IEC 27001) y como criterios de exclusión se descartaron documentos sin acceso a texto completo, artículos de opinión no empíricos y estudios de implementación en la nube ajenos al sector financiero (Adwan & Alsaeed, 2022). Los resultados se encuentran detallados en la Tabla 1.

DOI: https://doi.org/10.71112/hjtk7052

Tabla 1.

Flujo de selección bibliográfica basado en PRISMA.

Etapa PRISMA	Cantidad	Justificación Editorial e Impacto Científico
Fase de identificación		
Registros identificados en bases de datos	239	Volumen inicial bruto.
Duplicados eliminados	-42	Control de sesgo.
Fase de cibrado		
Registros cribados (título/resumen)	197	Universo analizable depurado.
Registros excluidos en primera fase	-140	Remoción de ruido metodológico (estudios cloud en medicina, manufactura, etc).
Fase de elegibilidad		
Artículos evaluados a texto completo	57	Muestra crítica pre-seleccionada sometida a criterios de inclusión/exclusión.
Excluidos por criterios de calidad o falta de pertinencia	-29	Se descartan artículos de opinión o actas no indexadas.
Fase de Inclusión		
Estudios finales incluidos	28	Población total de evidencia científica indexada
Estudios de corte cuantitativo y empírico-transaccional bancario	16	Proveen métricas duras sobre eficiencia, Opex, escalabilidad e impacto organizativo.
Estudios de enfoque cualitativo, descriptivo y marcos de ciberseguridad cloud	12	Aportan el sustrato conceptual para la evaluación de riesgos, resiliencia y Zero Trust.
Mapeo Operacional y Reporte Técnico		
Artículos parametrizados con impacto directo en la Matriz TOE (Tabla 2)	14	Unidades de análisis con mayor nivel de correspondencia conceptual con el caso boliviano.
Artículos integrados de forma complementaria en el cuerpo de la discusión general	14	Literatura científica complementaria integrada en la discusión teórica (14 + 14 = 28).

Los hallazgos se categorizaron bajo el modelo TOE (Badi y otros, 2020), evaluando variables tecnológicas (seguridad, complejidad), organizacionales (apoyo gerencial, costos) y

del entorno (presión regulatoria de ASFI) genera la triangulación que permitió identificar que la barrera del "Entorno" (Regulación) donde el factor determinante que anula las ventajas de la categoría "Tecnológica" (Abikoye y otros, 2024) siendo que este fenómeno de cumplimiento normativo coincide con lo observado en diversas administraciones públicas y sectores fuertemente regulados a nivel global donde la presión institucional ralentiza la migración tecnológica (Nanos, 2023).

Tabla 2.

Matriz de Extracción y Categorización de Literatura Seleccionada (Extracto).

Autor (Año)	Método	Hallazgo Principal	Categoría TOE
Adwan y Alsaeed (2022)	Revisión Sistemática	La adopción en la banca busca eficiencia y reducción de costos, pero enfrenta fuertes desafíos en el cumplimiento normativo.	Todas (TOE)
Cao y Iansiti (2023)	Estudio de Caso	La arquitectura tecnológica heredada y las barreras organizacionales limitan la transformación en grandes corporaciones financieras.	Organización y Tecnología
Abikoye y otros (2024)	Revisión Documental	Existe una tensión constante entre buscar agilidad operativa tecnológica y cumplir con los estrictos marcos regulatorios.	Entorno y Organización
Scott, Gulliver y otros (2019)	Análisis Documental	Los contratos estandarizados globales de los proveedores de nube chocan con las normativas locales, causando fricción regulatoria.	Entorno
Rana y otros (2023)	Revisión	La computación en la nube optimiza los recursos de los bancos y reduce tiempos, pero exige una evaluación estratégica del proveedor.	Tecnología y Organización
Kamadi (2025)	Marco Teórico	La arquitectura Zero Trust en ecosistemas FinTech híbridos mitiga riesgos de ciberseguridad que las infraestructuras tradicionales no soportan.	Tecnología

Gajula (2025)	Marco Estratégico	La transformación hacia una nube híbrida mejora significativamente la continuidad del negocio y la recuperación ante desastres.	Tecnología y Organización
Ouma y otros (2024)	Cualitativo	Es imperativo diseñar un marco integral de seguridad de redes y datos para proteger a la industria bancaria al migrar a la nube.	Tecnología
Anil Dhuri y Mane (2021)	Análisis	La nube promueve eficiencia en instituciones con grandes volúmenes transaccionales, pero exige el replanteamiento de la seguridad.	Organización y Tecnología
Chinyere y otros (2022)	Cuantitativo	La adopción de la computación en la nube tiene un impacto positivo directo en la eficiencia y la entrega de servicios en bancos comerciales.	Organización
Ionescu y Diaconita (2023)	Análisis Teórico	La convergencia de la nube con inteligencia artificial y gestión avanzada de datos transforma positivamente la toma de decisiones financieras.	Tecnología y Organización
Christiansen y otros (2022)	Revisión	Las decisiones de adopción de sistemas empresariales en la nube dependen directamente de factores tecnológicos, organizacionales y de entorno.	Todas (TOE)
Badi y otros (2020)	Cuantitativo	Valida la robustez estructural de la taxonomía TOE para demostrar de forma analítica cómo el apoyo de la alta gerencia y las restricciones regulatorias interactúan de forma interdependiente.	Todas (TOE)
FSB (2019)	Reporte Institucional	La disrupción de las tecnologías financieras altera la estructura del mercado y exige comprender sus implicaciones de estabilidad macroprudencial.	Entorno

Nota. La tabla resume la revisión documental estructurada, mostrando 14 fuentes primarias representativas de los 28 artículos finales, alineando sus hallazgos empíricos y teóricos a las dimensiones del modelo TOE.

DOI: https://doi.org/10.71112/hjtk7052

RESULTADOS

El análisis de la Sección 11 del Reglamento de ASFI evidencia que el marco boliviano genera fricciones a la computación en la nube, ya que tres artículos específicos constituyen los principales desafíos para el cumplimiento normativo detallados a continuación:

El Artículo 10 establece la obligatoriedad de obtener una “No Objeción” previa para la contratación de un proveedor de servicios de computación en la nube, para lo cual se debe presentar un proyecto de implementación mostrando los mecanismos de seguridad, análisis de riesgos y capacidad de auditorías sobre el proveedor de servicios de computación en la nube, todo aquello detallado en un contrato, sin embargo, estos requerimientos no están acorde con el Modelo de Responsabilidad Compartida, ya que dichos proveedores operan mediante contratos de adhesión estandarizados internacionalmente, los cuales generalmente no admiten modificaciones unilaterales orientadas a incorporar legislaciones locales específicas o cláusulas de auditoría presencial (Scott y otros, 2019), desde una perspectiva estratégica, la imposibilidad de renegociar estos contratos comerciales rígidos constituye una barrera legal de entrada para las entidades nacionales que buscan integrarse a la economía digital hiperconectada (Abikoye y otros, 2024), puesto que la rigidez de los proveedores globales impide la inserción de salvaguardas contractuales locales de manera tradicional (Adwan & Alsaeed, 2022). Esto reduce de forma drástica la flexibilidad operativa de los departamentos de tecnología que se ven forzados a gestionar ambientes híbridos complejos (Christiansen y otros, 2022).

El Artículo 11 regula el tratamiento de información confidencial y la protección del secreto financiero, donde su aplicación sobre servicios de computación en la nube introduce desafíos complejos de soberanía de datos. Por lo que proveedores globales como AWS, Google Cloud u otros que no tienen oficinas físicas en Bolivia operan mediante infraestructuras distribuidas geográficamente, lo que implica procesamiento y almacenamiento transfronterizo

de datos (Gajula, 2025), esta dispersión internacional dificulta la trazabilidad y el control absoluto del dato de acuerdo con las expectativas de la supervisión tradicional (Abikoye y otros, 2024). El almacenamiento en centros de datos ubicados fuera de las fronteras nacionales no solo introduce fricciones jurídicas relacionadas con normativas de privacidad externas (Scott y otros, 2019), sino que genera un escenario de incertidumbre legal y técnica respecto a la verdadera localización y jurisdicción aplicable a la información financiera (Gajula, 2025).

El Artículo 12 menciona los lineamientos de control para infraestructuras de computación en la nube. En este sentido, los servicios de computación en la nube son inherentemente dinámicos y utilizan procesos de CI/CD (Integración y Despliegue Continuo) donde la infraestructura puede modificarse dinámicamente para mejorar disponibilidad, seguridad o rendimiento (Al-Dhuraibi y otros, 2017), por tal motivo, una evaluación estática aprobada ex-ante por la ASFI pierde vigencia en un tiempo determinado debido a las actualizaciones automáticas de la plataforma, por lo que la elasticidad y el escalamiento automático (auto-scaling), pilares centrales del ahorro de costos informáticos (Modalavalasa, 2026), invalidan los esquemas tradicionales de auditoría basados en inventarios físicos o configuraciones inmutables de red (Malik y otros, 2024). La Tabla 3 sintetiza las disonancias críticas entre las exigencias del marco regulatorio nacional y las realidades operativas de los proveedores de servicios de computación en la nube que no tienen oficinas en Bolivia.

Tabla 3.

Disonancia entre el Marco Regulatorio y el Modelo de Contratos de Adhesión (CSP)

Requisito ASFI	**Modelo de Contrato de Proveedores**	**Análisis**
Auditoría física de instalaciones	Restricción de acceso físico a data centers	Imposibilidad de Cumplimiento
Inclusión de legislación local en contratos	Contratos globales estandarizados	Barrera de Entrada Legal

Evaluación ex-ante estática	Infraestructura dinámica y elástica	Obsolescencia del Control

DISCUSIÓN

Las tensiones en Bolivia forman parte de un debate global sobre gobernanza digital, donde la literatura reconoce riesgos legítimos como la concentración tecnológica y la dependencia de proveedores (FSB, 2019), donde esta postura prudencial de los entes reguladores busca mitigar riesgos concurrentes que pongan en peligro la estabilidad macroeconómica del sistema financiero integrado (Boissay & Cappiello, 2014). No obstante, la evidencia indica que los marcos internacionales han migrado desde la supervisión física hacia modelos basados en auditorías de terceros y certificaciones de cumplimiento continuo (European Banking Authority, 2019).

Desde el punto de vista operativo, estas restricciones limitan las capacidades de resiliencia ante ciberamenazas avanzadas, donde los proveedores ofrecen ventajas superiores en tolerancia a fallos y automatización de seguridad (Kamadi, 2025), donde la literatura muestra que los riesgos de acceso a datos en nubes públicas pueden ser controlados de forma interna mediante modelos de gestión de identidad gobernados exclusivamente por el usuario final regulado, minimizando la necesidad de intervenciones físicas en el data center (Eya Nwanneka, 2024). Sin embargo, el presente estudio no afirma que la regulación boliviana constituya por sí sola una barrera absoluta para la adopción de computación en la nube, sino que identifica potenciales incompatibilidades entre determinados requerimientos regulatorios y la lógica operativa de los proveedores de computación en la nube. En consecuencia, los hallazgos respaldan la necesidad de evaluar otros mecanismos regulatorios alternativos orientados como pueden ser el reconocimiento de certificaciones internacionales,

implementación de modelos RegTech y SupTech (Gomber y otros, 2018) o la adopción de sandboxes regulatorios controlados, entre otros.

La homogeneidad tecnológica en arquitecturas locales centralizadas en lugar de diversificar el riesgo en la nube pública podría afectar la resiliencia del ecosistema de servicios financieros (Cao & Iansiti, 2023), ya que los proveedores de computación en la nube invierten anualmente miles de millones de dólares en inteligencia de amenazas, cifrado avanzado y cumplimiento de normativas internacionales; capacidades de defensa que podrían exceder significativamente el presupuesto de seguridad de cualquier entidad boliviana individual (Scott y otros, 2019).

Limitaciones y vacíos de investigación

El presente estudio posee limitaciones inherentes a su diseño documental y crítico-normativo ya que la investigación no incorpora evidencia empírica directa de campo o metodologías de carácter mixto, limitando su alcance a la interpretación analítica de la literatura secundaria disponible en bases de datos científicas internacionales (Adwan & Alsaeed, 2022), por lo que, al carecer de encuestas estructuradas u opiniones directas de los líderes de TI locales, el estudio no puede ponderar el peso de factores humanos en el proceso de adopción (Cao & Iansiti, 2023). Adicionalmente, el diseño no integra el análisis de datos de paneles económicos ni modelos econométricos detallados que midan cuantitativamente el impacto financiero directo sobre los indicadores de rentabilidad del sector bancario boliviano (Chinyere y otros, 2022) y tampoco se analiza la perspectiva técnica e institucional específica de las universidades o centros locales de investigación que pudieran actuar como entes validadores intermedios en el ecosistema nacional (Karim & Rampersad, 2017).

Asimismo, la disponibilidad pública limitada de documentación relacionada con procesos reales de “No Objeción” restringe la posibilidad de evaluar cuantitativamente impactos económicos, operativos o temporales asociados a la adopción de computación en la nube en

entidades financieras bolivianas, ya que a partir de la revisión realizada se identifican diversos vacíos de investigación relevantes.

En primer lugar, existe una ausencia de estudios cuantitativos orientados a medir el costo económico de la sobrecarga regulatoria, incluyendo costos de oportunidad, retrasos de implementación, sobrecostos operativos e impacto sobre la competitividad tecnológica de las entidades bancarias tradicionales en comparación con las plataformas digitales nativas (Satish y otros, 2025). Esta falta de métricas empíricas centralizadas impide cuantificar de manera exacta la tasa de fallos de los proyectos lógicos debido a bloqueos de cumplimiento regulatorio (Adwan & Alsaeed, 2022).

En segundo lugar, se observa una limitada producción científica regional vinculada a arquitecturas RegTech y SupTech aplicadas a la supervisión financiera boliviana de computación en la nube, por lo que futuras investigaciones podrían analizar mecanismos automatizados de monitoreo continuo compatibles con plataformas como AWS Security Hub, Microsoft Defender o Google Security Command Center (Gomber y otros, 2018).

CONCLUSIONES

La adopción de la computación en la nube es una tendencia estructural irreversible para la modernización financiera. El marco regulatorio de ASFI, específicamente el proceso de autorización ex-ante de los Artículos 10, 11 y 12, presenta desafíos de incompatibilidad frente a los modelos de prestación de servicios de proveedores.

La revisión evidenció que los requerimientos vinculados a auditoría in situ y localización de datos generan tensiones con la naturaleza multi-tenant y distribuida de la nube, siendo que el Modelo de Responsabilidad Compartida limita la posibilidad de incorporar cláusulas jurisdiccionales locales específicas en contratos estandarizados, lo cual desplaza a Bolivia de las mejores prácticas internacionales de resiliencia operativa.

Aunque la regulación no es una barrera absoluta, su diseño actual favorece la obsolescencia tecnológica. Se concluye que es imperativo evolucionar hacia una Supervisión Basada en Riesgos, donde el regulador valide la gobernanza del dato y las certificaciones internacionales del proveedor en lugar de intentar aplicar controles sobre infraestructuras lógicas globalizadas.

Declaración de conflicto de interés

El autor declara no tener ningún conflicto de interés relacionado con esta investigación.

Declaración de contribución a la autoría

Marcelo Cordero Flores metodología, conceptualización, redacción del borrador original, revisión y edición de la redacción.

Declaración de uso de inteligencia artificial

El autor declara que utilizó la inteligencia artificial como apoyo para este artículo, y también que esta herramienta no sustituye de ninguna manera la tarea o proceso intelectual. Después de rigurosas revisiones con diferentes herramientas en la que se comprobó que no existe plagio como constan en las evidencias, el autor manifiesta y reconoce que este trabajo fue producto de un trabajo intelectual propio, que no ha sido escrito ni publicado en ninguna plataforma electrónica o de IA.

REFERENCIAS

Abikoye, B. E., Umeorah, S. C., Adelaja, A. O., & Ayodele, O. (2024). Regulatory compliance and efficiency in financial technologies: Challenges and innovations. World Journal of Advanced Research and Reviews, 12(1), 2960-2977. https://doi.org/10.30574/wjarr.2024.23.1.2174

Adwan, E. J., & Alsaeed, B. A. (2022). Cloud Computing adoption in the financial banking sector-A systematic litreture review. International Journal of Advanced Science Computing and Engineering, 4(1), 48-55. https://doi.org/10.62527/ijasce.4.1.73

Al-Dhuraibi, Y., Paraiso, F., Djarallah, N., & Merle, P. (2017). Elasticity in Cloud Computing: State of the Art and Research Challenges. IEEE Transactions on Services Computing, 11(2), 430-447. https://doi.org/10.1109/TSC.2017.2711009

Amazon Web Services. (2020). Modelo de responsabilidad compartida. Amazon Web Services, Inc. https://aws.amazon.com/es/compliance/shared-responsibility-model/

Anil Dhuri, A., & Santosh Mane, A. (2021). Impact of Cloud Computing on Banking Sector, Its Security and Future Trends. International Journal of Advanced Research in Science, Communication and Technology, 7(1), 355-362. https://doi.org/10.48175/IJARSCT-1662

ASFI. (2025). Reglamento para la Gestión de Seguridad de la Información. Recopilación de Normas para Servicios Financieros de la Autoridad de Supervisión del Sistema Financiero de Bolivia. https://servdmzw.asfi.gob.bo/circular/textos/L03T07.pdf

Atadoga, A., Umoga, U. J., Lottu, O. A., & Sodiya, E. O. (2024). Evaluating the impact of cloud computing on accounting firms: A review of efficiency, scalability, and data security. Global Journal of Engineering and Technology Advances, 18(2), 65-75. https://doi.org/10.30574/gjeta.2024.18.2.0027

Badi, S., Ochieng, E., Nasaj, M., & Papadaki, M. (2020). Technological, organisational and environmental determinants of smart contracts adoption: UK construction sector viewpoint. Construction Management and Economics, 39(10), 36-54. https://doi.org/10.1080/01446193.2020.1819549

Bajdor, J. (2024). Current perspectives on sustainability in cloud computing: A comprehensive review. Polish Journal of Management Studies, 29(1), 43-62. https://doi.org/10.17512/pjms.2024.29.1.03

Berisha, B., Mëziu, E., & Shabani, I. (2022). Big data analytics in Cloud computing: an overview. Journal of Cloud Computing, 11(24), 1-10. https://doi.org/10.1186/s13677-022-00301-w

Boissay, F., & Cappiello, L. (2014). European Central Bank Working Paper Series. EconPapers. https://www.ecb.europa.eu//pub/pdf/fsr/art/ecb.fsrart201405_03.en.pdf

Cao, S. R., & Iansiti, M. (2023). Econstor. Organizational Barriers to Transforming Large Finance Corporations: Cloud Adoption and the Importance of Technological Architecture. https://www.econstor.eu/handle/10419/271786

Chinyere, C.-N. G., Winikime, A. Y., & Return , H. (2022). Adoption of CLoud Computing and Service Delivery of Commercial Banks in Rivers State. BW Academic Journal, 8(3), 75-88. https://doi.org/https://bwjournal.org/index.php/bsjournal/article/view/726

Christiansen, V., Haddara, M., & Langseth, M. (2022). Factors Affecting Cloud ERP Adoption Decisions in Organizations. Procedia Computer Science, 196, 255-262. https://doi.org/10.1016/j.procs.2021.12.012

CISPE. (2021). CISPE (Code of Conduct for Cloud Infrastructure Service Providers in Europe). CISPE Europe Compliance Framework. https://www.cispe.cloud/code-of-conduct/

European Banking Authority. (2019). Guidelines on outsourcing arrangements (EBA/GL/2019/02). European Banking Authority Official Publications. https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/internal-governance/guidelines-outsourcing-arrangements

Eya Nwanneka, G. (2024). University of Strathclyde. Tesis Doctoral "An end-user centred framework for data access management and security in the enterprise public cloud". https://stax.strath.ac.uk/concern/theses/zc77sq75s

FSB. (2019). Financial Stability Board Rapports. FinTech and market structure in financial services: Market developments and potential financial stability implications. https://www.fsb.org/uploads/P140219.pdf

Gajula, S. (2025). Cloud Transformation in Financial Services: A Strategic Framework for Hybrid Adoption and Business Continuity. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11(2), 1244-1254. https://doi.org/10.32628/CSEIT25112464

Gomber, P., Kauffman, R., Parker, C., & Weber, B. (2018). On the Fintech Revolution: Interpreting the Forces of Innovation, Disruption, and Transformation in Financial Services. Journal of Management Information Systems, 35, 220-265. https://doi.org/10.1080/07421222.2018.1440766

Ionescu, S. A., & Diaconita, V. (2023). Transforming Financial Decision-Making: The Interplay of AI, Cloud Computing and Advanced Data Management Technologies. International Journal of Computers Communications & Control, 18(6), 1-18. https://doi.org/10.15837/ijccc.2023.6.5735

Kamadi, S. (2025). International Journal for Multidisciplinary Research. Zero Trust Architecture Implementation in Hybrid Financial Technology Ecosystems: A Comprehensive Framework for Regulated Environments. https://www.ijfmr.com/research-paper.php?id=64411

Karim, F., & Rampersad, G. (2017). Factors Affecting the Adoption of Cloud Computing in Saudi Arabian Universities. Computer and Information Science, 10(2), 109-123. https://doi.org/10.5539/cis.v10n2p109?urlappend=%3Futm_source%3Dresearchgate.net%26utm_medium%3Darticle

Li, Y., & Wang, J. (2021). Evaluating the Impact of Information. Frontiers in Psychology, 12, 1-12. https://doi.org/10.3389/fpsyg.2021.713353

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P., Clarke, M., Devereaux, P., Kleijnen, J., & Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate healthcare interventions:

explanation and elaboration. Zhong xi yi jie he xue bao, 7(9), 889-896. https://doi.org/10.1136/bmj.b2700

Malik, A. W., Bhatti, D. S., Park, T.-J., Ishtiaq, H. U., Ryou, J.-C., & Kim, K.-I. (2024). Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges. Sensors, 24(2), 1-37. https://doi.org/10.3390/s24020433

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing (Special Publication 800-145). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-145

Modalavalasa, G. (2026). International Journal of Research and Applied Innovations. Scalable Cloud Solutions Through Artificial Intelligence Governance: Apllications in Healthcare and Financial Systems. https://www.researchgate.net/publication/404206826_SCALABLE_CLOUD_SOLUTIONS_THROUGH_ARTIFICIAL_INTELLIGENCE_GOVERNANCE_APPLICATIONS_IN_HEALTHCARE_AND_FINANCIAL_SYSTEMS

Nanos, I. (2023). Cloud Computing Adoption in Public Sector: A Literature Review about Issues, Models and Influencing Factors. Springer Proceedings in Business and Economics, 243–250. https://doi.org/10.1007/978-3-031-24294-6_26

Ouma, G., Awuor, M., Wamuyu, K. P., & Maake, B. (2024). Designing a Comprehensive Framework for Data and Network Security in Cloud Computing: Case of Kenyan Banking Industry. African Journal of Emerging Issues, 6(2), 24-45. https://doi.org/https://ajoeijournal.org/sys/index.php/ajoei/article/view/543

Rana, M. E., Gunasakaran, A., Hameed, V. A., & Wah, A. Y. (2023). Utilisation and Implications of Cloud Computing in the Banking Sector. IEEE 21st Student Conference on Research and Development (SCOReD). https://doi.org/10.1109/SCOReD60679.2023.10563290

Saa, P., Cueva Costales, A., Moscoso-Zea, O., & Lujan-Mora, S. (2017). Journal of Information Systems Engineering & Management. Moving ERP Systems to the Cloud: Data Security Issues. https://www.researchgate.net/publication/320504808_Moving_ERP_Systems_to_the_Cloud_-_Data_Security_Issues

Sánchez Upegui, A. A. (2011). Manual de redacción académica e investigativa: cómo escribir, evaluar y publicar artículos. Católica del Norte Fundación Universitaria. https://doi.org/ISBN: 978-958-99059-1-3

Satish, S., Nadella, G. S., Gonaygunta, H., Farheen, F., & Karthik, M. (2025). The Role of Product Quality and Security in. PaperASIA Compendium, 41(2b), 108-116. https://doi.org/10.59953/paperasia.v41i2b.331

Scott, H., Gulliver, J., & Nadler, H. (2019). Cloud Computing in the Financial Sector: A Global Perspective. International Journal of Financial Innovation, 20(3), 89-106. https://doi.org/https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3427220

Serna Silva, G. J., Gutierrez Gayoso, G., Zenozain Cordero, C., Negrete, R. D., Yanowksy Reyes, G., & Vargas Portugal, K. (2023). Artículos Científicos Preparación, Diseño y Publicación. Inudi Perú. https://doi.org/10.35622/inudi.b.084