FACULTAD DE POSTGRADO

TESIS DE POSTGRADO

ANÁLISIS DEL ESTADO ACTUAL DE PROTECCIÓN DE DATOS EN SOLUCIONES DE IA DEL SISTEMA FINANCIERO HONDUREÑO.

SUSTENTADO POR:

Darry Jafet Padilla Torres 12423147

Omar de Jesús Ramírez Pacheco 12423062

PREVIA INVESTIDURA AL TÍTULO DE

MAESTRÍA EN GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

TEGUCIGALPA, FRANCISCO MORAZÁN, HONDURAS, C.A.

ABRIL, 2026

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA

UNITEC

FACULTAD DE POSTGRADO

AUTORIDADES UNIVERSITARIAS

RECTORA

ROSALPINA RODRÍGUEZ

SECRETARIO GENERAL / PRORRECTOR

ROGER MARTÍNEZ MIRALDA

VICERRECTOR ACADÉMICO NACIONAL

JAVIER ABRAHAM SALGADO LEZAMA

DIRECTORA NACIONAL DE POSTGRADO

ANA DEL CARMEN RETALLY VARGAS

ANÁLISIS DEL ESTADO ACTUAL DE PROTECCIÓN DE DATOS EN SOLUCIONES DE IA DEL SISTEMA FINANCIERO HONDUREÑO.

TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO DE MÁSTER EN

MAESTRÍA EN GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

ASESOR METODOLÓGICO

JUAN JACOBO PAREDES HELLER

FACULTAD DE POSTGRADO

ANÁLISIS DEL ESTADO ACTUAL DE PROTECCIÓN DE DATOS EN SOLUCIONES DE IA DEL SISTEMA FINANCIERO HONDUREÑO.

AUTORES:

Darry Jafet Padilla Torres & Omar de Jesús Ramírez Pacheco.

RESUMEN

La investigación evaluó el estado de la protección de datos personales en las soluciones de inteligencia artificial implementadas por entidades del sistema financiero hondureño, considerando tanto el contexto regulatorio nacional como las prácticas institucionales vinculadas al tratamiento automatizado de información sensible. Se analizó el uso de modelos de IA en procesos específicos del sistema financiero hondureño, con énfasis en la identificación de controles de seguridad y mecanismos básicos de transparencia y gobernanza de datos adoptados por las organizaciones. Del mismo modo, se examinó el grado de alineación de estas prácticas con principios de privacidad tales como licitud, minimización, finalidad, transparencia y responsabilidad, a partir de la revisión de fuentes documentales, normativas y técnicas. Los resultados evidenciaron avances en la adopción de tecnologías algorítmicas, pero también brechas significativas en la realización de

evaluaciones de impacto en privacidad, en la explicabilidad de las decisiones automatizadas y en la existencia de regulación específica sobre datos personales. Finalmente, se formularon recomendaciones orientadas a robustecer la gobernanza de datos, elevar la transparencia frente a los usuarios y orientar a entidades financieras y reguladores hacia una implementación más responsable de soluciones de IA.

Palabras clave: algoritmos, banca digital, inteligencia artificial, protección de datos, regulación.

GRADUATE SCHOOL

ANÁLISIS DEL ESTADO ACTUAL DE PROTECCIÓN DE DATOS EN SOLUCIONES DE IA DEL SISTEMA FINANCIERO HONDUREÑO.

AUTHORS:

Darry Jafet Padilla Torres & Omar de Jesús Ramírez Pacheco.

ABSTRACT

The study assessed the status of personal data protection in artificial intelligence solutions implemented by entities in the Honduran financial system, considering both the national regulatory context and institutional practices related to the automated processing of sensitive information. It analyzed the use of AI models in specific processes within the Honduran financial system, with emphasis on identifying security controls and basic mechanisms of data transparency and governance adopted by organizations. Likewise, it examined the degree of alignment of these practices with privacy principles such as lawfulness, data minimization, purpose limitation, transparency, and accountability, based on a review of documentary, regulatory, and technical sources. The results showed

progress in the adoption of algorithmic technologies, but also significant gaps in the performance of privacy impact assessments, in the explainability of automated decisions, and in the existence of specific regulation on personal data. Finally, recommendations were formulated aimed at strengthening data governance, enhancing transparency toward users, and guiding financial institutions and regulators toward a more responsible implementation of AI solutions.

Keywords: algorithms, digital banking, artificial intelligence, data protection, regulation.

DEDICATORIA

A Dios, por ser fuerza, sabiduría y sustento cada día; a su amor y misericordia, infinita, por darme la fortaleza y la inteligencia, infinita gratitud.

A mis abuelos, Alejandra Del Carmen Zúniga y Oscar David Torres, por el apoyo y formar parte de este proyecto de mi vida.

A mis tíos/as, por su apoyo, cariño y por acompañarme en este camino de crecimiento.

A mis hermanos, por el apoyo incondicional, su confianza y por motivación.

A mi madre Mery Lisseth Torres Zúniga, por ser mi mayor inspiración, por su amor, paciencia y apoyo. Infinitas gracias.

Darry Jafet Padilla Torres.

Dedico este trabajo, en primer lugar, a Dios, por la vida, la fortaleza y la sabiduría con que me ha guiado cada paso de esta etapa.

A mis padres, Mauricio Ramírez y Martha Pacheco, cuyo amor y ejemplo de integridad han sido la base de mis logros.

A mis hijas, Alicia Noemí y Abril Paulina, fuente diaria de inspiración y razón de mi perseverancia, con el deseo de heredarles un legado de esfuerzo y fe.

A mi amada, Genesis Medina, por su amor, paciencia y apoyo constante a lo largo de este camino.

Y, finalmente, a mi mascota Brownie, por su leal compañía en las largas jornadas de estudio y trabajo.

Omar de Jesús Ramírez Pacheco.

AGRADECIMIENTOS

A Dios, gracias por tu fidelidad, misericordia y amor, porque en medio de las exigencias de este posgrado fuiste fuente de fortaleza, dirección y esperanza, permitiéndonos culminar con éxito esta etapa académica. Agradecemos profundamente a los docentes de la maestría, por su entrega, paciencia y rigurosidad académica, que no solo fortalecieron nuestros conocimientos, sino también nuestro criterio profesional y ético. Extendemos este agradecimiento a la universidad y al personal administrativo que facilitaron los recursos, espacios y acompañamiento necesarios para el desarrollo del trabajo de investigación.

De manera muy especial, agradecemos a nuestra familia, por ser nuestro apoyo constante, por sus palabras de ánimo, comprensión y sacrificios silenciosos; su amor fue el sostén que nos impulsó a perseverar hasta el final y a transformar este logro en un testimonio de esfuerzo compartido.

ÍNDICE DE CONTENIDO

CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

En este primer capítulo se exponen las generalidades de este estudio, es decir, se realiza una introducción al tema análisis del estado actual de protección de datos en soluciones de IA del sistema financiero hondureño, para posteriormente presentar los antecedentes del problema y, la definición de este, abarcando aspectos como el enunciado del problema, la formulación del problema y las preguntas de investigación. De igual manera, se describen los objetivos generales y específicos planteados, finalizando con la justificación de este estudio.

1.1 INTRODUCCIÓN

La transformación digital ha generado un impacto significativo en el sector financiero, impulsando la incorporación de tecnologías avanzadas como la inteligencia artificial (IA) para optimizar procesos internos, mejorar la atención al cliente, prevenir fraudes y personalizar productos financieros (Aldboush et al., 2023). En Honduras, los bancos y entidades financieras han comenzado a implementar soluciones basadas en IA en diversas áreas operativas, incluyendo la evaluación de riesgos crediticios, la detección de transacciones sospechosas y la atención automatizada al cliente (U.S. Department of Commerce, 2024). Esta digitalización plantea importantes desafíos en términos de protección de datos, ya que la recopilación, procesamiento y almacenamiento de información personal sensible debe cumplir con las disposiciones generales o regulaciones de protección de datos personales de Honduras y con los estándares internacionales de privacidad (Ridzuan et al., 2024). La confianza del cliente en los servicios financieros digitales depende de la percepción de que sus datos están resguardados y que las decisiones automatizadas se realizan de forma ética y transparente (Srivastava et al., 2024).

El enfoque de esta investigación se centra en el análisis del estado actual de la protección de datos en soluciones de IA dentro del sistema financiero hondureño, con el objetivo de identificar fortalezas, debilidades y vacíos regulatorios que puedan comprometer la privacidad de los clientes. Si bien la literatura internacional ha abordado el uso de IA en la banca y sus implicaciones en la privacidad, en el contexto centroamericano y específicamente en Honduras existe poca evidencia científica que detalle cómo se gestionan los riesgos relacionados con los datos personales, las decisiones automatizadas y la transparencia algorítmica (Jim et al., 2024). Esto evidencia un vacío de conocimiento que hace necesaria una investigación que examine el

cumplimiento normativo y las prácticas efectivas de protección de datos en las soluciones de IA implementadas.

1.2 ANTECEDENTES DEL PROBLEMA.

En los antecedentes sobre la aplicación de la inteligencia artificial en el sector financiero, diversos estudios han señalado que su incorporación ha generado cambios relevantes en procesos como la evaluación crediticia, la detección de fraude, el monitoreo transaccional, la personalización de servicios y la automatización de operaciones. La literatura reciente coincide en que esta adopción ha favorecido la eficiencia operativa, el fortalecimiento de la capacidad analítica y la escalabilidad de los servicios financieros. No obstante, también se ha advertido que dicho avance ha incrementado la dependencia de grandes volúmenes de datos personales, así como los desafíos asociados con la privacidad, la seguridad de la información y la gobernanza de los datos (Martin & Zimmermann, 2024; Mooradian et al., 2025; Weber et al., 2024).

A nivel internacional, la literatura reciente coincide en que la inteligencia artificial aplicada al ámbito financiero no debe examinarse exclusivamente desde la perspectiva de la eficiencia tecnológica, sino también considerando sus implicaciones éticas, regulatorias y organizacionales. Diversos estudios han evidenciado que el uso de modelos algorítmicos en los servicios financieros puede dar lugar a problemas de opacidad, limitaciones en la explicabilidad, tratamiento intensivo de datos personales y riesgos de sesgo en decisiones de alto impacto, particularmente en áreas como el crédito, la segmentación de clientes, el cumplimiento normativo y la prevención del fraude. En este contexto, la discusión académica ha evolucionado desde un enfoque instrumental de la inteligencia artificial hacia una perspectiva orientada a la transparencia, la responsabilidad institucional y la gobernanza algorítmica (Weber et al., 2024; Pimentel & Pisoni, 2025; Mooradian et al., 2025).

En esta misma línea, la literatura especializada advierte que los beneficios de la inteligencia artificial coexisten con tensiones significativas entre la innovación y el control. Los estudios recientes muestran que, si bien el sector financiero ha progresado con rapidez en materia de automatización y uso estratégico de los datos, todavía presenta debilidades en la integración de principios como la minimización de datos, la explicabilidad, la supervisión humana, la trazabilidad y la rendición de cuentas. Por tanto, la problemática no radica únicamente en la disponibilidad de nuevas capacidades tecnológicas, sino también en la

insuficiente consolidación de mecanismos de control que permitan su implementación de forma responsable y en armonía con la protección de datos (Martin & Zimmermann, 2024; Mooradian et al., 2025; Pimentel & Pisoni, 2025).

En América Latina, los antecedentes reflejan un panorama heterogéneo en torno a la gobernanza de la inteligencia artificial. Si bien la región ha avanzado en la formulación de estrategias, marcos y discusiones sobre esta materia, dichos progresos no siempre se han traducido en mecanismos suficientemente consolidados para abordar de forma efectiva los efectos de la automatización en los datos personales y en la toma de decisiones. La literatura regional destaca que estos desafíos se relacionan con la influencia de referentes internacionales, la necesidad de adaptación a las realidades locales y la permanencia de desigualdades regulatorias e institucionales en el campo de la protección de datos y la gobernanza digital (Flórez Rojas, 2025; Belli & Zingales, 2022).

Desde una perspectiva crítica, los estudios regionales permiten identificar que gran parte de la discusión en América Latina se ha centrado en políticas públicas, estrategias nacionales y marcos regulatorios de carácter general, mientras que aún es limitado el desarrollo de evidencia empírica sobre la manera en que las organizaciones gestionan, en la práctica, los riesgos relacionados con la privacidad, la explicabilidad y la gobernanza de datos en sistemas algorítmicos. En consecuencia, aunque la región ha mostrado avances en el debate normativo y en la formulación de principios orientadores, persisten vacíos en la evidencia aplicada respecto al funcionamiento real de estos mecanismos en sectores sensibles, como el financiero (Flórez Rojas, 2025; Belli & Zingales, 2022).

En el caso hondureño, la brecha identificada resulta aún más evidente. A partir de la revisión de literatura indexada reciente con DOI, no se encontraron suficientes estudios específicos que analicen de forma directa la protección de datos personales en soluciones de inteligencia artificial aplicadas al sistema financiero hondureño. Esta carencia adquiere especial relevancia, ya que restringe la posibilidad de determinar con precisión cuáles son los controles institucionales existentes, qué grado de desarrollo presentan las prácticas de gobernanza algorítmica y cuál es el nivel de alineación de las entidades con principios contemporáneos de privacidad, transparencia y responsabilidad en la toma de decisiones automatizadas.

La limitada evidencia aplicada al contexto hondureño restringe una comprensión integral del problema, ya que impide identificar con claridad las brechas que persisten en el

tratamiento automatizado de datos personales, los riesgos que inciden con mayor intensidad en las instituciones financieras y los aspectos regulatorios e institucionales que requieren fortalecimiento. En este sentido, los antecedentes revisados permiten sostener que, si bien existe una base internacional y regional suficiente para comprender los riesgos y desafíos asociados al uso de la inteligencia artificial en el ámbito financiero, en Honduras persiste un vacío de investigación respecto al estado actual de la protección de datos personales en este tipo de soluciones (Martin & Zimmermann, 2024; Mooradian et al., 2025; Flórez Rojas, 2025).

En consecuencia, el vacío identificado no obedece a la ausencia de discusión sobre la relación entre inteligencia artificial y finanzas, sino a la limitada disponibilidad de estudios empíricos contextualizados que permitan analizar de qué manera se concretan en Honduras los principios de privacidad, transparencia, responsabilidad institucional y control del tratamiento automatizado de datos. Desde esta perspectiva, se justifica el desarrollo de una investigación orientada a examinar el estado actual de la protección de datos en soluciones de inteligencia artificial aplicadas al sistema financiero hondureño, a fin de identificar fortalezas, debilidades y vacíos regulatorios e institucionales vinculados con su implementación (Weber et al., 2024; Pimentel & Pisoni, 2025; Flórez Rojas, 2025).

1.3 DEFINICIÓN DEL PROBLEMA

En este apartado se realiza el enunciado y el planteamiento del problema y se formulan las preguntas de investigación.

1.3.1 ENUNCIADO DEL PROBLEMA

El rápido avance y la puesta en marcha de soluciones de inteligencia artificial en el sector financiero de Honduras han dado lugar a un escenario en el que la cantidad y diversidad de los datos personales manejados superan las normas convencionales de protección de datos. Este fenómeno se observa, por ejemplo, en el aumento en la utilización de algoritmos para el scoring crediticio, la detección de fraude y el monitoreo de transacciones, los cuales se alimentan de datos bancarios, comportamentales y biométricos. Aunque estas innovaciones proporcionan mejoras en la eficiencia operativa y en la atención al cliente, también aumentan los riesgos para los titulares de la información, incluyendo la falta de claridad en las decisiones automáticas, la dificultad para hacer valer derechos como el acceso, la corrección o la eliminación, así como el

riesgo de sesgos en los algoritmos o el manejo de datos sensibles sin la debida base legal. Investigaciones recientes indican que una adecuada formulación del problema debe situar el asunto en su contexto, ofrecer pruebas de su relevancia y definir el área de estudio.

En el ámbito nacional, aunque la Comisión Nacional de Bancos y Seguros y otras organizaciones han comenzado a promover iniciativas de innovación financiera y regulación de tecnología financiera, faltan directrices concretas para la protección de datos en los sistemas de inteligencia artificial en las instituciones financieras. Esto crea una discrepancia entre las tecnologías implementadas y las garantías normativas y operativas en términos de privacidad y seguridad. A nivel global, la literatura señala que una de las principales deficiencias en la inteligencia artificial aplicada al sector bancario es la gobernanza de algoritmos y la protección de datos desde el diseño, lo cual es crucial para los mercados emergentes donde las instituciones todavía están en proceso de consolidación.

Este contexto presenta un desafío serio, contemporáneo y significativo: en ausencia de una evaluación precisa sobre la situación de la protección de datos en las aplicaciones de inteligencia artificial utilizadas por las instituciones financieras en Honduras, y sin un análisis de los métodos de gobernanza, transparencia, derechos de los individuos y seguridad de la información existentes, existe el peligro de que se debilite la confianza de los usuarios, se impongan sanciones regulatorias, se pierda competitividad y se violen derechos fundamentales. Por lo tanto, es esencial llevar a cabo una investigación para determinar en qué medida estas aplicaciones de inteligencia artificial satisfacen las exigencias de protección de datos personales y cuáles son los elementos que promueven o impiden dicho cumplimiento en el sector financiero de Honduras.

La importancia de esta declaración del problema está directa y estrechamente relacionada con el avance de la tecnología, el incremento en la implementación de inteligencia artificial en instituciones financieras y bancarias, y la urgencia de garantizar que la innovación cumpla con criterios de privacidad, legalidad y ética. Al enfocar el estudio en Honduras, se ofrece evidencia específica que puede constituir una base para elaborar sugerencias de políticas, gobernanza y prácticas óptimas adaptadas al contexto local.

1.3.2 FORMULACIÓN DEL PROBLEMA

La literatura reciente destaca el uso de inteligencia artificial en el sector financiero exige mayores medidas de privacidad y protección de datos. Sin embargo, aún hay poca información sobre cómo estas prácticas se aplican específicamente en Honduras. Por ello surge la interrogante: ¿Cómo gestionan las instituciones financieras hondureñas la protección de datos personales en el desarrollo y aplicación de soluciones de inteligencia artificial dentro de sus operaciones?

1.3.3 PREGUNTAS ESPECÍFICAS DE INVESTIGACIÓN

1. ¿Cómo garantizan las entidades financieras hondureñas la transparencia en el uso de inteligencia artificial?

2. ¿Qué controles de seguridad aplican las entidades financieras para resguardar la información personal de los usuarios en sistemas basados en IA?

3. ¿Qué relación existe entre el nivel de adopción de soluciones de inteligencia artificial y el nivel de protección de datos personales en las instituciones participantes del sistema financiero hondureño?

1.4 OBJETIVOS DE LA INVESTIGACIÓN

A continuación, se formulan los objetivos que guiarán la presente investigación:

1.4.1 OBJETIVO GENERAL

Evaluar la relación entre el nivel de adopción de soluciones de inteligencia artificial y el nivel de protección de datos personales en instituciones del sistema financiero hondureño, con base en la percepción de profesionales vinculados a tecnología, seguridad de la información, gestión de datos, riesgos, canales digitales y cumplimiento normativo.

1.4.2 OBJETIVOS ESPECÍFICOS

1. Describir el nivel de adopción de soluciones de inteligencia artificial en instituciones del sistema financiero hondureño, considerando su uso en procesos clave, madurez de implementación y mecanismos de gobernanza institucional.
2. Determinar el nivel de protección de datos personales asociado al uso de soluciones de inteligencia artificial, considerando principios de protección de datos, controles técnicos, transparencia y mecanismos para el ejercicio de derechos de los titulares.
3. Analizar la relación entre el nivel de adopción de soluciones de inteligencia artificial y el nivel de protección de datos personales en las instituciones participantes del sistema financiero hondureño.

1.5 JUSTIFICACIÓN

El estudio que se presenta es necesario para examinar de manera crítica cómo el sistema financiero de Honduras está adoptando la inteligencia artificial sin comprometer la seguridad de datos personales, en un momento en que la regulación específica es aún inicial y la necesidad de innovar se intensifica. A nivel global, el Financial Stability Institute del Banco de Pagos Internacionales señala que la aplicación de la inteligencia artificial en el sector financiero, especialmente en áreas como la evaluación crediticia, el seguimiento de transacciones, la gestión de riesgos y el servicio al cliente, aumenta la vulnerabilidad a problemas de privacidad, el uso excesivo de datos, la falta de transparencia en los algoritmos y la dependencia de terceros, enfatizando la necesidad de establecer marcos apropiados de gobernanza y supervisión para estas tecnologías.

En la región latinoamericana, el análisis titulado “Caminos Regulatorios para la IA en América Latina” del grupo AlSur revela un rápido uso de IA a pesar de contar con marcos de protección de datos desarticulados o insuficientes, poniendo de manifiesto choques entre la innovación y la protección de derechos. No obstante, hay una falta de estudios empíricos que documenten, con información precisa, de qué manera las instituciones financieras aplican conceptos como legalidad, claridad, reducción, protección o responsabilidad en sus soluciones de IA.

Al focalizarse en el sistema financiero hondureño, este estudio contribuye a llenar un vacío académico: ofrece un diagnóstico sistemático sobre el grado de alineación entre las

prácticas tecnológicas de IA y los principios de protección de datos, combinando análisis documental, normativo y organizacional. Ello fortalece la base científica para futuras propuestas de regulación, modelos de gobernanza de IA y estudios comparados en la región. Para directivos, oficiales de cumplimiento, responsables de TI, ciberseguridad, auditoría y gestión de riesgos, la capacidad de evaluar el tratamiento de datos personales en sistemas de IA es hoy un requisito estratégico, no solo técnico. Documentos emitidos por la Comisión Nacional de Bancos y Seguros (CNBS), como la sección de Regulación Fintech y el marco regulatorio para innovaciones financieras, destacan la importancia de la estabilidad, transparencia, protección del usuario financiero y gestión de riesgos tecnológicos como condiciones clave para la innovación. (CNBS, 2024)

Este documento ofrece recursos útiles para los involucrados: posibilita detectar prácticas actuales, deficiencias en el cumplimiento y oportunidades para mejorar la gestión de datos y proyectos de inteligencia artificial en organizaciones reguladas. Para un posgrado enfocado en la administración de tecnologías de la información, seguridad, regulación o finanzas, el estudio refuerza habilidades avanzadas en análisis técnico-normativo, creación de controles y la toma de decisiones fundamentadas en evidencia. El tratamiento apropiado de la información personal en aplicaciones de inteligencia artificial tiene un impacto directo en la confianza de los ciudadanos en el sistema financiero. Riesgos como el perfilamiento indebido, decisiones automatizadas poco transparentes, sesgos discriminatorios o filtraciones de información delicada afectan derechos fundamentales y la imagen de las instituciones. El reporte sobre “Obstáculos Regulatorios en la Industria de Tecno-Finanzas en Honduras”, elaborado con la colaboración del BCH, CNBS y socios, ya señalaba la urgencia de aclarar las normativas sobre el uso y la compartición de información en servicios financieros digitales.

Al determinar la situación actual en la salvaguarda de datos en aplicaciones de inteligencia artificial y al sugerir propuestas fundamentadas en normativas globales (como las prácticas recomendadas por el BIS y análisis de AlSur), este estudio ayuda a: resguardar a los usuarios en el sector financiero, mejorar la claridad y la responsabilidad de las organizaciones, y asistir a los entes reguladores en el desarrollo de directrices más precisas para una innovación responsable. Todo esto genera un impacto beneficioso en la sociedad y una estabilidad en la industria, alineándose con las metas de integridad del sistema financiero. La investigación es factible desde un punto de vista técnico por diversas razones. Primero, hay acceso a fuentes oficiales y verificables: documentos públicos del BIS sobre la regulación de la inteligencia

artificial en el ámbito financiero, estudios realizados por el consorcio AlSur, informes del BCH y de la CNBS sobre obstáculos regulatorios, el marco fintech y el centro de innovación financiera, además de guías sobre la protección de los usuarios financieros. (AlSur, 2024)

En segundo lugar, el enfoque puede juntar la revisión de documentos y normativas, la evaluación de políticas internas y los avisos de privacidad de organizaciones elegidas, así como métodos de recolección de datos como entrevistas o encuestas destinadas a los encargados de cumplimiento, tecnología de la información y seguridad, sin necesitar una infraestructura especializada ni tener que acceder de manera intrusiva a los sistemas. En tercer lugar, el método es específico y manejable respecto a los tiempos y recursos que se asocian con una tesis de maestría: se puede limitar a un grupo de entidades que están bajo supervisión y a aplicaciones particulares de inteligencia artificial (por ejemplo, evaluación crediticia, vigilancia de fraudes o plataformas digitales).

Esta combinación de fuentes confiables, alcance definido y métodos factibles asegura la rigurosidad del estudio y su coherencia con estándares académicos de posgrado.

En resumen, el estudio que se sugiere cuenta con una base científica robusta, es relevante desde el punto de vista profesional, responde a una necesidad social y presenta un enfoque metodológico factible. Además, se relaciona directamente con la meta principal de examinar la situación presente de la salvaguarda de datos en aplicaciones de inteligencia artificial dentro del sector financiero en Honduras, ofreciendo información valiosa para la elaboración de decisiones en entidades financieras y organismos de regulación.

CAPÍTULO II. MARCO TEÓRICO

El presente capítulo desarrolla el marco teórico que sustenta la investigación sobre el estado actual de la protección de datos personales en soluciones de inteligencia artificial utilizadas en el sistema financiero hondureño. Se analizan antecedentes investigativos relevantes, fundamentos conceptuales y enfoques teóricos relacionados con la inteligencia artificial, la protección de datos y la gestión de riesgos tecnológicos en el sector financiero. Igualmente, se examina la relación entre la literatura existente y el problema de investigación, identificando hallazgos, vacíos y aportes teóricos que respaldan el estudio. Finalmente, se incorporan elementos metodológicos utilizados en investigaciones previas que orientan el diseño del estudio actual (Kelley et al., 2003; Sedgwick, 2014).

2.1 MARCO REFERENCIAL

El rápido avance de la inteligencia artificial ha transformado de manera significativa los procesos operativos, analíticos y decisionales en el sector financiero a nivel global. Las instituciones financieras han incorporado soluciones basadas en IA para optimizar la atención al cliente, mejorar la detección de fraudes, automatizar análisis de riesgos y fortalecer la eficiencia operativa. Sin embargo, esta adopción tecnológica ha incrementado la exposición a riesgos asociados al tratamiento de datos personales, especialmente cuando dichos sistemas procesan grandes volúmenes de información sensible (European Union Agency for Cybersecurity [ENISA], 2023).

Diversos estudios señalan que la implementación de soluciones de IA en entornos financieros requiere marcos sólidos de gobernanza de datos, controles de seguridad adecuados y mecanismos de cumplimiento normativo que garanticen la protección de los derechos de los titulares de la información (Floridi et al., 2018). En este contexto, la protección de datos personales se convierte en un eje crítico para la sostenibilidad y legitimidad del uso de la inteligencia artificial, particularmente en sectores altamente regulados como el financiero.

En países en desarrollo, como Honduras, el desafío se intensifica debido a limitaciones normativas, brechas tecnológicas y niveles heterogéneos de madurez institucional en materia de ciberseguridad y gestión de datos. Investigaciones recientes destacan que, si bien las instituciones financieras de la región han avanzado en la adopción de tecnologías digitales, persisten debilidades en la implementación efectiva de controles de protección de datos en

sistemas automatizados y algorítmicos (World Bank, 2022). Por ello, resulta necesario analizar el estado actual de dichas prácticas, a fin de identificar oportunidades de mejora y aportar evidencia empírica que respalde el fortalecimiento de la protección de datos en soluciones de inteligencia artificial dentro del sistema financiero hondureño.

2.1.1 REVISIÓN DE ESTUDIOS RELEVANTES

La investigación sobre la protección de datos personales en el contexto del uso de inteligencia artificial ha crecido de forma significativa en la última década, especialmente en sectores donde el tratamiento de información sensible es crítico, como el financiero. Estudios tempranos identificaron que los sistemas de decisión automatizada incrementan los riesgos de opacidad, discriminación y uso indebido de datos personales, lo que exige mecanismos de control y supervisión más estrictos (Zarsky, 2016).

Posteriormente, la literatura académica comenzó a profundizar en la relación entre inteligencia artificial y los marcos regulatorios de protección de datos. Wachter, Mittelstadt y Floridi (2017) analizaron los alcances y limitaciones del Reglamento General de Protección de Datos (RGPD) frente a la toma de decisiones automatizada, concluyendo que los sistemas algorítmicos complejos requieren medidas adicionales de transparencia, gobernanza y evaluación de impacto para garantizar la protección efectiva de los datos personales.

En el ámbito específico del sector financiero, diversos estudios han demostrado que el uso de inteligencia artificial en procesos como evaluación crediticia, detección de fraudes y segmentación de clientes incrementa la exposición a riesgos de privacidad. Binns et al. (2018) señalan que los sistemas algorítmicos pueden heredar sesgos y amplificar riesgos cuando no se diseñan bajo principios de protección de datos desde el inicio. Estos hallazgos respaldan la necesidad de integrar la protección de datos como un componente central en el diseño y operación de soluciones de inteligencia artificial.

Investigaciones recientes también han abordado el concepto de gobernanza de datos como elemento clave para el uso responsable de la inteligencia artificial. Según Kuner, Bygrave y Docksey (2020), una gobernanza adecuada permite establecer responsabilidades claras, controles técnicos y mecanismos de rendición de cuentas que

contribuyen a reducir los riesgos asociados al tratamiento de datos personales en sistemas automatizados.

En contextos de economías emergentes, la literatura señala que las instituciones financieras enfrentan desafíos adicionales relacionados con brechas regulatorias, limitaciones técnicas y ausencia de evaluaciones sistemáticas de riesgos. Estudios empíricos indican que estas limitaciones afectan la implementación efectiva de controles de protección de datos en soluciones de inteligencia artificial, generando niveles heterogéneos de cumplimiento y madurez institucional (Brkan & Bonnet, 2020).

En conjunto, los estudios revisados coinciden en que la protección de datos personales constituye un factor crítico para el uso legítimo y sostenible de la inteligencia artificial en el sector financiero. Sin embargo, también evidencian la existencia de vacíos empíricos en contextos nacionales específicos, particularmente en países en desarrollo. Esta ausencia de estudios focalizados refuerza la necesidad de investigaciones que analicen el estado actual de las prácticas de protección de datos en soluciones de inteligencia artificial dentro del sistema financiero hondureño.

2.1.2 IA Y PROTECCIÓN DE DATOS: ESTUDIOS INTERNACIONALES

A nivel global, la investigación científica ha documentado el crecimiento acelerado de soluciones de IA en procesos bancarios críticos, subrayando al mismo tiempo los riesgos para la privacidad y la transparencia. Richard y Blake (2024), en *Data Privacy Challenges in AI-driven Financial Services*, identifican que los modelos de aprendizaje automático utilizados para scoring crediticio, monitoreo transaccional y anti-fraude operan sobre volúmenes masivos de datos, generando dificultades para garantizar principios de licitud, minimización y finalidad. Su análisis metodológico combina revisión sistemática de literatura y estudio comparado de marcos regulatorios, concluyendo que incluso en jurisdicciones avanzadas persisten brechas entre teoría y práctica en la gobernanza algorítmica.

El Financial Stability Institute del Banco de Pagos Internacionales (BIS) profundiza esta preocupación. Crisanto et al. (2024), en su informe *Regulating AI in the Financial Sector*, examinan 14 jurisdicciones y encuentran retos comunes: opacidad algorítmica, ausencia de explicabilidad, incremento de riesgos operacionales y

dependencia de proveedores externos. Metodológicamente, el BIS utiliza análisis documental y entrevistas a reguladores, destacando que la IA en finanzas se clasifica como “tecnología de alto riesgo”, lo que demanda lineamientos robustos de gobernanza, auditoría y supervisión.

Otro aporte importante significativo proviene del campo de la personalización bancaria. Ashrafuzzaman et al. (2025), en una revisión PRISMA de más de 100 artículos, documentan cómo la hiperpersonalización basada en analítica conductual y modelos predictivos incrementa la calidad del servicio, pero también amplifica riesgos de perfilamiento intrusivo, discriminación indirecta y vulneraciones de privacidad. Metodológicamente, este estudio sintetiza evidencia empírica entre 2014 y 2024, destacando la necesidad de integrar explicabilidad algorítmica en procesos automatizados.

Un enfoque complementario es el análisis comparado de regulaciones. Irfan et al. (2024), en *Artificial Intelligence, Data Protection and Transparency: A Comparative Study of GDPR and CCPA*, identifican que ambos marcos coinciden en exigir transparencia, derechos del titular y evaluaciones de impacto, pero difieren en mecanismos de cumplimiento. Esta literatura establece estándares internacionales que sirven como referencia para evaluar vacíos en países sin regulación integral, como Honduras.

Finalmente, Selvam (2025) aporta evidencia técnica relevante mediante un marco metodológico que combina métricas de equidad y herramientas de explicabilidad (SHAP, LIME). Sus experimentos muestran que la mitigación de sesgos en IA bancaria es técnicamente viable sin afectar de manera significativa la precisión de los modelos, lo cual es clave para garantizar decisiones justas y transparentes.

Mencionar, que la literatura internacional señala tres patrones recurrentes:

- la IA financiera incrementa la eficiencia, pero también la exposición a riesgos de privacidad.
- la gobernanza algorítmica es todavía incipiente.
- las evaluaciones de impacto en privacidad son necesarias, pero poco implementadas.

2.1.3 ESTUDIOS REGIONALES Y LATINOAMERICANOS.

La literatura científica revisada permite establecer una relación directa entre el uso creciente de soluciones de inteligencia artificial en el sector financiero y los desafíos asociados a la protección de datos personales. Diversos estudios coinciden en que los sistemas basados en inteligencia artificial incrementan el volumen, la velocidad y la complejidad del tratamiento de datos personales, lo que amplifica los riesgos de uso indebido, sesgos algorítmicos y falta de transparencia en los procesos automatizados (Zarsky, 2016). Este escenario resulta especialmente crítico en el sistema financiero, donde se procesan datos sensibles vinculados a la identidad, el comportamiento financiero y el historial crediticio de los usuarios.

- Hallazgos clave de la literatura

  Los principales hallazgos identificados señalan que la protección de datos personales en soluciones de inteligencia artificial depende en gran medida de la existencia de marcos sólidos de gobernanza de datos, políticas internas claras y mecanismos de supervisión técnica y legal. Wachter, Mittelstadt y Floridi (2017) destacan que los marcos regulatorios actuales, como el RGPD, presentan limitaciones para abordar plenamente los riesgos derivados de la toma de decisiones automatizada, lo que exige medidas complementarias orientadas a la transparencia y rendición de cuentas. En ese mismo sentido, Binns et al. (2018) evidencian que los sistemas algorítmicos pueden reproducir o amplificar riesgos cuando no se diseñan bajo principios de protección de datos desde las etapas iniciales.

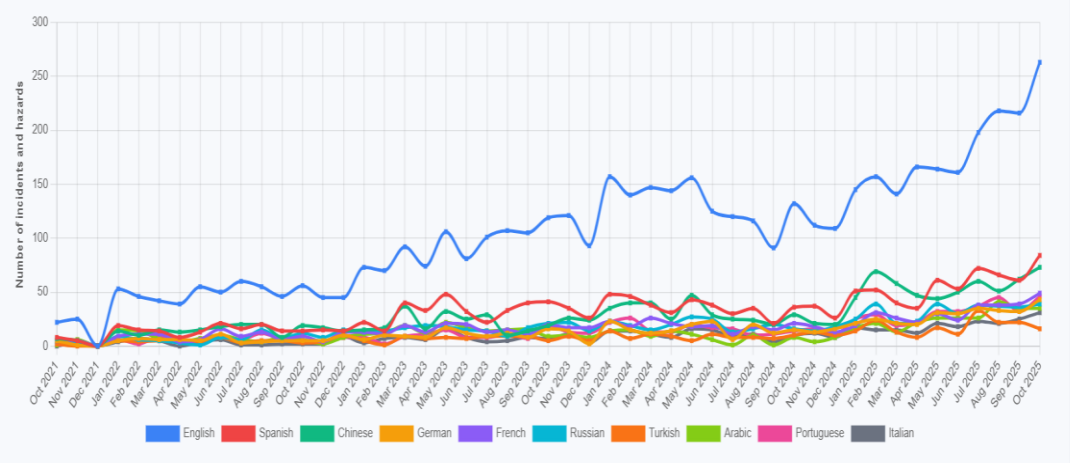


Figura 1. Evolución de incidentes y peligros por ubicación

Fuente: Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2024). AI incidents and hazards as reported by reputable international media, January 2016–January 2024. OECD.AI Incidents Monitor. https://oecd.ai/en/incidents

- Contradicciones y vacíos en la investigación

A pesar del consenso general sobre la importancia de la protección de datos en soluciones de inteligencia artificial, la literatura muestra vacíos relevantes. La mayoría de los estudios se concentran en contextos europeos o norteamericanos, mientras que existe una limitada evidencia empírica aplicada a países en desarrollo. Además, muchos trabajos abordan el problema desde un enfoque normativo o conceptual, sin evaluar de manera sistemática el estado actual de las prácticas de protección de datos en instituciones financieras específicas. Esta ausencia de estudios empíricos contextualizados limita la comprensión del nivel real de madurez institucional en materia de protección de datos en soluciones de inteligencia artificial (Brkan & Bonnet, 2020).

- Teorías y enfoques que respaldan la investigación

Desde el punto de vista teórico, la presente investigación se sustenta en los principios de protección de datos desde el diseño y por defecto, así como en los enfoques de gobernanza algorítmica y gestión de riesgos tecnológicos. Kuner, Bygrave y Docksey (2020) sostienen que la protección efectiva de los datos personales en sistemas automatizados requiere integrar controles técnicos, organizativos y legales de forma transversal. Estos enfoques respaldan la necesidad de analizar el estado actual de la protección de datos en soluciones de inteligencia artificial, particularmente en el sistema financiero hondureño, donde la adopción tecnológica avanza más rápido que la consolidación de mecanismos de protección.

En este contexto, la revisión de la literatura evidencia la pertinencia del problema de investigación y justifica la realización de un estudio que analice de manera empírica el estado actual de la protección de datos personales en soluciones de inteligencia artificial utilizadas en el sistema financiero hondureño.

2.1.4 EVIDENCIA NACIONAL Y ESTUDIOS EN HONDURAS

En Honduras, la literatura es menos abundante, pero existen documentos clave emitidos por organismos regulatorios y estudios de competitividad. El informe *Barreras Regulatorias en la Industria de Tecno-Finanzas* (BCH, CNBS, ACDI/VOCA, 2020–2021) identifica que el país carece de una ley integral de protección de datos personales, lo que limita la seguridad jurídica para proyectos de IA y fintech. El estudio utiliza entrevistas, análisis documental y revisión normativa, señalando que las entidades financieras suelen adoptar soluciones de IA sin criterios homogéneos sobre privacidad, consentimiento o licitud.

Adicionalmente, la Comisión Nacional de Bancos y Seguros (CNBS) ha publicado lineamientos fintech (2023–2024) que, aunque importantes, no abordan de forma explícita las decisiones automatizadas ni los riesgos de gobernanza algorítmica. Su enfoque está orientado a la innovación y estabilidad financiera, dejando un vacío en protección de datos para modelos de IA.

El *Hub de Innovación Financiera de Honduras* (CNBS, 2024) reconoce públicamente que la adopción tecnológica supera la capacidad regulatoria, y promueve espacios de sandbox regulatorio, pero aún sin lineamientos de privacidad específicos más allá de estándares tradicionales de seguridad.

Estos documentos nacionales, junto con los estudios internacionales, refuerzan un hallazgo central: en Honduras, la brecha entre innovación tecnológica y regulación de datos personales se amplifica cuando intervienen modelos de IA que procesan datos sensibles con poca supervisión algorítmica o transparencia operativa.

2.1.5 RELACIÓN DE LA LITERATURA CON EL PROBLEMA DE INVESTIGACIÓN

La revisión de literatura establece una relación directa entre el avance acelerado de la inteligencia artificial (IA) en el sector financiero y los desafíos emergentes en materia de protección de datos personales. Este vínculo es fundamental para comprender el problema central de la investigación: determinar el nivel de cumplimiento de los principios de privacidad en las soluciones de IA utilizadas por las entidades financieras hondureñas. Los estudios internacionales, regionales y nacionales coinciden en que la

adopción rápida de tecnologías algorítmicas no ha sido acompañada por marcos regulatorios equivalentes, lo que genera brechas críticas en transparencia, gobernanza y resguardo de información.

2.1.6 HALLAZGOS CLAVE DE LA LITERATURA

Los estudios internacionales muestran que la IA financiera opera sobre grandes volúmenes de datos sensibles y genera riesgos complejos relacionados con la opacidad algorítmica y la falta de mecanismos claros de control. Richard y Blake (2024) evidencian que los sistemas de aprendizaje automático utilizados para scoring crediticio, monitoreo de fraude y segmentación de clientes presentan dificultades para cumplir con principios como licitud, minimización y transparencia, incluso en jurisdicciones con regulaciones avanzadas.

El Financial Stability Institute del Banco de Pagos Internacionales coincide con esta perspectiva. Crisanto et al. (2024) señalan que, aunque los reguladores reconocen los beneficios de la IA en eficiencia operativa y supervisión financiera, persisten vacíos significativos en explicabilidad, gestión de riesgos y supervisión de proveedores externos. El informe concluye que la IA se ha convertido en una tecnología de alto riesgo para los sistemas financieros globales.

En el ámbito de la personalización digital, Ashrafuzzaman et al. (2025) documentan que el uso de analítica avanzada para hiperpersonalizar servicios bancarios aumenta la satisfacción del cliente, pero también expone a prácticas intrusivas de perfilamiento y a decisiones automatizadas difíciles de justificar ante los titulares de datos.

A nivel regional, AlSur (2024) demuestra que América Latina experimenta un avance tecnológico más rápido que su capacidad normativa para regular decisiones automatizadas, protección de datos o gobernanza algorítmica. Esta conclusión es coherente con el caso hondureño, donde documentos del Banco Central de Honduras y la Comisión Nacional de Bancos y Seguros destacan la ausencia de una ley integral de protección de datos y la falta de lineamientos específicos para IA en entidades financieras (BCH & CNBS, 2021).

Estos descubrimientos apoyan la relevancia del tema de estudio al evidenciar que la inteligencia artificial aumenta las amenazas a la información privada y necesita normativas de adherencia más desarrolladas, sobre todo en entornos como el de Honduras.

Figura 2. Incidentes y riesgos asociados a IA reportados por medios internacionales (2016–2024)

Fuente: Adaptado de OECD.AI Incidents Monitor (OECD, 2024). Datos obtenidos de: https://www.oecd.org/en/topics/artificial-intelligence.html

2.1.7 CONTRADICCIONES O VACÍOS IDENTIFICADOS

La literatura también presenta contradicciones relevantes. Jim et al. (2024) señalan que la IA puede fortalecer la privacidad mediante detección de anomalías en banca en la nube, pero al mismo tiempo reconocen que estos modelos requieren enormes cantidades de datos sensibles, creando nuevos puntos de vulnerabilidad. Un vacío central es la falta de estudios empíricos en Centroamérica que evalúen el nivel real de cumplimiento normativo en proyectos concretos de IA bancaria. La mayor parte de la literatura latinoamericana es comparativa o conceptual, pero no examina prácticas reales dentro de instituciones financieras específicas.

Otro vacío crítico es la escasa adopción de métricas de equidad, herramientas de aplicabilidad y auditorías de sesgo en países en desarrollo. Aunque Selvam (2025) demuestra técnicamente que es posible mitigar sesgos sin afectar significativamente la

precisión, estos mecanismos rara vez se aplican en contextos donde no existen obligaciones regulatorias.

En Honduras, la ausencia de una ley integral de protección de datos y la falta de marcos para decisiones automatizadas crean un vacío normativo que aumenta la exposición de los usuarios y limita la capacidad institucional de supervisión (CNBS, 2024).

2.1.8 TEORÍAS PREVIAS QUE RESPALDAN LA INVESTIGACIÓN

La investigación se apoya en diversos fundamentos teóricos:

a) Principios internacionales de protección de datos

El GDPR y las directrices de la OCDE establecen principios como licitud, finalidad, minimización, seguridad y responsabilidad (OECD, 2021). Estos principios constituyen el estándar global para evaluar el tratamiento de datos en sistemas basados en IA.

b) Privacidad por diseño

Propuesta por Cavoukian, sostiene que la privacidad debe incorporarse desde el diseño de los sistemas, lo cual es esencial para tecnologías algorítmicas en banca.

c) Gobernanza algorítmica

Plantea la necesidad de establecer mecanismos de control, supervisión y explicabilidad para modelos de IA. Estudios como los del BIS y Selvam (2025) respaldan esta perspectiva.

d) Teoría del riesgo tecnológico en sistemas financieros

El Financial Stability Board (FSB) enfatiza que las tecnologías emergentes deben evaluarse a partir de riesgos operacionales, de datos y de cumplimiento.

En conjunto, estas teorías refuerzan que evaluar el estado de la protección de datos en soluciones de IA del sistema financiero hondureño es una necesidad académica, técnica y regulatoria.

2.2 MARCO CONCEPTUAL

El presente Marco Conceptual establece las definiciones, criterios técnicos y categorías analíticas que permitirán comprender con precisión los elementos centrales del estudio sobre la protección de datos personales en soluciones de inteligencia artificial (IA) implementadas por

entidades del sistema financiero hondureño. Dado que la IA se integra cada vez más en procesos críticos como el análisis de riesgo, la detección de fraude, la segmentación de clientes y la operatividad de los canales digitales, resulta indispensable delimitar conceptualmente los términos que describen el funcionamiento, los riesgos y las obligaciones derivados del tratamiento automatizado de información sensible en este sector.

En Honduras, la adopción acelerada de tecnologías algorítmicas ocurre en un entorno donde aún no existe una ley integral de protección de datos personales y donde los lineamientos regulatorios para IA son incipientes. Esta realidad acentúa la importancia de contar con claridad conceptual para evaluar el grado de cumplimiento de principios esenciales como licitud, transparencia, minimización, seguridad y responsabilidad, reconocidos en estándares internacionales y discutidos ampliamente en la literatura analizada. En la misma línea, conceptos como "gobernanza algorítmica", "sesgo", "aplicabilidad", "evaluación de impacto en privacidad" y "tratamiento automatizado" adquieren relevancia en la interpretación de las prácticas actuales del sistema financiero hondureño.

El Marco Conceptual, por tanto, no solo define los términos clave del estudio, sino que actúa como puente entre el análisis teórico previo y la evaluación empírica, permitiendo interpretar de manera rigurosa las políticas, medidas de seguridad y mecanismos de transparencia adoptados por las entidades financieras. Este apartado proporciona el lenguaje técnico necesario para examinar de forma coherente y sistemática la interacción entre IA y protección de datos en el contexto nacional.

2.2.1 SELECCIÓN Y DEFINICIÓN DE CONCEPTOS CLAVE

La claridad conceptual es un requisito fundamental para analizar rigurosamente el uso de inteligencia artificial (IA) en procesos financieros y su impacto en la protección de datos personales. La literatura especializada y los estándares internacionales resaltan que la precisión terminológica permite evaluar el cumplimiento normativo, comprender los riesgos asociados al tratamiento automatizado de datos y establecer criterios coherentes de análisis. A continuación, se presentan los conceptos esenciales que sustentan este estudio.

2.2.2 DATOS PERSONALES

Los datos personales son toda información que identifica o permite identificar a una persona física, directa o indirectamente (OECD, 2021). En el sector financiero incluyen

información de cuentas, historiales crediticios, patrones transaccionales y datos biométricos utilizados para autenticación. Su relevancia radica en que constituyen la materia prima de los modelos de IA, cuyo tratamiento debe alinearse con principios de licitud, finalidad y minimización.

2.2.3 DATOS SENSIBLES

La literatura describe los datos sensibles como aquellos cuyo uso indebido puede afectar derechos fundamentales, tales como información financiera, biométrica, de salud o comportamiento (Irfan et al., 2024). Las entidades financieras procesan datos de alta sensibilidad, y su utilización en modelos algorítmicos exige medidas reforzadas de seguridad y control.

2.2.4 INTELIGENCIA ARTIFICIAL

La IA es definida como sistemas capaces de aprender patrones a partir de datos, tomar decisiones o generar predicciones con diferentes grados de autonomía (Crisanto et al., 2024). Incluye técnicas como machine learning, deep learning y modelos de analítica avanzada. Su uso en banca permite automatizar decisiones, mejorar eficiencia y detectar anomalías, pero también introduce riesgos de opacidad y sesgo.

2.2.5 TRATAMIENTO AUTOMATIZADO DE DATOS

Corresponde a cualquier operación realizada mediante sistemas algorítmicos sin intervención humana significativa, especialmente cuando produce efectos legales o relevantes para los usuarios (GDPR, art. 22). En el contexto financiero se observa en modelos de scoring crediticio, detección de fraude y segmentación automatizada.

2.2.6 GOBERNANZA ALGORÍTMICA

La gobernanza algorítmica abarca el conjunto de políticas, controles, procedimientos y responsabilidades destinados a asegurar que los modelos de IA operen de manera ética, transparente, segura y conforme con la normativa (BIS, 2024). Implica supervisión interna, trazabilidad, documentación de modelos y auditorías periódicas.

2.2.7 TRANSPARENCIA ALGORÍTMICA

La transparencia se refiere a la capacidad de explicar cómo funciona un modelo, qué datos utiliza, cómo toma decisiones y cuáles son sus impactos (Richard & Blake, 2024). Constituye un requisito clave para proteger a los titulares de datos frente a decisiones automatizadas y fortalecer la confianza en los servicios financieros.

2.2.8 SESGO ALGORÍTMICO

El sesgo es la distorsión en los resultados de un modelo debido a datos desbalanceados, reglas discriminatorias o diseño deficiente (Selvam, 2025). En banca puede afectar decisiones crediticias, evaluaciones de riesgo o procesos de verificación, generando discriminación no intencional.

2.2.9 EVALUACIÓN DE IMPACTO EN PRIVACIDAD

Es un proceso sistemático para identificar y mitigar riesgos asociados al tratamiento de datos personales en operaciones de alto riesgo, como las que utiliza IA (GDPR, art. 35). Permite determinar si el tratamiento es proporcional, seguro y respetuoso de los derechos del titular.

2.2.10 PRIVACIDAD POR DISEÑO

Este principio establece que la privacidad debe integrarse desde el diseño del sistema, incorporando medidas técnicas y organizativas preventivas antes de procesar datos (Cavoukian, 2010). Es un estándar internacional clave para asegurar que los modelos de IA no comprometan la confidencialidad o integridad de la información.

2.2.11 SEGURIDAD DE LA INFORMACIÓN

Conjunto de medidas administrativas, físicas y técnicas destinadas a preservar la confidencialidad, integridad y disponibilidad de los datos (ISO/IEC 27001). Su relevancia aumenta cuando la IA depende de infraestructuras digitales y arquitecturas de datos distribuidas.

2.2.12 RELACIÓN ENTRE CONCEPTOS Y POSIBLE MODELO CONCEPTUAL

El análisis conceptual previamente desarrollado permite establecer la manera en que los distintos elementos asociados al uso de inteligencia artificial (IA) y a la protección de datos personales interactúan dentro del sistema financiero hondureño. Esta relación es esencial para construir un modelo conceptual que integre las dinámicas del tratamiento automatizado, los principios de privacidad, los riesgos emergentes y los mecanismos de gobernanza necesarios para garantizar un uso responsable de estas tecnologías.

En primer lugar, los conceptos de datos personales y datos sensibles constituyen la base del modelo, dado que representan el insumo fundamental sobre el cual operan los sistemas de IA implementados por las entidades financieras. La literatura establece que el riesgo aumenta proporcionalmente con el volumen, variedad y criticidad de los datos procesados (OECD, 2021; Irfan et al., 2024). Por ello, estos elementos se ubican en el núcleo del modelo conceptual como la materia prima del tratamiento.

A partir de este núcleo, el concepto de inteligencia artificial actúa como el mecanismo técnico que transforma los datos mediante algoritmos, modelos predictivos y decisiones automatizadas. Este componente está asociado a otros conceptos clave como opacidad algorítmica, sesgo, aplicabilidad y tratamiento automatizado, los cuales describen los riesgos operativos que generan impacto directo en los titulares de los datos (Crisanto et al., 2024; Selvam, 2025). En el modelo, esta dimensión se interpreta como el “motor” que habilita nuevas capacidades, pero también nuevos riesgos.

En una capa superior se ubican los principios de protección de datos: licitud, minimización, finalidad, transparencia, seguridad y responsabilidad. Estos principios actúan como criterios evaluativos que permiten determinar si las prácticas de IA cumplen con estándares internacionales y con expectativas de protección en el contexto hondureño. Funcionan, por tanto, como variables normativas que orientan la valoración del cumplimiento.

La gobernanza algorítmica y la evaluación de impacto en privacidad representan los elementos de control dentro del modelo conceptual. Estos conceptos articulan procedimientos, roles, políticas y mecanismos diseñados para garantizar que el uso de IA esté alineado con los principios de privacidad y con los estándares técnicos de seguridad. La literatura demuestra

que, sin estos controles, la adopción tecnológica tiende a generar vulnerabilidades, usos indebidos o decisiones discriminatorias (BIS, 2024).

Finalmente, el modelo conceptual se completa con la seguridad de la información, que abarca las medidas técnicas y organizativas que protegen la confidencialidad, integridad y disponibilidad de los datos, especialmente relevantes en arquitecturas algorítmicas con alto grado de automatización.

De esta forma, el modelo conceptual propuesto se estructura en tres niveles:

1. Datos personales y sensibles como insumo.
2. Sistemas de IA como procesos de transformación y riesgo.
3. Principios normativos y mecanismos de control como protectores de la privacidad.

Este modelo permite analizar de manera integral cómo las entidades financieras hondureñas gestionan los riesgos asociados a la IA y en qué medida cumplen con estándares de protección de datos.

2.2.13 RELACIÓN ENTRE CONCEPTOS APLICADOS AL FENÓMENO INVESTIGADO

El fenómeno investigado la protección de datos personales en soluciones de inteligencia artificial (IA) usadas por entidades del sistema financiero hondureño requiere articular diversas perspectivas teóricas para comprender cómo interactúan la regulación, la tecnología y la gestión institucional. La literatura internacional, regional y local revela convergencias y tensiones que explican las brechas actuales entre la adopción acelerada de IA y la capacidad normativa para garantizar la privacidad de los usuarios.

Desde la perspectiva de la teoría clásica de protección de datos, los principios de licitud, finalidad, minimización, exactitud, seguridad y responsabilidad (OECD, 2021) constituyen el marco universal para evaluar cualquier tratamiento de información personal. Estos principios establecen límites claros al uso de datos y orientan la obligación de proteger al titular frente a riesgos derivados del tratamiento automatizado. En contraste, el carácter dinámico y autónomo

de la IA desafía la aplicación lineal de estos principios, debido a la opacidad inherente de los modelos y a la dificultad de rastrear cómo se generan las decisiones (Richard & Blake, 2024).

La teoría de la gobernanza algorítmica aporta una visión contemporánea al señalar que los sistemas de IA requieren marcos adicionales de control, tales como trazabilidad, explicabilidad y auditoría continua. Desde esta perspectiva, autores como Crisanto et al. (2024) destacan que los supervisores financieros deben adoptar enfoques basados en riesgo para regular modelos algorítmicos que operan con altos niveles de autonomía. Esta teoría permite explicar por qué los modelos financieros, a pesar de su eficiencia, pueden generar discriminación, decisiones injustificadas o vulnerabilidades si no existen mecanismos institucionales de control.

Por su parte, la literatura sobre sesgo y equidad algorítmica representada por estudios como el de Selvam (2025) introduce la importancia de integrar métricas de equidad y técnicas de mitigación de sesgos. Esto complementa la teoría de gobernanza algorítmica al demostrar que no basta con cumplir normas formales; es necesario que los modelos sean "justos" y verificables en su desempeño. En el sistema financiero, donde las decisiones impactan directamente el acceso al crédito, la asignación de riesgos y la interacción con servicios digitales, este enfoque resulta crucial.

Finalmente, la teoría del riesgo tecnológico usada por organismos como el Financial Stability Board y el BIS integra los elementos anteriores bajo una lógica de gestión institucional del riesgo. Esta teoría sostiene que tecnologías como la IA amplifican riesgos operativos, de ciberseguridad y reputacionales, por lo que deben evaluarse mediante esquemas estructurados como las evaluaciones de impacto en privacidad (DPIA) (BIS, 2024).

La articulación de estas teorías permite comprender el fenómeno investigado de manera integral: mientras la protección de datos establece los principios base, la gobernanza algorítmica y la equidad complementan la necesidad de transparencia, y la teoría del riesgo tecnológico marca la pauta para institucionalizar prácticas de supervisión en el sistema financiero hondureño.

2.3 MARCO TEÓRICO

El marco teórico de esta investigación se orienta al análisis de la protección de datos personales en soluciones de inteligencia artificial dentro del sistema financiero hondureño a

partir de tres enfoques complementarios: la protección de datos, la gobernanza responsable de la inteligencia artificial y la transparencia o explicabilidad en sistemas automatizados. Estos enfoques permiten examinar el problema desde una perspectiva analítica centrada en los mecanismos institucionales de control, la gestión de riesgos, la supervisión de procesos automatizados y la capacidad de las organizaciones para implementar soluciones tecnológicas de manera responsable y verificable.

A partir de esta estructura, el marco teórico proporciona una base coherente para analizar las prácticas actuales del sistema financiero hondureño en materia de protección de datos personales, considerando la necesidad de fortalecer la responsabilidad institucional, la trazabilidad, la supervisión y la transparencia en el uso de sistemas automatizados. Asimismo, orienta la interpretación de los hallazgos y facilita la formulación de recomendaciones dirigidas a promover una implementación responsable, verificable y alineada con criterios de protección de datos en el uso de inteligencia artificial dentro del sector financiero nacional.

2.3.1 COMPARACIÓN Y ARTICULACIÓN TEÓRICA APLICABLE AL FENÓMENO INVESTIGADO

El fenómeno investigado, la protección de datos personales en soluciones de inteligencia artificial (IA) usadas por entidades del sistema financiero hondureño requiere articular diversas perspectivas teóricas para comprender cómo interactúan la regulación, la tecnología y la gestión institucional. La literatura internacional, regional y local revela convergencias y tensiones que explican las brechas actuales entre la adopción acelerada de IA y la capacidad normativa para garantizar la privacidad de los usuarios.

Desde la perspectiva de la teoría clásica de protección de datos, los principios de licitud, finalidad, minimización, exactitud, seguridad y responsabilidad (OECD, 2021) constituyen el marco universal para evaluar cualquier tratamiento de información personal. Estos principios establecen límites claros al uso de datos y orientan la obligación de proteger al titular frente a riesgos derivados del tratamiento automatizado. En contraste, el carácter dinámico y autónomo de la IA desafía la aplicación lineal de estos principios, debido a la opacidad inherente de los modelos y a la dificultad de rastrear cómo se generan las decisiones (Richard & Blake, 2024).

La teoría de la gobernanza algorítmica aporta una visión contemporánea al señalar que los sistemas de IA requieren marcos adicionales de control, tales como trazabilidad,

explicabilidad y auditoría continua. Desde esta perspectiva, autores como Crisanto et al. (2024) destacan que los supervisores financieros deben adoptar enfoques basados en riesgo para regular modelos algorítmicos que operan con altos niveles de autonomía. Esta teoría permite explicar por qué los modelos financieros, a pesar de su eficiencia, pueden generar discriminación, decisiones injustificadas o vulnerabilidades si no existen mecanismos institucionales de control.

Por su parte, la literatura sobre sesgo y equidad algorítmica representada por estudios como el de Selvam (2025), introduce la importancia de integrar métricas de equidad y técnicas de mitigación de sesgos. Esto complementa la teoría de gobernanza algorítmica al demostrar que no basta con cumplir normas formales; es necesario que los modelos sean "justos" y verificables en su desempeño. En el sistema financiero, donde las decisiones impactan directamente el acceso al crédito, la asignación de riesgos y la interacción con servicios digitales, este enfoque resulta crucial.

Finalmente, la teoría del riesgo tecnológico usada por organismos como el Financial Stability Board y el BIS integra los elementos anteriores bajo una lógica de gestión institucional del riesgo. Esta teoría sostiene que tecnologías como la IA amplifican riesgos operativos, de ciberseguridad y reputacionales, por lo que deben evaluarse mediante esquemas estructurados como las evaluaciones de impacto en privacidad (DPIA) (BIS, 2024).

La articulación de estas teorías permite comprender el fenómeno investigado de manera integral: mientras la protección de datos establece los principios base, la gobernanza algorítmica y la equidad complementan la necesidad de transparencia, y la teoría del riesgo tecnológico marca la pauta para institucionalizar prácticas de supervisión en el sistema financiero hondureño.

2.4 MARCO METODOLÓGICO

El marco metodológico del presente estudio se orienta al análisis del estado actual de la protección de datos personales en soluciones de inteligencia artificial utilizadas en el sistema financiero hondureño. Para ello, se adopta un enfoque cuantitativo, el cual permite recopilar y analizar datos de manera objetiva, a partir de la percepción de profesionales que participan directamente en la gestión, implementación o supervisión de soluciones tecnológicas dentro de

las instituciones financieras. Este enfoque resulta adecuado cuando se busca describir y analizar fenómenos actuales mediante datos medibles y comparables (Sedgwick, 2014).

El diseño de la investigación es no experimental y de tipo transversal, dado que las variables no son manipuladas deliberadamente, sino observadas tal como se presentan en su contexto real en un momento determinado. Este tipo de diseño es ampliamente utilizado en estudios organizacionales y tecnológicos, especialmente cuando el objetivo es diagnosticar el estado actual de prácticas, procesos o controles relacionados con un fenómeno específico (Kelley et al., 2003).

En ese mismo sentido, el estudio adopta un alcance descriptivo–correlacional, ya que se busca identificar las características, condiciones y prácticas existentes en relación con la protección de datos personales en soluciones de inteligencia artificial, sin establecer relaciones causales. La elección de este enfoque metodológico se fundamenta en la necesidad de generar evidencia empírica que permita comprender el nivel de madurez institucional en materia de protección de datos dentro del sistema financiero hondureño, aportando información relevante para futuras investigaciones y procesos de mejora (Zarsky, 2016).

2.4.1 MÉTODOS UTILIZADOS EN ESTUDIOS PREVIOS

La revisión de la literatura sobre inteligencia artificial, protección de datos y banca evidencia un uso consistente de enfoques metodológicos que combinan análisis documental especializado, técnicas cualitativas y, en menor medida, estrategias mixtas orientadas al análisis de riesgo tecnológico. En términos generales, los estudios más influyentes parten de una revisión sistemática o estructurada de fuentes académicas, regulatorias y técnicas, para luego profundizar mediante estudios de caso, entrevistas o cuestionarios aplicados a actores clave del sistema financiero (Ashrafuzzaman et al., 2025; Crisanto et al., 2024).

En el plano analítico, uno de los métodos más recurrentes es la revisión documental de tipo sistemático o semisistemático. Trabajos como el de Ashrafuzzaman et al. (2025) sobre personalización bancaria impulsada por IA emplean protocolos PRISMA para depurar artículos, establecer criterios de inclusión y organizar los hallazgos en categorías temáticas relacionadas con comportamiento del cliente, riesgos de perfilamiento y retos de privacidad. De forma complementaria, estudios comparativos como el de Irfan et al. (2024) sobre GDPR y CCPA utilizan matrices analíticas para contrastar obligaciones, principios y mecanismos de

cumplimiento aplicables al tratamiento automatizado de datos. En el ámbito de política financiera, el Banco de Pagos Internacionales recurre al análisis de documentos regulatorios, respuestas de supervisores y casos de uso supervisados, con el fin de caracterizar los riesgos asociados a la IA y las respuestas regulatorias emergentes (Crisanto et al., 2024).

Junto a estas aproximaciones documentales, la literatura incorpora con frecuencia técnicas cualitativas orientadas a comprender cómo se implementan en la práctica las exigencias normativas y los principios de protección de datos. Entrevistas semiestructuradas con oficiales de cumplimiento, responsables de ciberseguridad, áreas de riesgo y equipos de ciencia de datos son un recurso metodológico habitual en investigaciones que abordan la gobernanza algorítmica y la gestión institucional de la privacidad en banca. Estas entrevistas permiten explorar el nivel de madurez de los procesos internos, las barreras organizacionales para adoptar evaluaciones de impacto en privacidad y los criterios utilizados para la selección y despliegue de modelos de IA. Adicionalmente, el análisis de contenido de políticas de privacidad, avisos a usuarios, manuales internos y lineamientos de cumplimiento constituye una técnica central para identificar vacíos, ambigüedades o falta de alineación con estándares internacionales como el GDPR o las directrices de la OCDE (OECD, 2021; Richard & Blake, 2024).

En estudios con foco en riesgo y equidad algorítmica, se observa el uso de marcos metodológicos basados en el análisis de riesgo tecnológico. Informes del BIS y trabajos académicos recientes emplean esquemas de identificación, valoración y tratamiento de riesgos que consideran la probabilidad y el impacto de fallas de modelo, sesgos, brechas de seguridad o dependencias críticas de terceros (BIS, 2024; Selvam, 2025). En algunos casos, estos análisis se complementan con la aplicación de métricas de desempeño y equidad en modelos de scoring o monitoreo transaccional, a fin de evaluar su comportamiento frente a grupos de usuarios diferenciados y detectar posibles efectos discriminatorios. Aunque este enfoque experimental o cuasiexperimental es menos frecuente en contextos regulados, su presencia en la literatura sirve como referencia metodológica para futuras evaluaciones técnicas de modelos en producción.

En el ámbito regional latinoamericano, los estudios sobre marcos regulatorios de IA y protección de datos se inclinan hacia diseños descriptivos y comparativos, apoyados principalmente en análisis documental y consultas a expertos. Informes como los de AlSur (2024) combinan revisión normativa y entrevistas con actores institucionales para mapear el estado de avance de los países en materia de regulación de IA y datos personales. En el caso hondureño, documentos como los estudios de barreras regulatorias en tecno-finanzas

elaborados por el Banco Central de Honduras y la CNBS utilizan metodologías de diagnóstico que integran revisión de normativa, análisis de casos y consultas con stakeholders del ecosistema financiero, con el fin de identificar brechas legales e institucionales.

En síntesis, los métodos utilizados en estudios previos muestran una clara preferencia por enfoques descriptivo–analíticos, basados en revisión documental rigurosa, análisis cuantitativo de contenido e incorporación selectiva de entrevistas y encuestas a actores clave. Allí donde se aborda directamente el desempeño de los modelos de IA, se incorporan técnicas de análisis de riesgo y, en menor medida, herramientas cuantitativas para evaluar sesgos y efectos distributivos. Este panorama metodológico ofrece un referente robusto para el diseño de investigaciones en el contexto hondureño, al demostrar que la combinación de análisis documental, aproximaciones cualitativas y marcos de riesgo constituye una vía adecuada para estudiar la protección de datos en soluciones de IA dentro del sistema financiero.

2.4.2 JUSTIFICACIÓN DEL ENFOQUE DEL ESTUDIO

El procedimiento metodológico seleccionado para este estudio de carácter descriptivo correlacional, con enfoque cuantitativo de corte transversal, apoyado en revisión documental y recolección de información en entidades financiera se justifica por la naturaleza compleja del fenómeno investigado: la protección de datos personales en soluciones de inteligencia artificial (IA) dentro del sistema financiero hondureño.

En primer lugar, un diseño descriptivo correlacional resulta pertinente porque el objetivo central no es probar una relación causal entre variables, sino caracterizar y analizar el nivel de cumplimiento de principios de protección de datos, la existencia de mecanismos de gobernanza algorítmica y las brechas entre marcos normativos de referencia y prácticas institucionales. La literatura metodológica señala que los estudios descriptivo–analíticos son adecuados cuando se busca examinar fenómenos poco explorados, ordenar información dispersa y generar un diagnóstico integral que sirva de base para futuras intervenciones o investigaciones explicativas (Hernández-Sampieri et al., 2014; Creswell & Creswell, 2018).

En segundo lugar, el enfoque cuantitativo se justifica porque el objeto de estudio implica comprender cómo los actores internos interpretan, implementan y gestionan la protección de datos en proyectos de IA. Aspectos como la gobernanza algorítmica, la evaluación de impacto en privacidad o la gestión de riesgos tecnológicos requieren captar percepciones, criterios de

decisión y dinámicas organizacionales que difícilmente pueden ser reducidas a indicadores numéricos. Estudios internacionales sobre IA y regulación financiera, como los del Financial Stability Institute del BIS, han recurrido precisamente a análisis documentales combinados con consultas a expertos y supervisores para entender la respuesta institucional frente a tecnologías emergentes (Crisanto et al., 2024; BIS, 2024).

El carácter transversal del estudio también es consistente con la práctica académica en este campo: tanto investigaciones sobre marcos regulatorios de IA en América Latina (AlSur, 2024) como diagnósticos de barreras regulatorias en fintech en Honduras (BCH & CNBS, 2021) analizan la situación en un momento determinado, con el fin de ofrecer una "fotografía" del estado actual que sirva de línea base para futuras actualizaciones. Dado que el ecosistema regulatorio y tecnológico evoluciona rápidamente, un diseño transversal permite capturar de manera realista el nivel de madurez alcanzado por las entidades financieras en el momento de la investigación.

Finalmente, la combinación de revisión documental especializada (normativa internacional, lineamientos de la CNBS, políticas internas, avisos de privacidad) con técnicas cualitativas (entrevistas y/o cuestionarios a responsables de cumplimiento, TI, ciberseguridad y riesgo) se alinea con las mejores prácticas observadas en estudios sobre privacidad y IA en el sector financiero. Investigaciones recientes sobre personalización bancaria, sesgo algorítmico y protección de datos han mostrado que la triangulación entre documentos normativos, evidencia organizacional y testimonios de actores clave aumenta la validez y la profundidad interpretativa de los resultados (Ashrafuzzaman et al., 2025; Selvam, 2025). En consecuencia, el procedimiento seleccionado permite responder de forma rigurosa y contextualizada a la pregunta de investigación, aportando un diagnóstico sólido y útil para entidades financieras y reguladores hondureños.

CAPÍTULO III. METODOLOGÍA

En este capítulo se presenta la metodología que respalda la investigación, especificando el tipo y enfoque del estudio, la conceptualización y adaptación de las variables, así como la población, la muestra y las unidades de análisis consideradas. Además, se detallan los instrumentos y métodos utilizados para la recolección y análisis de datos, junto con los principios éticos aplicados y las principales limitaciones del estudio. La organización de esta sección asegura la consistencia entre el marco teórico, los objetivos establecidos y la etapa empírica de la investigación, garantizando la rigurosidad científica en la obtención e interpretación de los resultados.

3.1 TIPO Y ENFOQUE DE INVESTIGACIÓN

La presente investigación se desarrolla bajo un enfoque cuantitativo, en tanto se orienta a medir y analizar, mediante datos numéricos, diversos aspectos relacionados con el uso de soluciones de inteligencia artificial y la protección de datos personales en el sistema financiero hondureño. Este enfoque permite operacionalizar las variables de interés en indicadores observables como nivel de adopción de herramientas de IA, grado de cumplimiento de principios de protección de datos o percepción de confianza de los usuarios y someterlos a procedimientos estadísticos descriptivos y correlacionales que brinden evidencia objetiva para la interpretación de los resultados (Hernández-Sampieri et al., 2014).

El estudio adopta un diseño no experimental, debido a que las variables no serán manipuladas deliberadamente, sino observadas tal y como se presentan en su contexto natural dentro de las instituciones financieras. El investigador no introducirá tratamientos ni intervenciones sobre los procesos de gestión de datos ni sobre el funcionamiento de las soluciones de IA; más bien, se limitará a registrar la información obtenida a través de instrumentos estructurados y fuentes documentales. En ese mismo sentido, el diseño es de corte transversal, puesto que la recolección de datos se llevará a cabo en un único momento del tiempo, con el propósito de ofrecer una caracterización del estado actual de la relación entre inteligencia artificial y protección de datos personales en el sistema financiero hondureño (Bisquerra, 2014).

Por su alcance, la investigación se clasifica como descriptiva–correlacional. Se considera descriptiva porque busca detallar cómo se utilizan las soluciones de IA en las

entidades financieras, qué medidas de protección de datos se han implementado y cuál es el nivel de cumplimiento de los marcos normativos aplicables. De forma complementaria, se considera correlacional, ya que pretende identificar y analizar las asociaciones estadísticas entre variables como el nivel de adopción de IA, el grado de madurez en protección de datos y la confianza de los usuarios en los servicios financieros digitales. Este tipo de estudio resulta pertinente para generar evidencia empírica que fortalezca la gobernanza de datos, oriente la formulación de políticas internas y respalde propuestas de mejora para un uso ético, seguro y responsable de la inteligencia artificial en el sistema financiero. Asimismo, la elección de este enfoque metodológico es coherente con los objetivos específicos del estudio, al posibilitar la comparación entre grupos de interés y la obtención de resultados empíricos replicables y contrastables en futuras investigaciones.

3.2 VARIABLES

En esta investigación se distinguen dos tipos de variables: independiente y dependiente. Desde la perspectiva de la metodología cuantitativa, las variables representan propiedades observables de los fenómenos que pueden adoptar distintos valores y se emplean para contrastar hipótesis sobre relaciones o diferencias entre grupos (Hernández-Sampieri & Mendoza, 2018). En los estudios con hipótesis causales, la variable independiente se asocia con la posible causa o factor explicativo, mientras que la variable dependiente corresponde al efecto o resultado esperado de dicha influencia.

La variable independiente que se examina en esta investigación se refiere a la cantidad de implementación de herramientas de inteligencia artificial dentro del sector financiero de Honduras. Se comprende en términos generales como el nivel en que las instituciones financieras integran tecnologías de IA, incluyendo algoritmos de machine learning, sistemas para identificar fraudes o asistentes virtuales en sus actividades de atención al cliente, administración de riesgos y operaciones internas. La investigación existente sobre IA en el ámbito financiero la describe como la aplicación de algoritmos sofisticados y modelos de machine learning para evaluar grandes conjuntos de datos, automatizar procesos y mejorar la toma de decisiones en productos y servicios financieros en línea.

La variable dependiente que se considera es el grado de resguardo de información personal al utilizar herramientas de inteligencia artificial. Se define como el conjunto de principios, reglamentaciones, políticas y medidas técnicas y organizativas que tienen como

objetivo asegurar que el manejo de datos personales mantenga su confidencialidad, integridad y disponibilidad, así como los derechos de los titulares frente al uso inapropiado de la información. Diferentes orientaciones y marcos normativos definen la protección de datos como un sistema de acciones legales y tecnológicas que brindan a los individuos control sobre su información personal y exigen a las entidades implementar medidas de seguridad adecuadas al riesgo, particularmente cuando se utilizan tecnologías de gran impacto como la inteligencia artificial.

3.3 OPERACIONALIZACIÓN DE VARIABLES

La operacionalización de variables consiste en transformar conceptos teóricos en dimensiones e indicadores observables y medibles, definiendo además las escalas de medición y los procedimientos de recolección de datos. Este proceso permite vincular el marco teórico con la fase empírica, asegurando que la medición sea coherente con las definiciones conceptuales de las variables independiente y dependiente del estudio.

En el caso de la variable independiente, nivel de adopción de soluciones de inteligencia artificial en el sistema financiero hondureño, la operacionalización se estructura en dimensiones que recogen el uso de IA en procesos clave, el grado de madurez de su implementación y la existencia de mecanismos de gobernanza. Estudios y marcos recientes sobre adopción de IA en servicios financieros proponen indicadores como presencia de sistemas de IA en procesos críticos, número de casos de uso en producción, existencia de estrategia formal de IA y mecanismos de supervisión interna. Estos indicadores suelen medirse mediante encuestas estructuradas y cuestionarios dirigidos a responsables de negocio y tecnología, utilizando escalas tipo Likert u opciones categóricas (sí/no, niveles de adopción) para permitir análisis descriptivos y correlacionales.

Respecto a la variable dependiente, nivel de protección de datos personales en el uso de soluciones de IA, la operacionalización se basa en dimensiones vinculadas al cumplimiento de principios de protección de datos, la implementación de salvaguardas técnicas y organizativas, y la transparencia frente a los titulares de la información. Los marcos internacionales, como las Directrices de Privacidad de la OCDE y los principios de protección de datos del Reglamento General de Protección de Datos (GDPR), procedimientos y avisos de privacidad, utilizando escalas ordinales (por ejemplo, grado de cumplimiento percibido en escala de 1 a 5) y listas de cotejo para validar la existencia de controles formales.

Tabla 1. Operacionalización de variables de la investigación

Variable independiente	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Ítems	Unidades/ categorías	Escala
Nivel de adopción de soluciones de IA	El nivel de adopción de soluciones de inteligencia artificial se entiende como el grado en que las instituciones financieras incorporan tecnologías basadas en IA en sus procesos operativos, de análisis y toma de decisiones.	El nivel de adopción de soluciones de IA se mide a través del uso de IA en procesos clave, la madurez de implementación y la gobernanza y gestión de IA, mediante un cuestionario tipo Likert aplicado a profesionales del sistema financiero.	Uso de IA en procesos clave	Atención al cliente con IA	¿Cómo considera usted el impacto de la atención a la cliente apoyada en inteligencia artificial sobre la eficiencia operativa de los servicios financieros en la institución?	Totalmente de acuerdo	5
						De acuerdo	4
						Ni de acuerdo ni en desacuerdo	3
						En desacuerdo	2
						Totalmente en desacuerdo	1
				Detección y prevención de fraude con IA	¿La inteligencia artificial contribuye a la detección y prevención de fraudes financieros??	Totalmente de acuerdo	5
						De acuerdo	4
						Ni de acuerdo ni en desacuerdo	3
						En desacuerdo	2
						Totalmente en desacuerdo	1
				Automatización del análisis de riesgo / crédito con IA	¿La automatización del análisis de riesgo y crédito mediante IA mejora la toma de decisiones financieras?	Totalmente de acuerdo	5
						De acuerdo	4
						Ni de acuerdo ni en desacuerdo	3
						En desacuerdo	2
						Totalmente en desacuerdo	1

Variable independiente	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Ítems	Unidades/ categorías	Escala
Nivel de adopción de soluciones de IA			Madurez de implementación de IA	Casos de uso de IA en producción	En mi institución existen casos de uso de inteligencia artificial operando en ambientes de producción.	Totalmente de acuerdo	5
						De acuerdo	4
						Ni de acuerdo ni en desacuerdo	3
						En desacuerdo	2
						Totalmente en desacuerdo	1
				Integración de IA con sistemas centrales del banco	¿Las soluciones de inteligencia artificial están integradas con los sistemas centrales del banco?	Totalmente de acuerdo	5
						De acuerdo	4
						Ni de acuerdo ni en desacuerdo	3
						En desacuerdo	2
						Totalmente en desacuerdo	1
				Estrategia u hoja de ruta de IA	¿La institución cuenta con una estrategia u hoja de ruta definida para la implementación de inteligencia artificial?	Totalmente de acuerdo	5
						De acuerdo	4
						Ni de acuerdo ni en desacuerdo	3
						En desacuerdo	2
						Totalmente en desacuerdo	1

Variable independiente	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Ítems	Unidades/ categorías	Escala
Nivel de adopción de soluciones de IA			Gobernanza y gestión de IA	Políticas internas sobre IA	¿Mi institución cuenta con políticas internas que regulan el uso de soluciones de inteligencia artificial?	Totalmente de acuerdo	5
						De acuerdo	4
						Ni de acuerdo ni en desacuerdo	3
						En desacuerdo	2
						Totalmente en desacuerdo	1
				Roles y comités responsables de IA	¿Existen roles y comités responsables de la supervisión de la inteligencia artificial en la institución?	Totalmente de acuerdo	5
						De acuerdo	4
						Ni de acuerdo ni en desacuerdo	3
						En desacuerdo	2
						Totalmente en desacuerdo	1
				Evaluaciones de impacto en datos personales	¿La institución realiza evaluaciones de impacto en protección de datos para los sistemas de inteligencia artificial?	Totalmente de acuerdo	5
						De acuerdo	4
						Ni de acuerdo ni en desacuerdo	3
						En desacuerdo	2
						Totalmente en desacuerdo	1

Tabla 2. Operacionalización de variables de la investigación

Variable dependiente	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Ítems	Unidades/ categorías	Escala
Nivel de protección de datos personales en el uso de IA	El nivel de protección de datos personales se entiende como el conjunto de principios, normas y medidas técnicas y organizativas destinadas a garantizar la confidencialidad, integridad, disponibilidad y licitud del tratamiento de datos personales, particularmente en sistemas basados en inteligencia artificial.	El nivel de protección de datos personales se mide a través del cumplimiento de principios de protección de datos, la aplicación de medidas de seguridad y controles técnicos, y la transparencia y ejercicio de derechos del titular.	Cumplimiento de principios de protección de datos	Licitud y finalidad del tratamiento	¿Considera usted que la institución define y deja por escrito las finalidades para las cuales se utilizan los datos personales en sistemas de inteligencia artificial?	Totalmente de acuerdo	5
						De acuerdo	4
						Ni de acuerdo ni en desacuerdo	3
						En desacuerdo	2
						Totalmente en desacuerdo	1
				Minimización y proporcionalidad	¿Solo se utilizan los datos personales estrictamente necesarios para el funcionamiento de los sistemas de IA??	Totalmente de acuerdo	5
						De acuerdo	4
						Ni de acuerdo ni en desacuerdo	3
						En desacuerdo	2
						Totalmente en desacuerdo	1
				Plazo de conservación	¿Considera usted que, en la institución, se definen y aplican criterios claros para el tiempo de conservación de los datos personales utilizados por sistemas de inteligencia artificial?	Totalmente de acuerdo	5
						De acuerdo	4
						Ni de acuerdo ni en desacuerdo	3
						En desacuerdo	2
						Totalmente en desacuerdo	1

Variable dependiente	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Ítems	Unidades/ categorías	Escala
Nivel de protección de datos personales en el uso de IA			Medidas de seguridad y controles técnicos	Autenticación y control de acceso	¿Los sistemas de IA cuentan con mecanismos de autenticación y control de acceso para proteger los datos personales??	Totalmente de acuerdo	5
						De acuerdo	4
						Ni de acuerdo ni en desacuerdo	3
						En desacuerdo	2
						Totalmente en desacuerdo	1
				Cifrado y registro de auditoría	¿Los datos personales tratados por sistemas de IA se encuentran cifrados y sujetos a registros de auditoría??	Totalmente de acuerdo	5
						De acuerdo	4
						Ni de acuerdo ni en desacuerdo	3
						En desacuerdo	2
						Totalmente en desacuerdo	1
				Gestión de incidentes y violaciones de datos	¿Existen procedimientos definidos para gestionar incidentes y violaciones de datos relacionados con sistemas de IA??	Totalmente de acuerdo	5
						De acuerdo	4
						Ni de acuerdo ni en desacuerdo	3
						En desacuerdo	2
						Totalmente en desacuerdo	1

Variable dependiente	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Ítems	Unidades/ categorías	Escala
Nivel de protección de datos personales en el uso de IA			Transparencia y derechos del titular	Avisos de privacidad específicos para IA	¿Mi institución cuenta con avisos de privacidad específicos para el uso de inteligencia artificial??	Totalmente de acuerdo	5
						De acuerdo	4
						Ni de acuerdo ni en desacuerdo	3
						En desacuerdo	2
						Totalmente en desacuerdo	1
				Canales para ejercer derechos	¿La institución dispone de mecanismos accesibles para que los titulares de datos personales puedan ejercer sus derechos?	Totalmente de acuerdo	5
						De acuerdo	4
						Ni de acuerdo ni en desacuerdo	3
						En desacuerdo	2
						Totalmente en desacuerdo	1
				Información sobre decisiones automatizadas y perfiles	¿Considera usted que, en la institución, existen canales claros y accesibles para que los titulares de datos personales ejerzan sus derechos?	Totalmente de acuerdo	5
						De acuerdo	4
						Ni de acuerdo ni en desacuerdo	3
						En desacuerdo	2
						Totalmente en desacuerdo	1

3.4 DIAGRAMA DE LAS VARIABLES

En este apartado se presentan el diagrama de cada una de las variables de investigación:

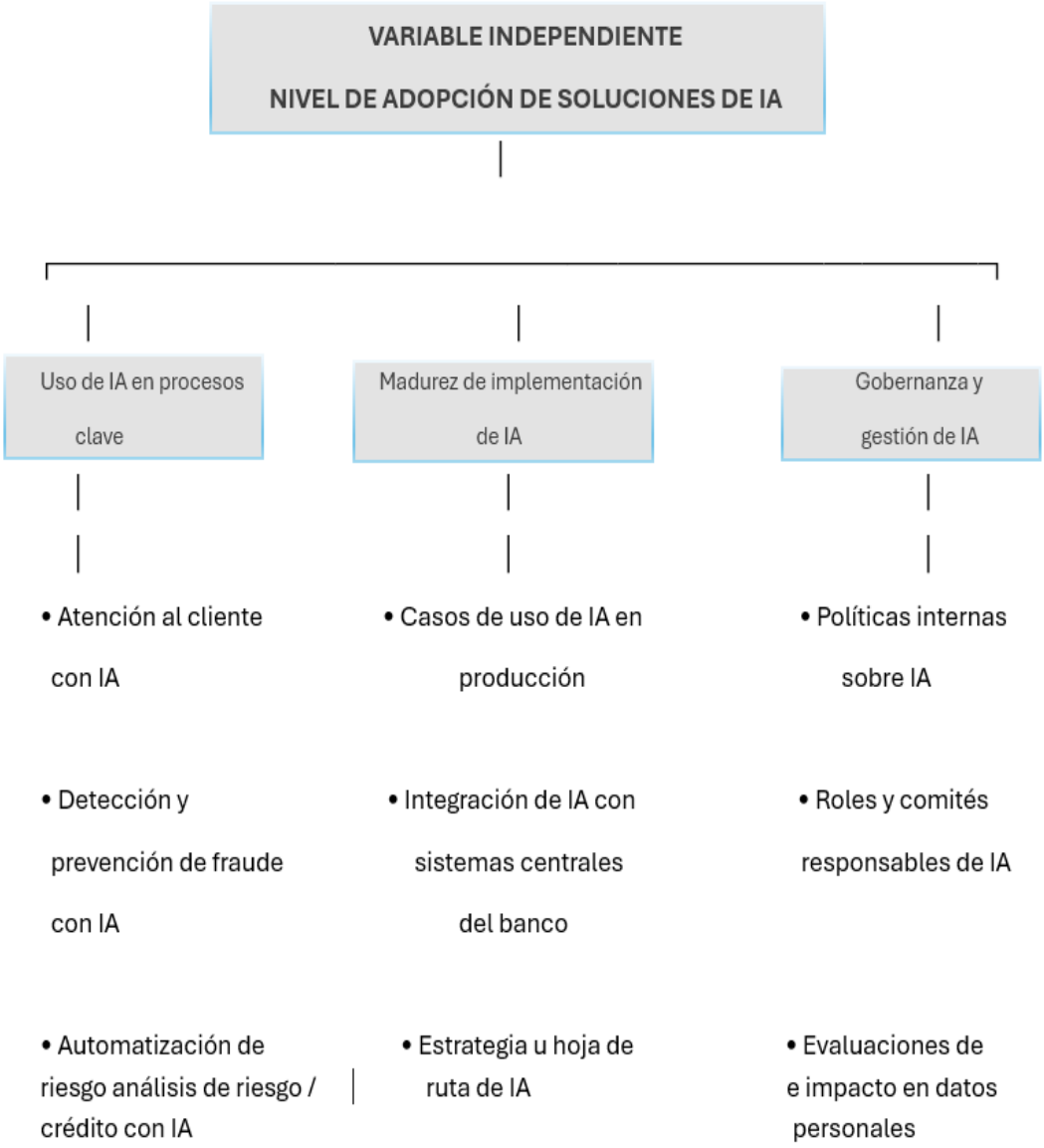


Figura 3. Diagramas de variables independiente

Fuente: Elaboración propia.

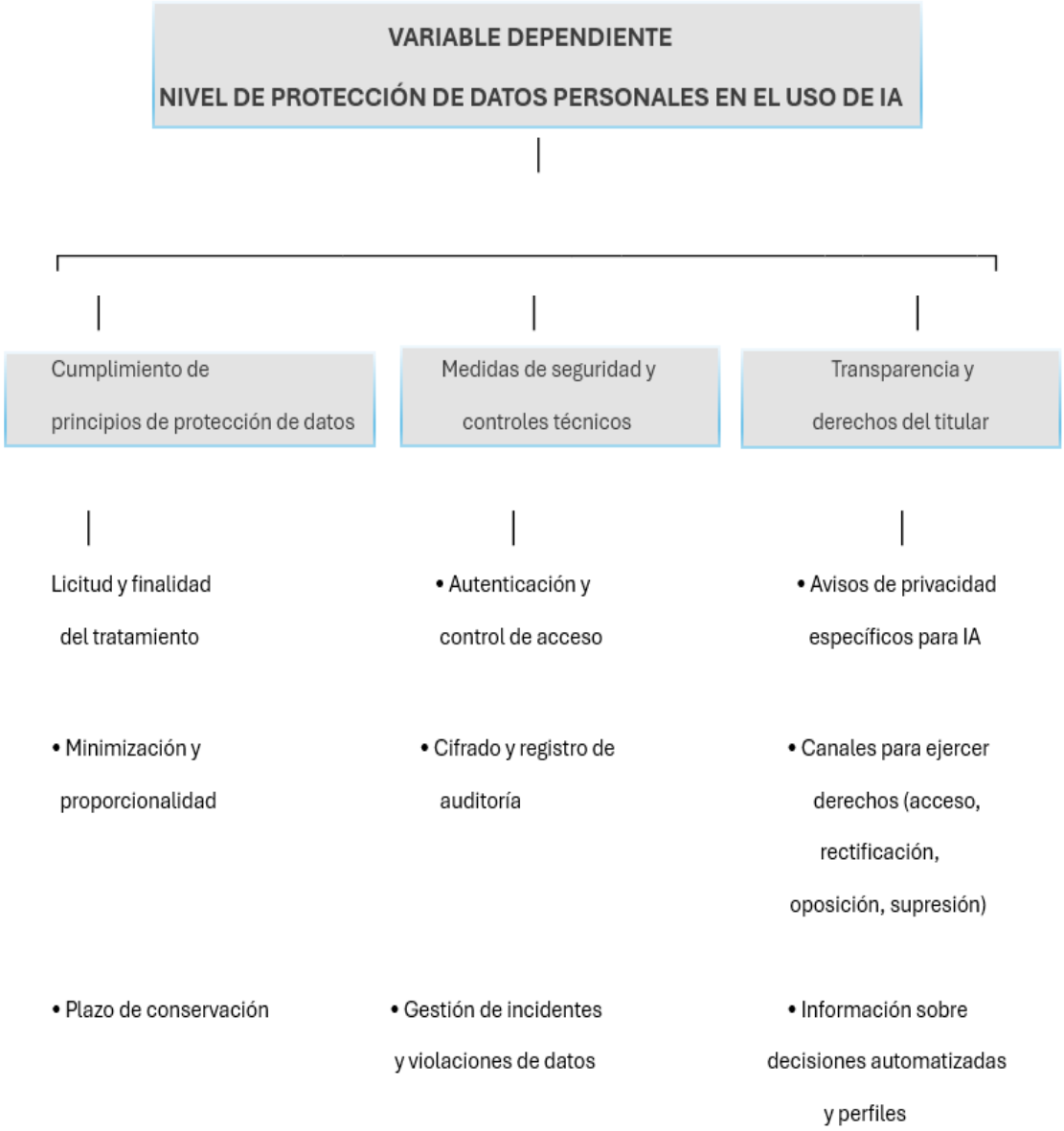


Figura 4. Diagramas de variables dependiente

Fuente: Elaboración propia.

3.5 HIPÓTESIS

Las hipótesis del estudio se formulan a partir de la relación entre el nivel de adopción de soluciones de inteligencia artificial y el nivel de protección de datos personales en el sistema financiero hondureño.

Diversos enfoques teóricos señalan que la implementación de inteligencia artificial requiere el fortalecimiento de marcos de gobernanza de datos, controles de seguridad y prácticas de privacidad, lo que sugiere una posible relación entre ambas variables.

En este sentido, se plantea la siguiente hipótesis de investigación:

Hi: A mayor nivel de adopción de soluciones de inteligencia artificial en las instituciones del sistema financiero hondureño, mayor será el nivel de protección de datos personales asociado a su uso.

Del mismo modo, se establece la hipótesis nula:

H_0: El nivel de adopción de soluciones de inteligencia artificial en las instituciones del sistema financiero hondureño no se relaciona de manera significativa con el nivel de protección de datos personales.

La contrastación de estas hipótesis se realizará mediante análisis estadístico correlacional, acorde con el enfoque cuantitativo y el diseño no experimental transversal del estudio.

3.6 MATRIZ DE ALINEACIÓN METODOLÓGICA

Con el propósito de asegurar la coherencia interna de la investigación, se presenta la matriz de alineación metodológica, en la cual se relacionan los objetivos específicos con las variables, dimensiones, instrumentos de medición, técnicas de análisis y resultados esperados. Esta matriz permite evidenciar que lo planteado en los objetivos de la investigación corresponde directamente con lo medido mediante el instrumento aplicado, lo analizado en los resultados y lo abordado posteriormente en las conclusiones y recomendaciones.

Tabla 3. Matriz de alineación metodológica de la investigación

Objetivo específico	Variable relacionada	Dimensiones evaluadas	Ítems del instrumento	Técnica de análisis	Resultado esperado
Describir el nivel de adopción de soluciones de inteligencia artificial en instituciones del sistema financiero hondureño, considerando su uso en procesos clave, madurez de implementación y mecanismos de gobernanza institucional.	Nivel de adopción de soluciones de IA	Uso de IA en procesos clave; madurez de implementación; gobernanza y gestión de IA.	Ítems 3 al 11	Estadística descriptiva: frecuencias, porcentajes, media y desviación estándar.	Identificar el grado de adopción de soluciones de IA en las instituciones participantes.
Determinar el nivel de protección de datos personales asociado al uso de soluciones de inteligencia artificial, considerando principios de protección de datos, controles técnicos, transparencia y mecanismos para el ejercicio de derechos de los titulares.	Nivel de protección de datos personales en el uso de IA	Cumplimiento de principios de protección de datos; medidas de seguridad y controles técnicos; transparencia y derechos del titular.	Ítems 12 al 20	Estadística descriptiva: frecuencias, porcentajes, media y desviación estándar.	Identificar el nivel de protección de datos personales asociado al uso de IA.
Analizar la relación entre el nivel de adopción de soluciones de inteligencia artificial y el nivel de protección de datos personales en las instituciones participantes del sistema financiero hondureño.	Nivel de adopción de soluciones de IA y nivel de protección de datos personales en el uso de IA.	Relación entre ambas variables principales del estudio.	Promedios agrupados de los ítems 3 al 11 y 12 al 20.	Correlación de Spearman.	Determinar si existe una relación estadísticamente significativa entre la adopción de IA y la protección de datos personales.

Fuente: Elaboración propia.

3.7 POBLACIÓN Y MUESTRA

Para esta investigación, la población se define como el conjunto de profesionales que laboran en instituciones del sistema financiero hondureño y que participan en la gestión de tecnologías de información, seguridad de la información, analítica de datos, riesgo operativo o canales digitales. En el contexto específico del estudio, la población está conformada por un total de 32 personas que cumplen con estas características dentro de las áreas señaladas. Metodológicamente, la población corresponde al grupo objetivo que comparte características relevantes para los objetivos del estudio y sobre el cual se pretende extrapolar los resultados empíricos; es decir, del cual se selecciona la muestra para representar sus atributos de forma práctica.

Dentro de esta población, el universo específico de interés está constituido por los colaboradores que poseen conocimiento directo del uso de soluciones de inteligencia artificial y de los controles de protección de datos personales implementados en sus instituciones. La población accesible se integra por quienes puedan ser contactados a través de las áreas de tecnología, seguridad de la información, riesgos, cumplimiento normativo o transformación digital, de modo que dispongan de información pertinente sobre ambas variables de estudio.

Los criterios de inclusión consideran: (a) desempeñar funciones relacionadas con TI, seguridad de la información, gestión de datos, riesgos, canales digitales o cumplimiento normativo; (b) contar con al menos un año de experiencia en la institución; y (c) aceptar participar de forma voluntaria y anónima completando el cuestionario en línea. Se excluyen colaboradores de áreas sin vinculación directa con los procesos de inteligencia artificial o protección de datos personales, personal temporal o en práctica profesional y respuestas incompletas o inconsistentes.

Dado que no existe un marco muestral público y exhaustivo de todos los profesionales que cumplen estos criterios, se empleó un muestreo no probabilístico por conveniencia, dirigido a informantes clave que cumplen con las características definidas para el estudio. Este enfoque permitió seleccionar participantes accesibles y vinculados funcionalmente con áreas de tecnología, seguridad de la información, gestión de datos, riesgos, canales digitales y cumplimiento normativo. Aunque esta estrategia limita la generalización estadística de los resultados, resulta pertinente para estudios aplicados en los que se requiere obtener información de perfiles con conocimiento directo o indirecto sobre el fenómeno investigado.

El tamaño de la muestra se fija en un mínimo de 30 cuestionarios válidos, criterio coherente con recomendaciones para investigaciones con análisis descriptivo y correlacional, que subrayan la necesidad de contar con tamaños muestrales suficientes para garantizar una potencia estadística razonable y estimaciones estables de las relaciones entre variables. Referentes clásicos como Krejcie y Morgan, así como revisiones recientes sobre tamaño muestral para estudios de encuesta, respaldan la utilización de este orden de magnitud para poblaciones moderadas.

No obstante, se procurará maximizar el número de respuestas obtenidas, de manera que, si la tasa de participación lo permite, se supere este umbral mínimo y se incremente la robustez de los análisis estadísticos previstos.

3.8 UNIDAD DE ANÁLISIS Y RESPUESTA

La unidad de análisis de esta investigación está constituida por los profesionales que laboran en instituciones del sistema financiero hondureño y que participan en la gestión de tecnologías de información, seguridad de la información, analítica de datos, riesgo operativo, canales digitales o cumplimiento normativo. Metodológicamente, la unidad de análisis corresponde al “quién” o “qué” del estudio, es decir, la entidad sobre la cual se observan y miden las variables y respecto de la cual se formulan inferencias y conclusiones (Sedgwick, 2014; Flannelly, Flannelly & Jankowski, 2014). En este caso, cada profesional constituye una unidad de análisis individual, al proporcionar información sobre el nivel de adopción de soluciones de inteligencia artificial y el nivel de protección de datos personales en su institución.

La unidad de respuesta coincide con la unidad de análisis, dado que cada cuestionario será completado por un único profesional que actúa como informante clave de su organización. Las percepciones y valoraciones de estos participantes se recogerán mediante un instrumento estructurado basado en una escala tipo Likert de cinco puntos, que permite graduar el grado de acuerdo o desacuerdo con enunciados relativos a las dimensiones de las variables estudiadas. Las escalas Likert se utilizan de forma extensiva en investigaciones de encuesta para medir actitudes y opiniones de manera ordinal, a través de categorías que van típicamente desde “totalmente en desacuerdo” hasta “totalmente de acuerdo”, facilitando así la cuantificación de las respuestas y su posterior análisis estadístico descriptivo y correlacional (Joshi et al., 2015; Boone & Boone, 2012).

Con el propósito de asegurar la pertinencia de las respuestas obtenidas, se consideraron como participantes válidos aquellos profesionales vinculados con áreas relacionadas con tecnología de la información, seguridad de la información, gestión de datos, riesgo operativo, canales digitales y cumplimiento normativo. Estos roles fueron seleccionados porque mantienen relación directa o indirecta con la adopción de soluciones de inteligencia artificial, el tratamiento de datos personales, la aplicación de controles de seguridad y la supervisión de riesgos tecnológicos dentro de las instituciones financieras.

El mapeo de roles permite justificar que los participantes cuentan con conocimiento funcional sobre las variables analizadas en el estudio: el nivel de adopción de soluciones de inteligencia artificial y el nivel de protección de datos personales asociado a su uso.

Tabla 4. Mapeo de roles de los participantes del estudio

Rol o área funcional	Justificación de inclusión en el estudio
Tecnología de la Información	Se incluye por su relación con la implementación, administración e integración de soluciones tecnológicas utilizadas por las instituciones financieras.
Seguridad de la Información	Se incluye por su relación con la protección de la confidencialidad, integridad y disponibilidad de los datos personales tratados por sistemas de IA.
Gestión de Datos / Analítica de Datos	Se incluye por su participación en el tratamiento, análisis, calidad, uso y gestión de datos institucionales.
Riesgo Operativo / Gestión de Riesgos	Se incluye por su función en la identificación, evaluación y tratamiento de riesgos asociados a procesos tecnológicos y financieros.
Canales Digitales / Transformación Digital	Se incluye por su relación con la implementación de soluciones digitales, automatización de servicios y experiencia del usuario.
Cumplimiento Normativo	Se incluye por su vinculación con políticas internas, normativa aplicable, principios de protección de datos y derechos de los titulares.

Fuente: Elaboración propia.

El mapeo anterior evidencia que los participantes pertenecen a áreas funcionales relacionadas con la adopción tecnológica, la protección de datos, la gestión de riesgos y el

cumplimiento institucional. Por tanto, sus respuestas constituyen insumos pertinentes para analizar el estado actual de la protección de datos personales en soluciones de inteligencia artificial dentro del sistema financiero hondureño.

3.9 INSTRUMENTOS DE RECOLECCIÓN DE DATOS

El instrumento principal de recolección de datos de la presente investigación es una encuesta estructurada, diseñada y administrada mediante Microsoft Forms, herramienta ampliamente utilizada en estudios cuantitativos por su facilidad de acceso, estandarización del formato y eficiencia en la recopilación de información. El uso de encuestas permite obtener datos homogéneos sobre percepciones, prácticas y niveles de adopción tecnológica en un periodo determinado, lo cual resulta coherente con el enfoque cuantitativo y el diseño no experimental transversal del estudio (Ranganathan & Aggarwal, 2024).

El cuestionario está dirigido a profesionales del sistema financiero hondureño vinculados a áreas de tecnología, seguridad de la información, gestión de datos, riesgos y canales digitales, quienes actúan como informantes clave. La estructura del instrumento contempla una sección inicial de datos generales del participante y un bloque principal de ítems formulados como afirmaciones, alineadas con las dimensiones de las variables independiente y dependiente. Estos ítems se miden mediante una escala tipo Likert de cinco puntos, que va desde “totalmente en desacuerdo” hasta “totalmente de acuerdo”, permitiendo captar el grado de acuerdo del encuestado de forma ordinal y facilitar el análisis estadístico posterior (Joshi et al., 2015; Boone & Boone, 2012).

La selección de Microsoft Forms se justifica adicionalmente por su capacidad para reducir errores de captura, facilitar el anonimato de los participantes y permitir la exportación directa de los datos a formatos compatibles con software estadístico. Estudios metodológicos señalan que las encuestas en línea constituyen un medio válido y confiable para la recolección de datos en investigaciones organizacionales, siempre que se apliquen criterios adecuados de diseño y control ético (Ranganathan et al., 2023). Finalmente, el instrumento será sometido a procesos de validez de contenido y confiabilidad interna, mediante el coeficiente alfa de Cronbach, conforme a las recomendaciones clásicas para instrumentos de medición en ciencias sociales (Carmines & Zeller, 1979).

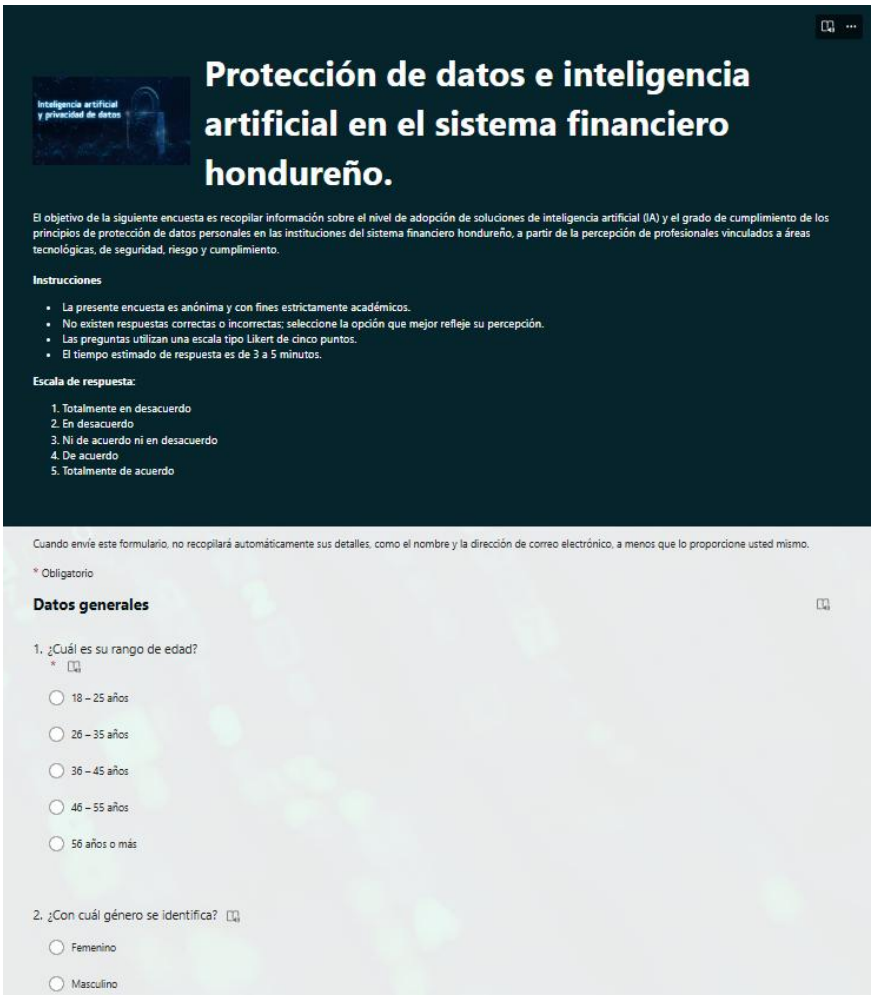


Figura 5. Elaboración propia.

Fuente: Elaboración propia.

3.10 TÉCNICAS DE RECOLECCIÓN Y ANÁLISIS

La técnica de recolección de datos utilizada en esta investigación es la encuesta, aplicada de forma electrónica mediante Microsoft Forms. La aplicación del instrumento se realizará de manera autoadministrada, enviando el enlace del cuestionario a los participantes que cumplan con los criterios de inclusión previamente establecidos. Este método permite recopilar información de forma estandarizada, minimizar sesgos del entrevistador y facilitar la participación voluntaria y anónima de los encuestados, aspectos fundamentales en estudios organizacionales de carácter cuantitativo (Ranganathan & Aggarwal, 2024).

De forma complementaria a la encuesta, se incorporó una revisión documental orientada a fortalecer la evidencia del estudio y contrastar los resultados obtenidos mediante el instrumento aplicado. Esta revisión incluyó fuentes normativas, técnicas e institucionales relacionadas con inteligencia artificial, protección de datos personales, seguridad de la información, innovación financiera y gestión de riesgos tecnológicos. La incorporación de evidencia documental resulta pertinente en estudios de encuesta, debido a que contribuye a mejorar la calidad, credibilidad e interpretación de los resultados obtenidos mediante instrumentos estructurados (Kelley et al., 2003). En este sentido, la revisión documental permitió ampliar el análisis más allá de la percepción de los participantes, vinculando los hallazgos empíricos con referencias aplicables al contexto del sistema financiero hondureño.

Una vez finalizado el proceso de recolección, los datos serán exportados a una hoja de cálculo y posteriormente depurados, verificando la integridad de las respuestas y eliminando registros incompletos o inconsistentes. El procesamiento de los datos incluirá la codificación de las respuestas de la escala Likert, asignando valores numéricos a cada categoría de respuesta para su análisis estadístico. Este procedimiento es consistente con las recomendaciones metodológicas para el tratamiento de datos ordinales en investigaciones sociales y administrativas (Joshi et al., 2015).

La información documental fue analizada mediante revisión de contenido, identificando aspectos relacionados con principios de protección de datos, gobernanza algorítmica, controles de seguridad, transparencia, gestión de incidentes y supervisión institucional. Esta técnica permitió utilizar los documentos revisados como insumo complementario para interpretar los hallazgos de la encuesta, fortalecer la discusión de resultados y sustentar la matriz de riesgos identificados. Además, dado que el estudio es de corte transversal, la revisión documental contribuyó a contextualizar la situación observada en un momento específico, sin asumir relaciones causales directas entre las variables analizadas (Sedgwick, 2014).

El análisis de datos se realizará mediante técnicas de estadística descriptiva y correlacional. En la fase descriptiva se emplearán frecuencias, porcentajes, medias y desviaciones estándar para caracterizar el comportamiento de las variables y sus dimensiones. Posteriormente, se aplicarán análisis correlacionales con el objetivo de identificar la relación entre el nivel de adopción de soluciones de inteligencia artificial y el nivel de protección de datos personales. Para garantizar la calidad del instrumento, se evaluará la confiabilidad interna a través del coeficiente alfa de Cronbach, técnica ampliamente utilizada para medir la

consistencia interna de instrumentos tipo Likert (Boone & Boone, 2012; Carmines & Zeller, 1979). Estas técnicas permitirán obtener resultados objetivos y coherentes con el enfoque cuantitativo del estudio.

3.11 FUENTES DE INFORMACIÓN

Las fuentes de información primarias de la presente investigación están constituidas por los datos obtenidos directamente de personas, mediante la aplicación de encuestas estructuradas. Los participantes son profesionales que laboran en instituciones del sistema financiero hondureño y que desempeñan funciones relacionadas con tecnología, seguridad de la información, gestión de datos, riesgos y cumplimiento. El uso de encuestas como fuente primaria permite recolectar información original, específica y contextualizada, lo cual es fundamental en investigaciones empíricas de enfoque cuantitativo (Kelley et al., 2003).

La encuesta se utiliza como fuente primaria debido a su capacidad para recopilar datos estandarizados de manera sistemática, facilitando la medición de percepciones y prácticas organizacionales. Este método resulta especialmente adecuado para estudios descriptivos y correlacionales, ya que permite analizar relaciones entre variables a partir de respuestas obtenidas directamente de los sujetos de estudio, sin intervención del investigador durante la recolección de datos (Sedgwick, 2014).

En este estudio, las respuestas obtenidas mediante la encuesta constituyen la fuente primaria principal de información y representan la base empírica del análisis estadístico. Los datos recolectados permiten identificar patrones y relaciones entre la adopción de soluciones de inteligencia artificial y la protección de datos personales, asegurando coherencia entre el diseño metodológico y los objetivos de la investigación (Groves, 2006).

De forma complementaria, se utilizaron fuentes documentales, tales como lineamientos técnicos, documentos regulatorios, literatura académica y estándares internacionales relacionados con inteligencia artificial, protección de datos y gestión de riesgos tecnológicos. Estas fuentes permitieron contextualizar los resultados obtenidos mediante la encuesta y fortalecer el análisis documental del estudio.

3.12 ÉTICA EN LA INVESTIGACIÓN

La presente investigación se desarrollará en estricto apego a los principios éticos que rigen los estudios con participación de personas como fuente de información. En primer término, se garantizará el consentimiento informado de todos los participantes. Previo a la aplicación del cuestionario, se les proporcionará una explicación clara sobre los objetivos del estudio, el carácter estrictamente académico de los resultados, la naturaleza voluntaria de su participación y la posibilidad de retirarse en cualquier momento sin consecuencia alguna. Solo se incorporarán al estudio aquellos sujetos que manifiesten su conformidad de manera expresa.

En segundo lugar, se asegurará la confidencialidad de la información recolectada. El instrumento de medición no incluirá nombres ni datos que permitan la identificación directa de los participantes o de las instituciones; los resultados se presentarán de forma agregada y exclusivamente con fines analíticos. Los registros serán resguardados en soportes protegidos mediante controles de acceso y no serán compartidos con terceros ajenos al equipo investigador.

Asimismo, el estudio se regirá por los principios de honestidad e imparcialidad. La honestidad se reflejará en el registro fidedigno de los datos, en la aplicación responsable de las técnicas de análisis y en la comunicación transparente de los hallazgos, evitando cualquier forma de manipulación, ocultamiento o tergiversación de la información. La imparcialidad implicará valorar los datos con objetividad, sin prejuicios ni favoritismos hacia personas o instituciones, y reconociendo expresamente las limitaciones metodológicas del estudio. En conjunto, estas consideraciones tienen por finalidad salvaguardar la dignidad de los participantes, preservar la confianza en el proceso investigativo y garantizar la integridad científica del trabajo.

3.13 LIMITACIONES DEL ESTUDIO

Las limitaciones del estudio se derivan, en primer término, del diseño no experimental de corte transversal. Al efectuarse la recolección de datos en un único momento, los resultados permiten identificar asociaciones entre el nivel de adopción de soluciones de inteligencia artificial y el nivel de protección de datos personales, pero no posibilitan establecer relaciones de causalidad ni analizar la evolución temporal de dichas variables. En consecuencia, los hallazgos deben interpretarse como una fotografía del estado actual y no como evidencia de efectos causales directos.

En segundo lugar, la investigación emplea un muestreo no probabilístico por conveniencia, dirigido a profesionales que cumplen criterios específicos dentro de instituciones del sistema financiero. Aunque esta estrategia facilita el acceso a informantes clave y es coherente con el carácter exploratorio–aplicado del estudio, restringe la posibilidad de generalizar los resultados a la totalidad de la población, dado que la muestra no es estadísticamente representativa del sistema financiero hondureño en su conjunto.

Adicionalmente, el uso de un cuestionario estructurado autoadministrado, aplicado en formatos físico y digital, puede incorporar sesgos propios de la autopercepción y la deseabilidad social, en la medida en que algunos participantes tiendan a ofrecer respuestas más favorables respecto a las prácticas de su institución. A ello se suma la eventual presencia de cuestionarios incompletos o con patrones de respuesta poco consistentes, que requieren ser depurados en la fase de análisis.

Finalmente, la naturaleza sensible de la temática en particular, los mecanismos internos de seguridad de la información y protección de datos puede estar sujeta a restricciones de divulgación institucional, lo que limita el acceso a ciertos documentos o detalles operativos. Estas condiciones deben considerarse al interpretar los resultados y formular recomendaciones, reconociendo que el estudio ofrece una aproximación válida, pero acotada, a la realidad investigada.

CAPÍTULO IV. RESULTADOS Y ANÁLISIS

El presente capítulo expone los resultados obtenidos a partir de la aplicación del instrumento de recolección de datos y de la revisión documental complementaria. Su propósito es presentar los hallazgos relacionados con el nivel de adopción de soluciones de inteligencia artificial, el nivel de protección de datos personales asociado a su uso y la relación estadística entre ambas variables, conforme a los objetivos específicos de la investigación.

4.1 PRESENTACIÓN DE RESULTADOS

Los resultados se presentan de acuerdo con los objetivos específicos de la investigación y las variables definidas en el marco metodológico. En primer lugar, se describen los hallazgos relacionados con el nivel de adopción de soluciones de inteligencia artificial. En segundo lugar, se analizan los resultados vinculados con el nivel de protección de datos personales en el uso de dichas soluciones. Finalmente, se expone la prueba estadística utilizada para determinar la relación entre ambas variables, conforme al enfoque cuantitativo y correlacional del estudio.

Figura 6. Edad de los participantes
Fuente: Microsoft 365 Forms

La mayoría de los participantes se concentra en los rangos de 36–45 y 46–55 años (37% cada uno), lo que indica una muestra compuesta principalmente por profesionales con experiencia.

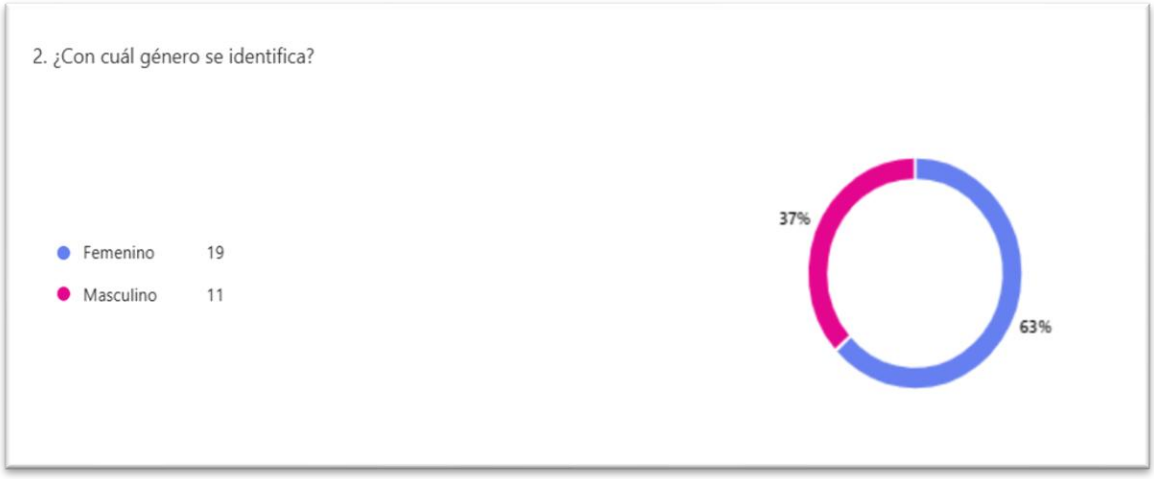


Figura 7. Género de los participantes
Fuente: *Microsoft 365 Forms*

Los resultados indican que el 63% de los participantes se identifica como femenino y el 37% como masculino, evidenciando una mayor representación femenina en la muestra analizada.

Además de la caracterización demográfica de los participantes, se incorpora el mapeo de roles funcionales, con el propósito de complementar la descripción de la muestra desde una perspectiva organizacional. Mientras las figuras de edad y género permiten conocer rasgos generales de los encuestados, la identificación de los roles permite establecer su vinculación con áreas relacionadas con tecnología, seguridad de la información, riesgos, cumplimiento normativo y gestión de datos. Esta información fortalece la pertinencia de las respuestas obtenidas antes de presentar los resultados específicos sobre adopción de inteligencia artificial y protección de datos personales.

Tabla 5. Caracterización funcional de los participantes del estudio

Rol o área funcional participante	Relación con las variables del estudio	Información que aporta al análisis
Tecnología de la Información	Se relaciona con la variable de adopción de soluciones de IA.	Aporta información sobre implementación tecnológica, integración con sistemas centrales, operación de soluciones de IA y controles técnicos.
Seguridad de la Información	Se relaciona con la variable de protección de datos personales.	Aporta información sobre controles de acceso, autenticación, cifrado, auditoría, monitoreo y gestión de incidentes.
Gestión de Datos / Analítica de Datos	Se relaciona con ambas variables, especialmente con el uso y tratamiento de datos en sistemas de IA.	Aporta información sobre minimización, calidad, finalidad, trazabilidad y tratamiento automatizado de datos personales.
Riesgo Operativo / Gestión de Riesgos	Se relaciona con la identificación de riesgos derivados del uso de IA y del tratamiento de datos personales.	Aporta información sobre riesgos tecnológicos, impacto, probabilidad, controles existentes y madurez institucional.
Canales Digitales / Transformación Digital	Se relaciona con el uso de IA en servicios digitales y atención al cliente.	Aporta información sobre automatización de servicios, experiencia del usuario, transparencia y uso de IA en canales digitales.
Cumplimiento Normativo	Se relaciona con los principios de protección de datos personales y responsabilidad institucional.	Aporta información sobre licitud, finalidad del tratamiento, avisos de privacidad, derechos del titular y cumplimiento interno.

Fuente: Elaboración propia con base en la caracterización de la población y unidad de análisis del estudio.

La caracterización funcional evidencia que los participantes se encuentran relacionados con áreas clave para el análisis de la adopción de inteligencia artificial y la protección de datos personales. Esta composición fortalece la pertinencia de la información recolectada, ya que las respuestas provienen de perfiles vinculados con procesos tecnológicos, normativos, operativos y de control dentro de las instituciones financieras.

4.1.1 NIVEL DE ADOPCIÓN DE SOLUCIONES DE IA

Esta sección responde al primer objetivo específico de la investigación, orientado a describir el nivel de adopción de soluciones de inteligencia artificial en instituciones del sistema financiero hondureño. Para ello, se analizan los resultados relacionados con el uso de IA en procesos clave, la madurez de implementación y los mecanismos de gobernanza institucional identificados mediante el instrumento aplicado.

Figura 8. Impacto de la IA en la eficiencia operativa

Fuente: Microsoft 365 Forms

La figura evidencia una percepción principalmente positiva. Se observa una mayor concentración en el nivel 4, lo que sugiere que los participantes consideran que la inteligencia artificial contribuye de forma positiva a la eficiencia operativa.

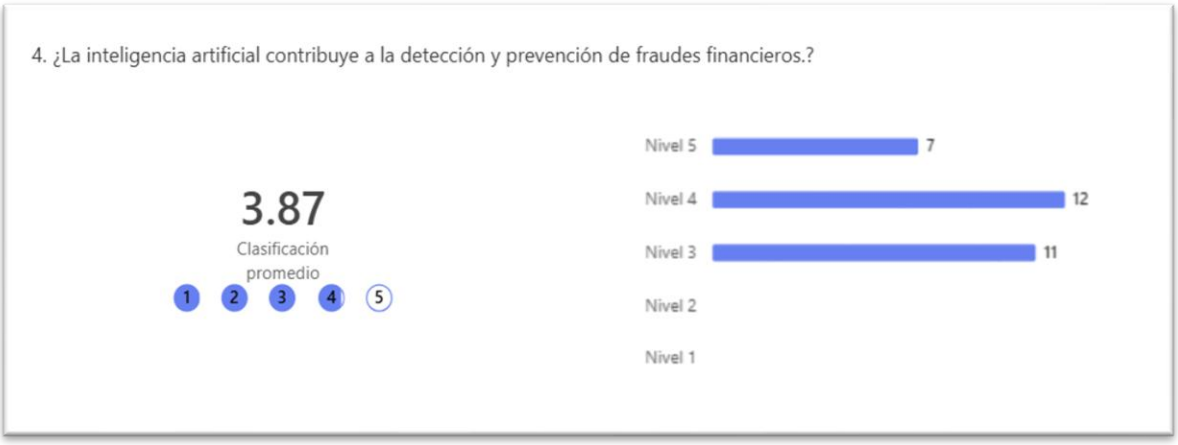


Figura 9. IA en detección de fraude

Fuente: Microsoft 365 Forms

La figura muestra una apreciación en general positiva sobre el aporte de la inteligencia artificial en la detección y prevención de fraudes financieros. Las respuestas se agrupan sobre todo en los niveles 4 y 3, lo que indica una inclinación hacia el acuerdo, junto con una presencia significativa de opiniones sin definición clara.

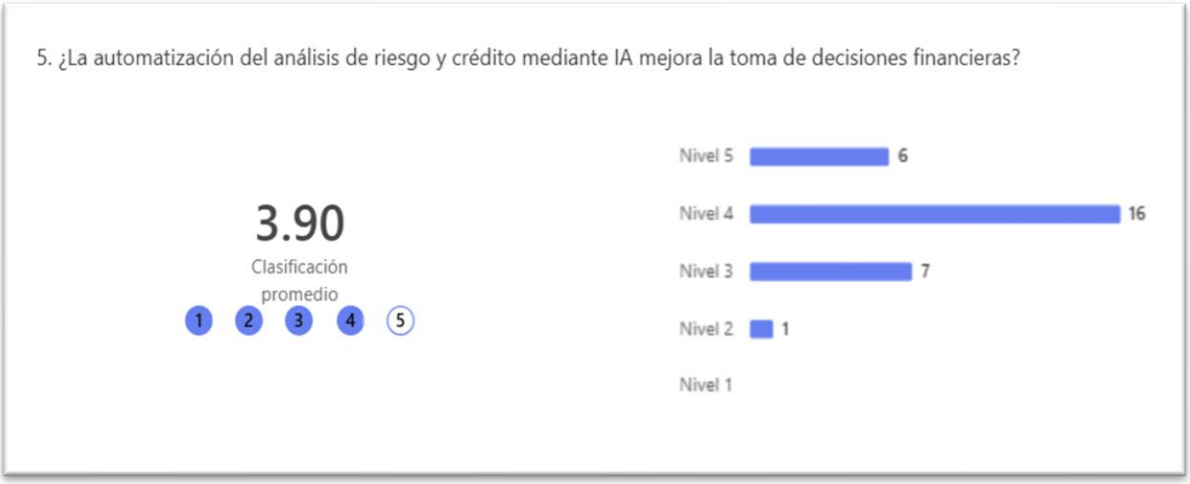


Figura 10. IA en análisis de riesgo y crédito

Fuente: Microsoft 365 Forms

La figura evidencia una percepción positiva sobre la automatización del análisis de riesgo y crédito mediante inteligencia artificial. La mayoría de los participantes seleccionó el nivel 4, lo que indica que consideran que la IA mejora la toma de decisiones financieras

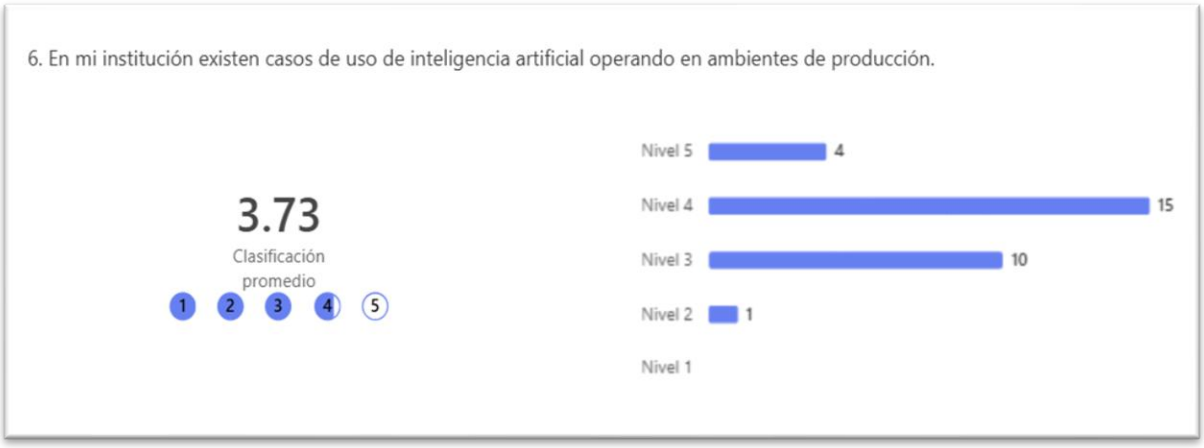


Figura 11. Casos de uso de IA en producción

Fuente: Microsoft 365 Forms

La figura muestra que en las instituciones participantes existen casos de uso de inteligencia artificial operando en ambientes de producción. En ella resalta principalmente el nivel 4, lo que indica una implementación moderadamente consolidada de estas soluciones en el entorno operativo.

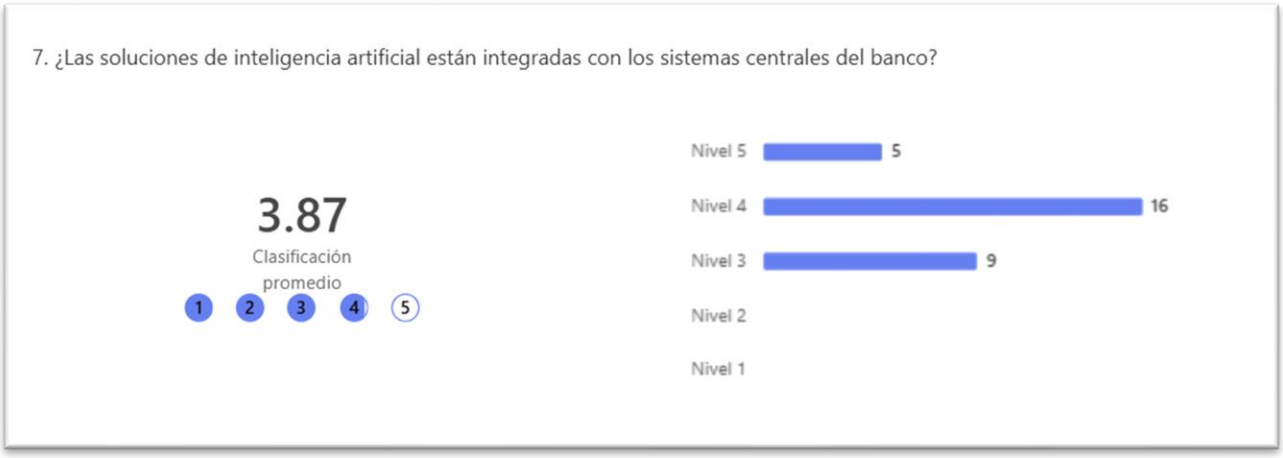


Figura 12. Integración de IA con sistemas centrales

Fuente: Microsoft 365 Forms

La figura indica que las soluciones de inteligencia artificial presentan un nivel favorable de integración con los sistemas centrales del banco. Predomina el nivel 4, lo que sugiere una integración de moderada a alta en las instituciones evaluadas.

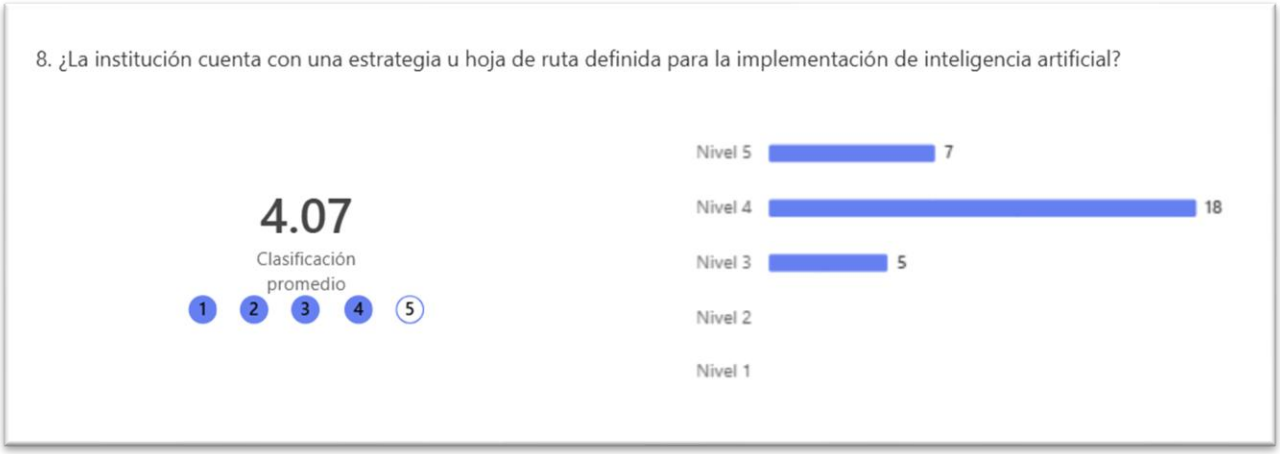


Figura 13. Estrategia institucional de IA

Fuente: Microsoft 365 Forms

La figura muestra que la mayoría de las instituciones cuenta con una estrategia u hoja de ruta definida para la implementación de inteligencia artificial. Registra la mayor frecuencia el nivel 4, lo que indica una planificación estratégica consolidada en la mayoría de los casos.

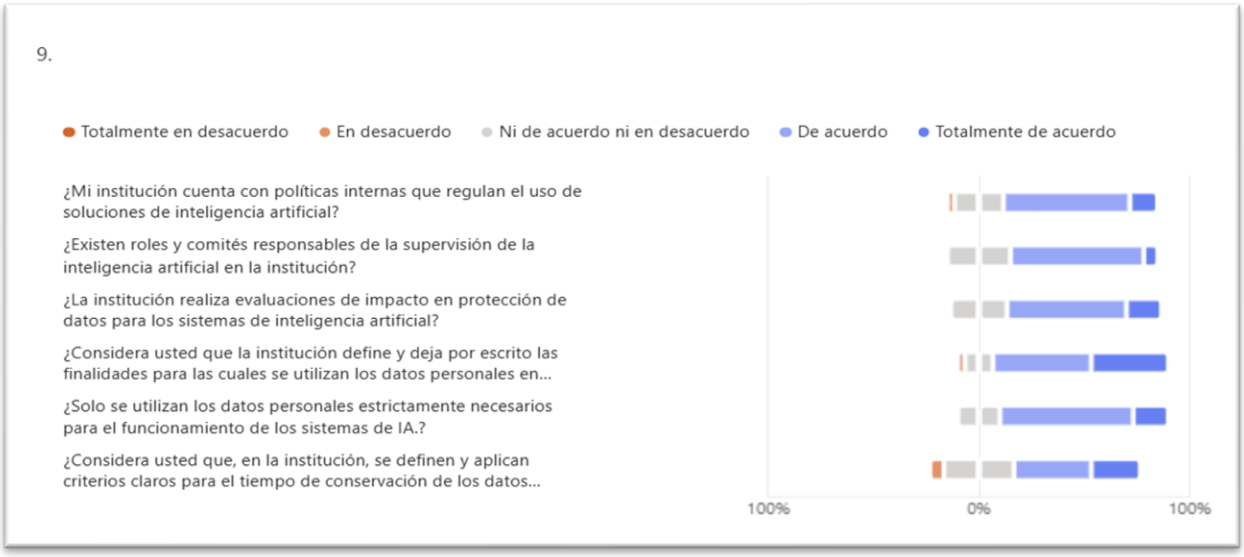
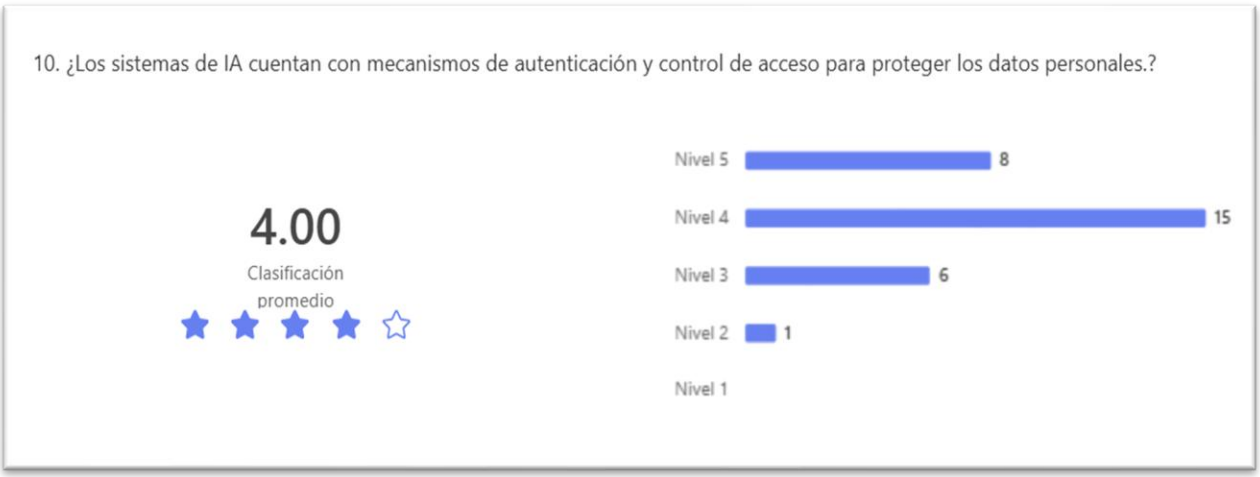


Figura 14. Gobernanza y protección de datos en IA
Fuente: Microsoft 365 Forms

La figura muestra una tendencia mayoritaria hacia las categorías “De acuerdo” y “Totalmente de acuerdo” en relación con la existencia de políticas internas, comités de supervisión, evaluaciones de impacto y criterios de uso y conservación de datos en soluciones de inteligencia artificial. No obstante, se observan respuestas neutrales y algunos desacuerdos, lo que evidencia áreas de mejora en la formalización y aplicación de mecanismos de gobernanza



y protección de datos dentro de las instituciones evaluadas.

Figura 15. *Controles de acceso en sistemas de IA*
Fuente: *Microsoft 365 Forms*

La figura sugiere que los sistemas de inteligencia artificial, en general, disponen de mecanismos de autenticación y control de acceso. El nivel 4 concentra la mayor parte de las respuestas, esto refleja una percepción favorable sobre la protección de datos personales a través de controles técnicos de seguridad.

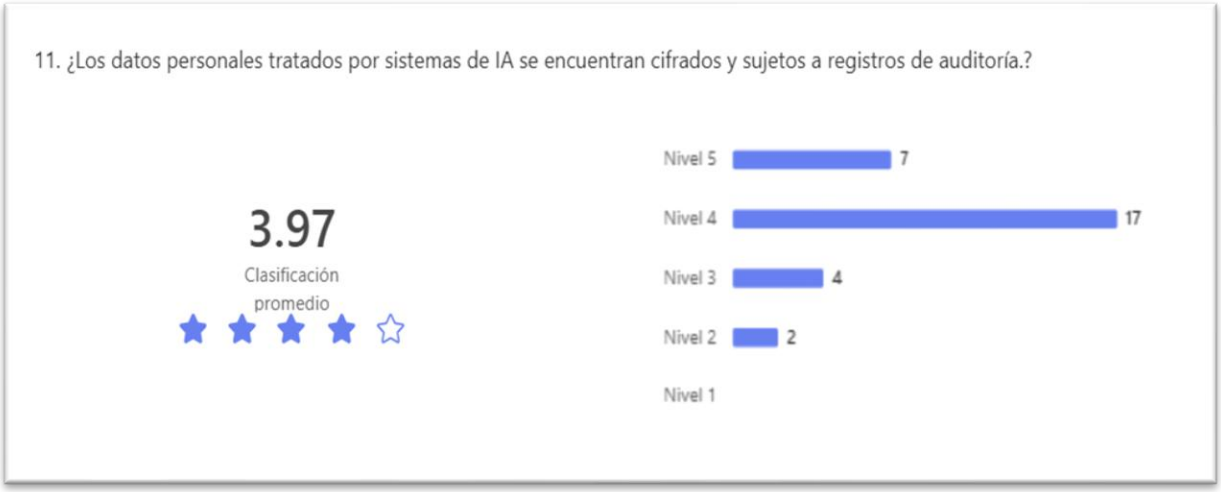


Figura 16. Cifrado y auditoría en sistemas de IA
Fuente: Microsoft 365 Forms

La figura refleja que, en las instituciones participantes, el tratamiento de datos personales mediante sistemas de inteligencia artificial incorpora prácticas como el cifrado y el registro de auditoría. Se observa una mayor concentración en el nivel 4, evidenciando una apreciación positiva sobre el grado de control, seguridad y seguimiento aplicado.

4.1.2 NIVEL DE PROTECCIÓN DE DATOS PERSONALES EN EL USO DE IA

Esta sección responde al segundo objetivo específico de la investigación, orientado a determinar el nivel de protección de datos personales asociado al uso de soluciones de inteligencia artificial. El análisis considera aspectos relacionados con principios de protección de datos, medidas de seguridad, controles técnicos, transparencia institucional y mecanismos para el ejercicio de derechos de los titulares.

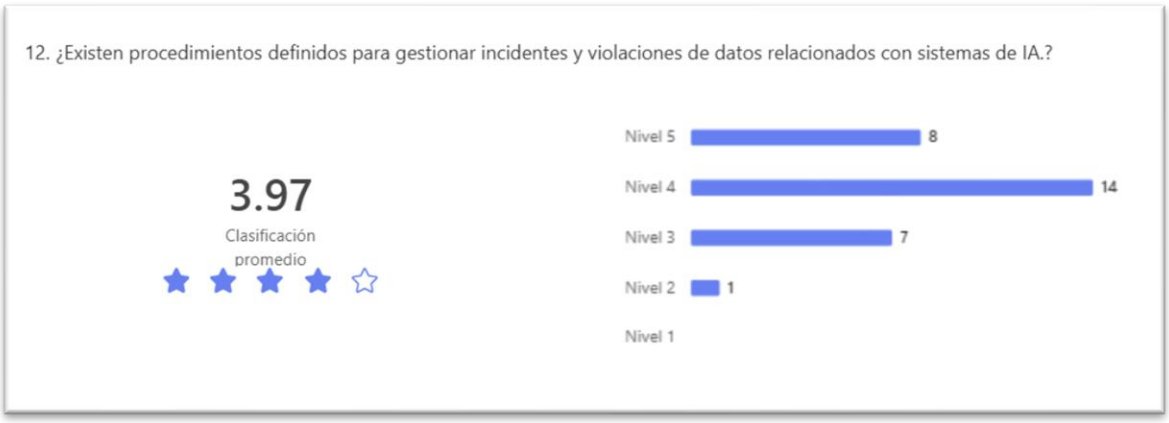


Figura 17. *Gestión de incidentes en sistemas de IA*
Fuente: *Microsoft 365 Forms*

La figura muestra que las instituciones participantes han definido procesos para la atención de incidentes y eventos de violación de datos asociados a sistemas de inteligencia artificial. La mayor concentración de respuestas se ubica en el nivel 4, esto sugiere una apreciación positiva sobre la capacidad institucional para responder de manera estructurada ante este tipo de situaciones.

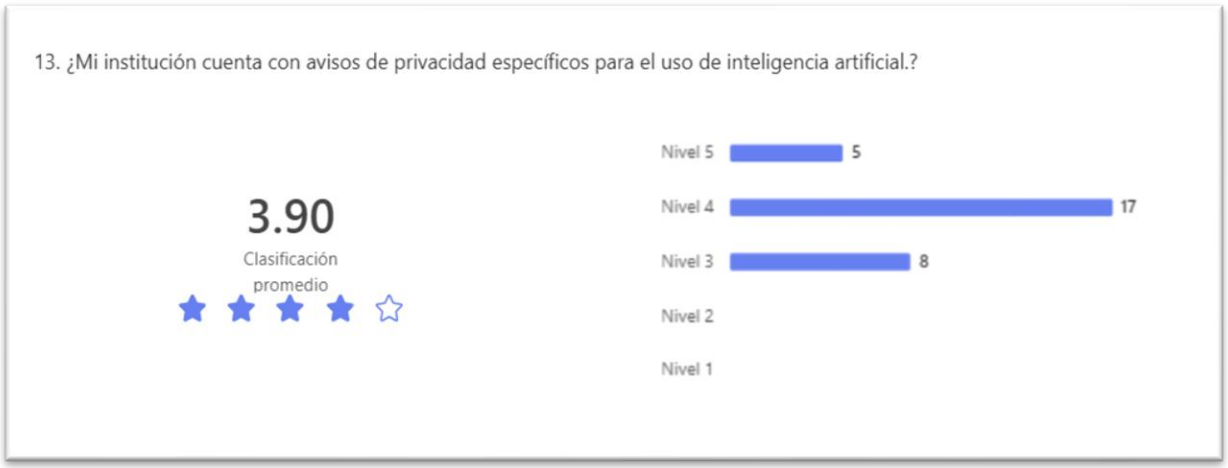


Figura 18. *Avisos de privacidad para IA*
Fuente: *Microsoft 365 Forms*

La figura muestra que la mayoría de las instituciones cuenta con avisos de privacidad específicos para el uso de inteligencia artificial. Destaca el nivel 4, indicando una percepción satisfactoria respecto a la formalización de mecanismos de transparencia informativa.

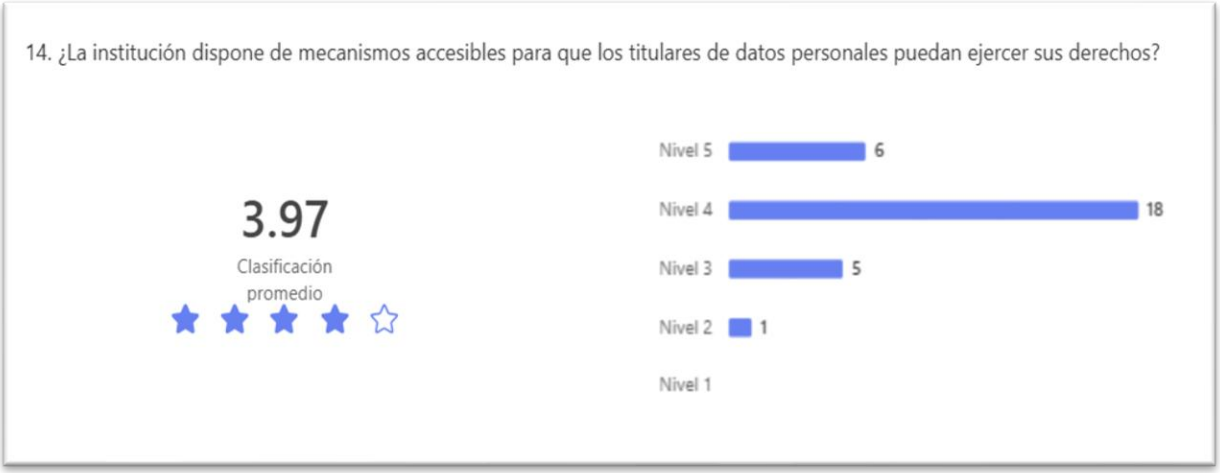


Figura 19. *Mecanismos para ejercicio de derechos*
Fuente: *Microsoft 365 Forms*

La figura indica que las instituciones disponen, en su mayoría, de mecanismos accesibles para que los titulares de datos personales puedan ejercer sus derechos. Predomina el nivel 4, lo cual refleja una percepción positiva sobre la garantía de derechos en el contexto del uso de inteligencia artificial.

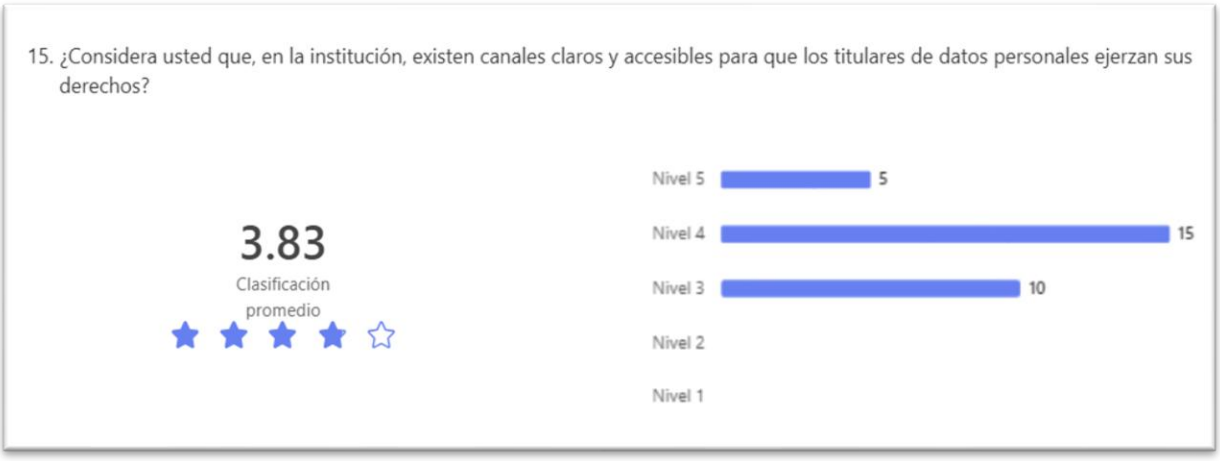


Figura 20. *Canales para ejercicio de derechos*
Fuente: *Microsoft 365 Forms*

La figura muestra que las instituciones cuentan mayoritariamente con canales claros y accesibles para que los titulares ejerzan sus derechos. Aunque predomina el nivel 4, se observan

valoraciones en nivel 3, lo que sugiere oportunidades de mejora en la claridad y accesibilidad de dichos canales.

4.1.3 EVIDENCIA DOCUMENTAL COMPLEMENTARIA

Con el propósito de fortalecer el análisis de los resultados obtenidos mediante la encuesta, se incorporó una revisión documental complementaria de fuentes técnicas, normativas e institucionales relacionadas con inteligencia artificial, protección de datos personales y gestión de riesgos tecnológicos en el sector financiero. Esta revisión permitió contrastar las percepciones de los participantes con documentos de referencia, evitando que la interpretación de los hallazgos se sustentara únicamente en opiniones individuales. En estudios basados en encuestas, la calidad de la evidencia mejora cuando los resultados son interpretados junto con fuentes documentales pertinentes y criterios metodológicos claros (Kelley et al., 2003; Groves, 2006).

La evidencia documental revisada no constituye una auditoría técnica de los sistemas internos de las instituciones participantes, sino un insumo de análisis que permite contextualizar los resultados y relacionarlos con buenas prácticas, principios internacionales y lineamientos aplicables al entorno financiero hondureño. En particular, la literatura sobre decisiones automatizadas advierte que los sistemas algorítmicos requieren mecanismos de transparencia, trazabilidad y rendición de cuentas para reducir riesgos de opacidad, sesgo o afectación de derechos (Diakopoulos, 2016; Wachter et al., 2017; Zarsky, 2016).

Tabla 6. Evidencia documental complementaria revisada

Documento o fuente revisada	Aspecto evaluado	Relación con la investigación	Hallazgo documental
Documentos FinTech de la Comisión Nacional de Bancos y Seguros	Innovación financiera, supervisión y gestión de riesgos tecnológicos	Contextualiza el avance de soluciones tecnológicas en el sistema financiero hondureño	Evidencia la importancia de fortalecer lineamientos de supervisión, transparencia, control y gestión de riesgos asociados a la innovación financiera.
Hub de Innovación Financiera de Honduras / CNBS	Desarrollo de innovación financiera y acompañamiento regulatorio	Permite contextualizar la adopción de tecnologías emergentes en instituciones financieras	Refuerza la necesidad de identificar barreras regulatorias, monitorear innovaciones financieras y evaluar sus beneficios y riesgos potenciales.
Barreras Regulatorias en la Industria de Tecno-Finanzas en Honduras / BCH, CNBS y ACDI/VOCA	Vacíos regulatorios, innovación financiera y protección del usuario	Sustenta la necesidad de analizar el contexto hondureño en materia de tecnología financiera y protección de datos	Identifica desafíos regulatorios e institucionales relacionados con servicios financieros digitales, uso de información y protección del usuario financiero.
BIS — *Regulating AI in the Financial Sector*	Gobernanza, supervisión, riesgos y explicabilidad de la IA en finanzas	Respalda la necesidad de controles específicos para soluciones de IA en entidades financieras	Señala que el uso de IA en el sector financiero requiere mecanismos de gobernanza, monitoreo, gestión de riesgos, explicabilidad y supervisión institucional.
OECD Privacy Guidelines	Principios internacionales de protección de datos personales	Sirve como referencia para evaluar finalidad, minimización, seguridad, transparencia y responsabilidad	Establece principios orientadores para el tratamiento adecuado de datos personales y la protección de los derechos de los titulares.
ISO/IEC 27001	Seguridad de la información y controles organizativos	Respalda la importancia de controles técnicos y administrativos para proteger datos personales	Refuerza la necesidad de controles de acceso, gestión de incidentes, auditoría, confidencialidad, integridad y disponibilidad de la información.
Reglamento General de Protección de Datos de la Unión Europea	Tratamiento de datos personales, derechos del titular y decisiones automatizadas	Sirve como referencia comparada para analizar riesgos asociados al tratamiento automatizado de datos	Destaca la importancia de la licitud, transparencia, derechos del titular, evaluación de impacto y control sobre decisiones automatizadas.
Literatura indexada sobre transparencia y rendición de cuentas algorítmica	Explicabilidad, supervisión y control de decisiones automatizadas	Permite fortalecer el análisis teórico y documental sobre IA y protección de datos	Advierte que los sistemas algorítmicos pueden generar riesgos de opacidad, sesgo y falta de rendición de cuentas si no existen controles institucionales adecuados.

Fuente: Elaboración propia con base en la revisión documental complementaria.

La revisión documental complementaria evidencia que los principales temas identificados mediante la encuesta también se encuentran presentes en fuentes técnicas, normativas y académicas relacionadas con inteligencia artificial, protección de datos y gestión de riesgos financieros. En particular, los documentos revisados destacan la importancia de fortalecer la gobernanza, la transparencia, los controles de seguridad, las evaluaciones de impacto y la supervisión del tratamiento automatizado de datos personales. Estos aspectos coinciden con la literatura especializada, la cual sostiene que la adopción de IA requiere controles organizacionales, técnicos y éticos que permitan gestionar riesgos de privacidad, sesgo y opacidad (Cath et al., 2018; Dwivedi et al., 2021; Wachter et al., 2017).

En este sentido, los resultados obtenidos no se interpretan únicamente como percepciones de los participantes, sino como hallazgos que pueden contrastarse con referencias documentales que respaldan la necesidad de fortalecer la protección de datos personales en soluciones de inteligencia artificial dentro del sistema financiero hondureño. Esta aclaración resulta relevante porque el propio diseño del estudio se fundamenta en información recolectada mediante encuesta y no en auditorías técnicas independientes, por lo que la revisión documental cumple una función de contraste, contextualización y fortalecimiento analítico.

4.1.4 CONFIABILIDAD DEL INSTRUMENTO (ALFA DE CRONBACH)

En este apartado se presentan las estadísticas de fiabilidad del instrumento, con el fin de evaluar la consistencia interna de los ítems aplicados en el estudio.

Tabla 7. Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
0.955	20

La tabla muestra un Alfa de Cronbach de 0.955 para un total de 20 ítems, lo que indica un nivel de consistencia interna excelente. Este resultado evidencia que los elementos del instrumento presentan alta coherencia entre sí y miden de forma uniforme el constructo evaluado.

4.1.5 ESTADÍSTICA DESCRIPTIVA DE LAS VARIABLES

Se presenta el análisis descriptivo de los resultados obtenidos, donde se detallan los estadísticos principales para cada indicador evaluado. Esta información permite observar las tendencias y el nivel de consenso entre los participantes respecto a la adopción tecnológica. Las siguientes tablas resumen estos valores fundamentales para comprender el comportamiento de las variables en la institución.

Tabla 8. Nivel de adopción de soluciones de IA

3. ¿Cómo considera usted el impacto de la atención a la cliente apoyada en inteligencia artificial sobre la eficiencia operativa de los servicios financieros en la institución?	4. ¿La inteligencia artificial contribuye de manera efectiva a la detección y prevención de fraudes financieros en la institución?	5. ¿La automatización del análisis de riesgo y crédito mediante inteligencia artificial mejora la toma de decisiones financieras en la institución?	6. ¿Las soluciones de inteligencia artificial están adecuadamente integradas con los sistemas centrales de la institución?	7. ¿La institución cuenta con políticas internas formales que regulan el uso de soluciones de inteligencia artificial?	8. ¿La institución dispone de una estrategia o hoja de ruta claramente definida para la implementación de inteligencia artificial?	9. ¿Existen roles y comités formalmente establecidos para la supervisión del uso de la inteligencia artificial en la institución?	10. ¿La institución cuenta con procesos definidos para la identificación y gestión de riesgos asociados al uso de inteligencia artificial?	11. ¿La institución realiza evaluaciones de impacto antes de implementar sistemas de inteligencia artificial?
30	30	30	30	30	30	30	30	30
0	0	0	0	0	0	0	0	0
4.00	4.00	4.00	4.00	4.00	4.00	4.00	4.00	4.00
De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo
-0.548	0.242	-0.335	-0.067	0.170	-0.054	-0.409	-0.013	0.107
0.427	0.427	0.427	0.427	0.427	0.427	0.427	0.427	0.427
0.830	-1.261	0.041	-0.178	-0.715	-0.352	0.591	-0.168	-0.557
0.833	0.833	0.833	0.833	0.833	0.833	0.833	0.833	0.833

En relación con la variable Nivel de adopción de soluciones de inteligencia artificial (IA), los resultados evidencian una percepción alta y homogénea dentro de la institución. La media de 4.00 en todos los ítems indica acuerdo general respecto a la implementación de IA en

procesos clave como atención al cliente, detección y prevención de fraudes, análisis de riesgo y crédito, integración con sistemas centrales y existencia de políticas, estrategias y mecanismos de supervisión. La baja desviación estándar (0.427) sugiere consenso organizacional, lo que puede interpretarse como un nivel avanzado de madurez digital y de gobernanza tecnológica.

Desde una perspectiva analítica, la adopción observada no se limita al uso operativo de herramientas de IA, sino que incluye dimensiones estructurales como marcos normativos internos, comités formales y evaluaciones de impacto. Esto coincide con el enfoque de adopción integral propuesto en la literatura, donde la implementación efectiva de IA requiere alineación estratégica, gestión de riesgos y supervisión continua (Dwivedi et al., 2021).

En comparación con estudios publicados en revistas indexadas, los hallazgos son consistentes con investigaciones que señalan que el sector financiero lidera la adopción de IA debido a su necesidad de optimizar eficiencia operativa y fortalecer la gestión del riesgo (Ashta & Herrmann, 2021; Ryll et al., 2020). Asimismo, estudios recientes destacan que la automatización del análisis crediticio y la detección de fraude constituyen áreas prioritarias de implementación (Gomber et al., 2018). No obstante, parte de la literatura advierte que muchas organizaciones enfrentan desafíos en integración tecnológica y en la consolidación de marcos éticos y de gobernanza. A diferencia de esos contextos, los resultados de este estudio reflejan una percepción interna uniforme y positiva, lo que podría indicar un mayor nivel de formalización institucional o, alternativamente, una posible sobreestimación perceptual.

Entre las limitaciones del estudio se encuentra el tamaño de la muestra (n = 30), lo que restringe la generalización de los resultados. Además, los datos son de naturaleza perceptual y no se contrastan con indicadores objetivos de desempeño, auditorías técnicas o métricas de impacto financiero. Sin embargo, el principal aporte radica en proporcionar evidencia empírica sobre el nivel de adopción de soluciones de IA desde una perspectiva organizacional interna, contribuyendo a la literatura sobre transformación digital y gobernanza tecnológica en el sector financiero.

Tabla 9. Nivel de protección de datos personales en el uso de IA

12. ¿Considera usted que la institución define y deja por escrito las finalidades para las cuales se utilizan los datos personales en sistemas de inteligencia artificial?	13. ¿Solo se utilizan los datos personales estrictamente necesarios para el funcionamiento de los sistemas de inteligencia artificial?	14. ¿Considera usted que, en la institución, se definen y aplican criterios claros para el tiempo de conservación de los datos personales utilizados por sistemas de inteligencia artificial?	15. ¿Los sistemas de inteligencia artificial cuentan con mecanismos adecuados de autenticación y control de acceso para proteger los datos personales?	16. ¿Los datos personales tratados por sistemas de inteligencia artificial se encuentran cifrados y sujetos a registros de auditoría?	17. ¿Existen procedimientos formalmente definidos para la gestión de incidentes y violaciones de datos relacionados con sistemas de inteligencia artificial?	18. ¿La institución comunica a los clientes información sobre el uso de inteligencia artificial en el tratamiento de sus datos personales?	19. ¿La institución dispone de mecanismos accesibles para que los titulares de datos personales puedan ejercer sus derechos?	20. ¿Considera usted que, en la institución, existen canales claros y accesibles para que los titulares de datos personales ejerzan sus derechos?
30	30	30	30	30	30	30	30	30
0	0	0	0	0	0	0	0	0
4.00	4.00	4.00	4.00	4.00	4.00	4.00	4.00	4.00
De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo
-0.762	0.016	-0.116	-0.453	-0.776	-0.356	0.107	-0.548	0.240
0.427	0.427	0.427	0.427	0.427	0.427	0.427	0.427	0.427
0.421	-0.092	-0.778	-0.034	0.768	-0.343	-0.557	0.830	-0.831
0.833	0.833	0.833	0.833	0.833	0.833	0.833	0.833	0.833

En relación con la variable Nivel de protección de datos personales en el uso de inteligencia artificial (IA), los resultados evidencian una percepción alta y homogénea dentro de la institución. La media de 4.00 en todos los ítems indica acuerdo general respecto a la existencia de finalidades definidas por escrito, aplicación del principio de minimización de datos, criterios de conservación, mecanismos de autenticación y control de acceso, cifrado, auditoría, gestión de incidentes y garantía de los derechos de los titulares. La baja desviación estándar (0.427) sugiere consenso organizacional, lo que puede interpretarse como un nivel consolidado de formalización en materia de protección de datos vinculada al uso de IA.

Desde una perspectiva analítica, los resultados indican que la institución no solo implementa soluciones tecnológicas, sino que también integra dimensiones normativas y organizativas en su gobernanza digital. Este enfoque integral coincide con el principio de privacy by design, que plantea la incorporación de salvaguardas de protección de datos desde

la fase de diseño y desarrollo de los sistemas de IA (Cath et al., 2018). Asimismo, la presencia percibida de procedimientos formales y mecanismos de auditoría sugiere alineación con estándares internacionales de gestión de riesgos tecnológicos y cumplimiento regulatorio.

En comparación con estudios publicados en revistas indexadas, los hallazgos son consistentes con investigaciones que señalan que el sector financiero tiende a fortalecer sus marcos de protección de datos debido a la alta sensibilidad de la información tratada y a las exigencias regulatorias (Dwivedi et al., 2021; Gomber et al., 2018). Sin embargo, parte de la literatura advierte que, en muchas organizaciones, la implementación práctica de principios como minimización de datos, transparencia y rendición de cuentas aún presenta brechas significativas. A diferencia de esos contextos, los resultados obtenidos reflejan una percepción interna ampliamente favorable, lo que podría indicar un mayor grado de madurez institucional o, alternativamente, una evaluación basada principalmente en percepciones y no en auditorías técnicas independientes.

Entre las limitaciones del estudio se encuentra el tamaño de la muestra (n = 30), lo cual restringe la generalización de los resultados. Además, los datos son de naturaleza subjetiva y no se contrastan con evidencia documental, evaluaciones externas o indicadores técnicos de cumplimiento. No obstante, el estudio aporta evidencia empírica relevante sobre el nivel de protección de datos personales en el uso de IA desde una perspectiva organizacional, contribuyendo al análisis académico de la gobernanza digital y la gestión responsable de tecnologías emergentes en el sector financiero.

4.2 PRUEBA DE HIPÓTESIS

La prueba de hipótesis responde al tercer objetivo específico de la investigación, el cual busca analizar la relación entre el nivel de adopción de soluciones de inteligencia artificial y el nivel de protección de datos personales en las instituciones participantes del sistema financiero hondureño. Para ello, se aplicó el coeficiente de correlación de Spearman, considerando la naturaleza ordinal de los datos obtenidos mediante escala tipo Likert.

4.2.1 FORMULACIÓN DE HIPÓTESIS

En coherencia con el objetivo general de la investigación, orientado a evaluar la relación entre el nivel de adopción de soluciones de inteligencia artificial y el nivel de protección de

datos personales en instituciones del sistema financiero hondureño, se plantearon las siguientes hipótesis:

- Hipótesis nula (H_0): No existe relación estadísticamente significativa entre el nivel de adopción de soluciones de inteligencia artificial y el nivel de protección de datos personales en el sistema financiero hondureño.
- Hipótesis alternativa (Hi): Existe relación estadísticamente significativa entre el nivel de adopción de soluciones de inteligencia artificial y el nivel de protección de datos personales en el sistema financiero hondureño.

4.2.2 NIVEL DE SIGNIFICANCIA (A = 0.05)

Para la contrastación de las hipótesis se estableció un nivel de significancia de $\alpha = 0.05$, lo que implica aceptar un 5% de probabilidad de cometer error tipo I, es decir, rechazar la hipótesis nula cuando esta sea verdadera.

4.2.3 RESULTADOS DE LA PRUEBA ESTADÍSTICA

Dado que los datos fueron recolectados mediante una escala tipo Likert, se utilizó el coeficiente de correlación de Spearman (ρ) para evaluar la relación entre las variables.

Los resultados obtenidos muestran:

- Coeficiente de correlación $\rho = 0.906$
- Valor de significancia bilateral $p < 0.001$
- Tamaño de muestra $N = 30$

El coeficiente indica una correlación positiva muy fuerte entre el nivel de adopción de soluciones de inteligencia artificial y el nivel de protección de datos personales.

4.2.4 DECISIÓN E INTERPRETACIÓN ESTADÍSTICA

Dado que el valor p obtenido (< 0.001) es menor que el nivel de significancia establecido ($\alpha = 0.05$), se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alternativa (H_1).

En consecuencia, se concluye que existe una relación estadísticamente significativa y positiva entre el nivel de adopción de soluciones de inteligencia artificial y el nivel de protección de datos personales en el sistema financiero hondureño. Esto sugiere que un mayor grado de implementación de soluciones de IA se asocia con un mayor nivel de aplicación de medidas de protección de datos personales dentro de las instituciones analizadas.

4.3 DISCUSIÓN DE RESULTADOS

Los resultados obtenidos en la presente investigación evidencian la existencia de una relación estadísticamente significativa y positiva muy fuerte entre el nivel de adopción de soluciones de inteligencia artificial y el nivel de protección de datos personales en el sistema financiero hondureño ($\rho = 0.906$; $p < 0.001$). Este hallazgo indica que, a medida que las instituciones financieras incrementan la implementación de tecnologías basadas en inteligencia artificial, también tienden a fortalecer sus mecanismos de protección de datos, control institucional y gobernanza tecnológica.

Desde una perspectiva analítica, este resultado sugiere que la transformación digital en el sistema financiero hondureño no se desarrolla de manera aislada respecto a las obligaciones de cumplimiento y gestión de riesgos. Por el contrario, parece existir una articulación entre innovación tecnológica y fortalecimiento de políticas internas, procedimientos formales, controles de acceso y medidas de seguridad vinculadas al tratamiento de datos personales. Esto podría interpretarse como un indicador de madurez organizacional, donde la adopción tecnológica se acompaña de estructuras de control más robustas.

El hallazgo resulta coherente con la literatura internacional que sostiene que la implementación de inteligencia artificial en el sector financiero implica necesariamente la gestión de riesgos asociados a privacidad, seguridad de la información y gobernanza algorítmica. Organismos internacionales han señalado que la inteligencia artificial constituye una tecnología de alto impacto en entornos financieros, por lo que requiere marcos sólidos de supervisión, auditoría y rendición de cuentas. En este sentido, la fuerte correlación observada respalda la idea de que las instituciones que avanzan en innovación tecnológica también fortalecen sus capacidades de gestión del riesgo y cumplimiento normativo.

Asimismo, el principio de “privacidad por diseño” plantea que las salvaguardas de protección de datos deben integrarse desde la concepción y desarrollo de los sistemas

tecnológicos. La correlación encontrada podría interpretarse como evidencia de que, en el contexto analizado, la adopción de soluciones de inteligencia artificial estaría acompañada de medidas como cifrado, control de acceso, gestión de incidentes y definición formal de finalidades para el uso de datos personales. Esto sugiere una integración progresiva de estándares internacionales de protección de datos en las prácticas institucionales.

No obstante, el nivel elevado del coeficiente de correlación ($\rho = 0.906$) también requiere un análisis crítico. Una relación de esta magnitud puede indicar que ambas variables comparten dimensiones estructurales relacionadas con la gobernanza tecnológica, la cultura organizacional y la capacidad institucional para gestionar innovación bajo criterios de control y responsabilidad. En este sentido, es posible que el nivel de adopción de IA y el nivel de protección de datos no sean fenómenos completamente independientes, sino manifestaciones de un constructo más amplio vinculado a la madurez institucional general.

En el contexto hondureño, donde no existe aún una ley integral de protección de datos personales plenamente consolidada y donde la regulación específica sobre inteligencia artificial se encuentra en desarrollo, este resultado adquiere relevancia particular. A pesar de las brechas normativas identificadas en los antecedentes y en la literatura regional, los datos sugieren que las entidades financieras podrían estar adoptando prácticas alineadas con estándares internacionales, ya sea por exigencias de supervisión sectorial, presión reputacional o necesidad de mantener la confianza de los usuarios.

Desde el punto de vista práctico, estos hallazgos implican que la promoción de la adopción responsable de inteligencia artificial puede contribuir simultáneamente al fortalecimiento de la protección de datos personales. Para reguladores y supervisores, la evidencia refuerza la importancia de desarrollar lineamientos específicos que integren innovación tecnológica, gestión de riesgos y transparencia algorítmica. Para las instituciones financieras, el resultado destaca que la inversión en gobernanza tecnológica no solo facilita la adopción de IA, sino que también fortalece la confianza y sostenibilidad institucional.

Sin embargo, es importante reconocer que los resultados se basan en percepciones de los participantes encuestados y no en auditorías técnicas independientes de los sistemas implementados. Por tanto, aunque la correlación observada es estadísticamente significativa y robusta, no implica necesariamente una relación causal ni garantiza que todos los mecanismos de protección de datos cumplan plenamente con estándares internacionales avanzados.

En síntesis, la investigación demuestra que existe una asociación fuerte y significativa entre la adopción de soluciones de inteligencia artificial y la implementación de medidas de protección de datos en el sistema financiero hondureño. Este hallazgo contribuye al análisis académico sobre gobernanza tecnológica en economías emergentes y proporciona evidencia relevante para el diseño de políticas públicas y estrategias institucionales orientadas a una implementación ética, segura y responsable de la inteligencia artificial en el sector financiero.

4.4 MATRIZ DE RIESGOS IDENTIFICADOS EN PROTECCIÓN DE DATOS E INTELIGENCIA ARTIFICIAL

La matriz de riesgos se construye a partir de dos insumos principales: los resultados obtenidos mediante el instrumento aplicado y la revisión documental complementaria desarrollada en el presente capítulo. Los resultados de la encuesta permitieron identificar la percepción de los participantes respecto a la adopción de soluciones de inteligencia artificial y la protección de datos personales, mientras que la evidencia documental permitió contextualizar dichos hallazgos frente a buenas prácticas, principios internacionales y lineamientos técnicos aplicables al sector financiero. Esta integración metodológica permite fortalecer la interpretación de los riesgos, dado que combina evidencia empírica con respaldo documental y académico (Kelley et al., 2003; Diakopoulos, 2016; Zarsky, 2016).

De esta manera, la matriz no se limita únicamente a percepciones de los encuestados, sino que funciona como una herramienta de análisis cualitativo sustentada en evidencia empírica y documental. A partir de esta integración, se identifican riesgos asociados con gobernanza algorítmica, transparencia, minimización de datos, evaluaciones de impacto, seguridad de la información y ejercicio de derechos de los titulares.

Tabla 10. Matriz de riesgos identificados

N.º	Riesgo identificado	Relación con el instrumento aplicado	Causa probable	Impacto	Probabilidad	Nivel de riesgo	Medida recomendada
1	Uso de datos personales sin una finalidad claramente documentada	Ítems sobre licitud, finalidad y uso de datos personales en sistemas de IA	Falta de documentación formal sobre los fines del tratamiento de datos en modelos de IA	Alto	Media	Alto	Documentar formalmente las finalidades del tratamiento de datos personales antes de implementar soluciones de IA y revisarlas periódicamente.
2	Tratamiento excesivo de datos personales en soluciones de IA	Ítems relacionados con minimización y proporcionalidad de datos	Uso de más datos de los necesarios para entrenar, operar o validar modelos de IA	Alto	Media	Alto	Aplicar criterios de minimización y proporcionalidad de datos, asegurando que solo se utilice la información estrictamente necesaria para cada finalidad.
3	Insuficiente transparencia sobre decisiones automatizadas	Ítems sobre comunicación al cliente, avisos de privacidad y canales de información	Falta de explicaciones claras sobre cómo la IA incide en decisiones financieras	Alto	Media	Alto	Fortalecer los avisos de privacidad e incorporar información clara sobre el uso de IA, decisiones automatizadas y sus posibles efectos para los titulares.
4	Falta de evaluaciones de impacto en privacidad antes de implementar IA	Ítems sobre evaluaciones de impacto y gestión de riesgos	Ausencia de un procedimiento formal para evaluar riesgos de privacidad en proyectos de IA	Alto	Media	Alto	Implementar evaluaciones de impacto en privacidad antes de desarrollar o poner en producción soluciones de IA que traten datos personales.

N.º	Riesgo identificado	Relación con el instrumento aplicado	Causa probable	Impacto	Probabilidad	Nivel de riesgo	Medida recomendada
5	Debilidad en la gobernanza algorítmica institucional	Ítems sobre políticas internas, roles, comités y supervisión de IA	Roles y responsabilidades no completamente formalizados para supervisar el ciclo de vida de la IA	Alto	Media	Alto	Establecer un modelo formal de gobernanza algorítmica que defina políticas, responsables, comités, controles y mecanismos de supervisión continua.
6	Riesgo de sesgos en decisiones automatizadas	Ítems sobre análisis de riesgo, crédito, toma de decisiones y supervisión de IA	Falta de auditorías periódicas para validar equidad, precisión y comportamiento del modelo	Alto	Media	Alto	Realizar auditorías algorítmicas periódicas y pruebas de sesgo, especialmente en modelos que incidan en decisiones crediticias, riesgo o atención al cliente.
7	Acceso no autorizado a datos personales procesados por IA	Ítems sobre autenticación, control de acceso y seguridad técnica	Controles de acceso insuficientes o falta de revisión periódica de privilegios	Alto	Baja	Medio	Reforzar controles de acceso basados en roles, autenticación robusta, revisión periódica de privilegios y segregación de funciones.
8	Falta de trazabilidad sobre el uso de datos personales en IA	Ítems sobre cifrado, auditoría y monitoreo	Registros insuficientes sobre quién accede, modifica o utiliza datos en sistemas de IA	Medio	Media	Medio	Implementar registros de auditoría, monitoreo continuo y mecanismos de trazabilidad sobre el acceso, modificación y uso de datos personales en sistemas de IA.
9	Gestión limitada de incidentes relacionados con IA y datos personales	Ítems sobre gestión de incidentes y violaciones de datos	Procedimientos generales de incidentes que no contemplan escenarios específicos de IA	Alto	Baja	Medio	Incorporar escenarios específicos de IA y tratamiento automatizado de datos dentro de los procedimientos de respuesta.

N.º	Riesgo identificado	Relación con el instrumento aplicado	Causa probable	Impacto	Probabilidad	Nivel de riesgo	Medida recomendada
10	Canales poco claros para ejercer derechos sobre datos tratados por IA	Ítems sobre derechos del titular y canales accesibles	Falta de mecanismos específicos para consultas o reclamos relacionados con IA	Medio	Media	Medio	Definir canales claros y accesibles para que los titulares puedan consultar, reclamar o ejercer derechos relacionados con el uso de sus datos en sistemas de IA.

Fuente: Elaboración propia con base en los resultados del instrumento aplicado y la revisión documental complementaria.

La matriz evidencia que los riesgos de mayor criticidad se relacionan con la falta de documentación formal de finalidades, el tratamiento excesivo de datos, la transparencia limitada, la ausencia de evaluaciones de impacto en privacidad, la gobernanza algorítmica y los posibles sesgos en decisiones automatizadas. Estos aspectos coinciden con estudios que señalan la necesidad de fortalecer la gobernanza, la trazabilidad, la explicabilidad y la rendición de cuentas en sistemas algorítmicos, especialmente cuando estos procesan datos sensibles en sectores regulados como el financiero (Crisanto et al., 2024; Diakopoulos, 2016; Wachter et al., 2017; Zarsky, 2016). Por ello, las medidas recomendadas se orientan a reforzar controles técnicos, documentales, organizativos y de supervisión durante todo el ciclo de vida de las soluciones de inteligencia artificial.

4.5 MADUREZ INSTITUCIONAL

El nivel de madurez identificado (nivel 4) refleja que las instituciones financieras han incorporado herramientas de inteligencia artificial en procesos estratégicos como análisis de riesgo, perfilamiento crediticio y monitoreo transaccional; sin embargo, la evidencia sugiere que la gobernanza algorítmica aún no se encuentra completamente institucionalizada. La literatura especializada sostiene que la adopción de sistemas automatizados de toma de decisiones requiere mecanismos formales de rendición de cuentas (accountability), transparencia y supervisión continua para evitar riesgos de opacidad y afectación de derechos fundamentales (Diakopoulos, 2016).

Asimismo, estudios en el ámbito del derecho de protección de datos han señalado que la automatización en decisiones financieras plantea desafíos significativos respecto a la explicabilidad y el derecho de los individuos a comprender el razonamiento detrás de decisiones automatizadas (Wachter et al., 2017). En este sentido, un sistema puede considerarse técnicamente avanzado, pero no plenamente maduro desde la perspectiva de protección de datos si no incorpora evaluaciones sistemáticas de impacto y mecanismos de revisión humana.

Adicionalmente, la literatura advierte que los sistemas algorítmicos pueden generar efectos discriminatorios involuntarios cuando no se aplican controles adecuados de equidad y supervisión regulatoria (Zarsky, 2016). Esto refuerza la interpretación de que el nivel actual (4) representa una fase avanzada en términos tecnológicos, pero aún en consolidación desde la perspectiva de gobernanza integral.

Para alcanzar un nivel 5 de madurez, sería necesario institucionalizar la privacidad por diseño, implementar auditorías algorítmicas periódicas y establecer estructuras formales de supervisión basadas en riesgo, integrando principios jurídicos y técnicos en todo el ciclo de vida del modelo (Kuner et al., 2020).

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

En continuidad con el análisis de los resultados presentados en el capítulo anterior, el presente capítulo tiene como finalidad exponer los principales hallazgos derivados del estudio sobre el estado actual de protección de datos personales en soluciones de inteligencia artificial dentro del sistema financiero hondureño. En este apartado se sintetizan los resultados obtenidos en relación con los objetivos planteados y las preguntas de investigación formuladas, permitiendo establecer conclusiones fundamentadas en la evidencia recopilada. Se presentan recomendaciones orientadas a fortalecer la gobernanza algorítmica, la transparencia institucional y el marco regulatorio aplicable, con el propósito de promover una implementación responsable de la inteligencia artificial, garantizando la protección de los derechos de los titulares de datos y el fortalecimiento de la confianza en el sistema financiero nacional.

5.1 CONCLUSIONES

Las conclusiones se presentan en correspondencia con los objetivos específicos de la investigación, a fin de mantener la coherencia entre lo planteado, lo medido y lo analizado. En este sentido, cada conclusión sintetiza los principales hallazgos relacionados con el nivel de adopción de soluciones de inteligencia artificial, el nivel de protección de datos personales y la relación estadística entre ambas variables.

En relación con los resultados obtenidos en el Capítulo IV, se concluye lo siguiente:

1. Se concluye que las instituciones participantes presentan una percepción favorable respecto al nivel de adopción de soluciones de inteligencia artificial en el sistema financiero hondureño. Los resultados evidencian que la IA se utiliza principalmente en procesos vinculados con eficiencia operativa, detección de fraude, análisis de riesgo, integración con sistemas centrales y planificación estratégica. Esta valoración, complementada con la revisión documental, permite reconocer que la innovación financiera requiere mecanismos formales de gobernanza, supervisión y gestión de riesgos tecnológicos para asegurar una adopción ordenada y responsable.

2. Se concluye que el nivel de protección de datos personales asociado al uso de soluciones de inteligencia artificial es valorado positivamente por los participantes del estudio. Los resultados muestran una percepción favorable sobre la existencia de controles de acceso, cifrado, auditoría, gestión de incidentes, avisos de privacidad y mecanismos para el ejercicio de derechos de los titulares. Sin embargo, la revisión documental complementaria evidencia que estos controles deben fortalecerse mediante evaluaciones de impacto en privacidad, documentación formal, trazabilidad y mecanismos de supervisión que permitan respaldar objetivamente el cumplimiento de los principios de protección de datos.

3. Se concluye que existe una relación positiva, muy fuerte y estadísticamente significativa entre el nivel de adopción de soluciones de inteligencia artificial y el nivel de protección de datos personales en las instituciones participantes del sistema financiero hondureño. El coeficiente de correlación de Spearman evidencia que, a mayor adopción de IA, mayor es también la percepción de aplicación de medidas de protección de datos personales. No obstante, esta relación no debe interpretarse como causalidad, sino como una asociación estadística que debe ser comprendida junto con la evidencia documental revisada y las limitaciones metodológicas del estudio.

5.2 RECOMENDACIONES

Con base en las conclusiones anteriores, se brindan las siguientes recomendaciones:

1. Se recomienda que las instituciones del sistema financiero hondureño fortalezcan sus mecanismos de gobernanza para la adopción de soluciones de inteligencia artificial, mediante la formalización de políticas internas, definición de roles responsables, creación de comités de supervisión y documentación del ciclo de vida de los modelos. Estas acciones deben estar respaldadas por evidencia documental verificable, de manera que la implementación de IA pueda ser evaluada no solo desde la percepción interna, sino también mediante registros, políticas, procedimientos y controles formalmente establecidos.

2. Se recomienda reforzar los mecanismos de protección de datos personales asociados al uso de inteligencia artificial, incorporando evaluaciones de impacto en privacidad, controles de minimización de datos, revisión periódica de accesos, cifrado,

registros de auditoría y procedimientos específicos para la gestión de incidentes relacionados con sistemas automatizados. Estas medidas deben documentarse y revisarse periódicamente, a fin de contar con evidencia objetiva que permita demostrar el cumplimiento de los principios de protección de datos personales.

3. Se recomienda que los organismos supervisores y las instituciones financieras impulsen lineamientos específicos sobre transparencia, explicabilidad y responsabilidad en el uso de inteligencia artificial. Dichos lineamientos deben promover la generación de evidencia documental, la comunicación clara hacia los titulares de datos, la revisión humana de decisiones automatizadas y la trazabilidad de los criterios utilizados por los sistemas de IA, con el propósito de fortalecer la confianza en los servicios financieros digitales.

CAPÍTULO VI. APLICABILIDAD

En el presente capítulo se desarrolla la propuesta de aplicabilidad derivada de los resultados obtenidos en la investigación sobre la protección de datos personales en soluciones de inteligencia artificial dentro del sistema financiero hondureño. A partir de los hallazgos identificados, se plantea un modelo orientado a fortalecer la gobernanza de datos, la transparencia y el cumplimiento de principios de privacidad en las instituciones financieras.

6.1 NOMBRE DE LA PROPUESTA

Modelo de gobernanza y protección de datos personales en soluciones de inteligencia artificial para el sistema financiero hondureño.

6.2 JUSTIFICACIÓN DE LA PROPUESTA

De acuerdo con los resultados obtenidos en el Capítulo IV, se identificó una percepción favorable respecto a la adopción de soluciones de inteligencia artificial y a la existencia de controles de protección de datos personales. No obstante, la matriz de riesgos y la revisión documental complementaria evidencian áreas que requieren fortalecimiento, especialmente en gobernanza algorítmica, transparencia, trazabilidad, evaluaciones de impacto en privacidad y documentación formal de controles. En este contexto, la presente propuesta se justifica como un instrumento orientativo que busca promover la adopción progresiva de buenas prácticas y controles básicos, conforme al nivel de madurez institucional de cada entidad.

Desde el punto de vista teórico, la propuesta se sustenta en los principios internacionales de protección de datos personales, tales como licitud, finalidad, minimización, transparencia y responsabilidad, así como en el enfoque de privacidad por diseño, el cual establece que la protección de datos debe integrarse desde las etapas iniciales del desarrollo de sistemas tecnológicos. Asimismo, se apoya en la teoría de la gobernanza algorítmica y en la gestión del riesgo tecnológico, que resaltan la necesidad de establecer mecanismos de control, supervisión y mitigación de riesgos en sistemas basados en inteligencia artificial.

En este contexto, la propuesta resulta pertinente, ya que busca fortalecer la gestión de los datos personales en soluciones de inteligencia artificial, mejorar los niveles de seguridad de la información y contribuir al incremento de la confianza de los usuarios en el sistema

financiero. De igual forma, proporciona lineamientos que pueden servir como referencia para el desarrollo de futuras regulaciones en materia de protección de datos en Honduras.

La propuesta también se fundamenta en la matriz de riesgos identificados en el Capítulo IV, la cual permitió organizar los principales riesgos derivados del uso de soluciones de inteligencia artificial y del tratamiento de datos personales. Estos riesgos evidencian la necesidad de fortalecer la gobernanza algorítmica, la transparencia, las evaluaciones de impacto en privacidad, la trazabilidad y los controles de seguridad, por lo que el modelo propuesto busca ofrecer lineamientos prácticos para reducir dichas brechas de manera progresiva y conforme al nivel de madurez institucional.

La propuesta también se fundamenta en la revisión documental complementaria incorporada en el Capítulo IV, la cual permitió contrastar los resultados obtenidos mediante la encuesta con fuentes técnicas, normativas e institucionales vinculadas con inteligencia artificial, protección de datos personales y gestión de riesgos tecnológicos. Esta integración fortalece la aplicabilidad del modelo propuesto, ya que permite orientar los lineamientos no solo a partir de la percepción de los participantes, sino también con base en evidencia documental y buenas prácticas reconocidas.

6.3 ALCANCE DE LA PROPUESTA

La presente propuesta establece lineamientos para una posible implementación orientados a fortalecer las medidas básicas de seguridad de la información y la protección de datos personales en soluciones de inteligencia artificial utilizadas por las entidades del sistema financiero. Su alcance se enfoca en proporcionar una guía estructurada que permita identificar controles iniciales y orientar su adopción de forma progresiva según el nivel de madurez institucional. Asimismo, se plantea como un modelo adaptable, no obligatorio, que sirve como referencia para mejorar prácticas existentes. Finalmente, se orienta a apoyar a las instituciones en la incorporación gradual de lineamientos básicos de protección de datos.

6.3.1 OBJETIVOS DE LA PROPUESTA

1. Promover la adopción de medidas iniciales de seguridad de la información en el tratamiento de datos personales en sistemas basados en inteligencia artificial.
2. Orientar a las entidades en la incorporación de lineamientos básicos de protección de datos conforme a su nivel de madurez institucional.

6.4 DESCRIPCIÓN Y DESARROLLO DE LA PROPUESTA

En este apartado se desarrolla el contenido esencial de la propuesta, la cual se fundamenta en los hallazgos obtenidos durante la investigación. Aunque los resultados muestran una percepción favorable respecto a la adopción de soluciones de inteligencia artificial y a la existencia de controles de protección de datos personales, también se identificaron áreas que requieren fortalecimiento, especialmente en gobernanza algorítmica, transparencia, trazabilidad, evaluaciones de impacto en privacidad y documentación formal de controles. En este sentido, la propuesta se estructura mediante lineamientos y elementos prácticos que permiten a las instituciones identificar riesgos, fortalecer controles básicos y adoptar buenas prácticas de forma progresiva, conforme al nivel de madurez institucional de cada entidad.

6.4.1 ¿QUÉ SE HARÁ Y CÓMO SE HARÁ?

Se propone el diseño de lineamientos básicos orientados a fortalecer la protección de datos personales en soluciones de inteligencia artificial utilizadas por las instituciones del sistema financiero hondureño, incorporando medidas iniciales de seguridad de la información como base para garantizar la confidencialidad, integridad y disponibilidad de los datos. Estas acciones incluyen la identificación de riesgos en el tratamiento automatizado de datos personales, la definición de controles básicos de seguridad y la adopción de prácticas iniciales de protección de datos. El diseño de la propuesta se fundamenta metodológicamente en los hallazgos obtenidos en el Capítulo IV, así como en los enfoques teóricos abordados en el marco teórico, permitiendo estructurar una guía práctica y adaptable que podría ser aplicada de forma progresiva según el nivel de madurez institucional de cada entidad.

6.4.2 DESARROLLO DE LOS ELEMENTOS DE LA PROPUESTA.

En función de los hallazgos obtenidos en la investigación, se desarrollan los siguientes entregables orientados a fortalecer la protección de datos personales y la adopción de medidas básicas de seguridad de la información en soluciones de inteligencia artificial dentro del sistema financiero hondureño:

1. Análisis básico de riesgos en datos personales

Se propone la identificación de riesgos asociados al tratamiento automatizado de datos personales en sistemas de inteligencia artificial, considerando posibles vulnerabilidades

relacionadas con el acceso no autorizado, uso indebido de la información y falta de controles de seguridad. Este análisis permitirá a las instituciones reconocer los principales puntos críticos en el manejo de datos.

2. Lineamientos básicos de protección de datos

Se establecen lineamientos orientados a promover buenas prácticas en el tratamiento de datos personales, incluyendo principios de confidencialidad, minimización de datos, control de acceso y uso adecuado de la información. Estos lineamientos servirán como guía inicial para fortalecer la gestión de datos en entornos de inteligencia artificial.

3. Medidas iniciales de seguridad de la información

Se plantean controles básicos de seguridad de la información, tales como gestión de accesos, resguardo de la información, uso de contraseñas seguras y monitoreo básico de actividades, con el fin de reducir riesgos en el tratamiento de datos personales en sistemas automatizados.

4. Plan básico de capacitación y sensibilización

Se propone la implementación de acciones de capacitación dirigidas al personal de las instituciones financieras, orientadas a fortalecer el conocimiento sobre protección de datos personales, riesgos asociados a la inteligencia artificial y la importancia de aplicar medidas básicas de seguridad de la información.

5. Protocolo básico de buenas prácticas en IA

Se plantea la elaboración de un protocolo que oriente el uso responsable de soluciones de inteligencia artificial, estableciendo criterios básicos de transparencia, uso adecuado de los datos y responsabilidad en los procesos automatizados.

6.5 CRONOGRAMA DE EJECUCIÓN

El cronograma de ejecución organiza las actividades necesarias para el desarrollo de la propuesta, desde el diagnóstico hasta la presentación final. Su estructura en cuatro meses permite una implementación ordenada y el cumplimiento de los objetivos del proyecto.

Tabla 11. Cronograma de ejecución del modelo de gobernanza de datos

Fase	Actividad	Mes 1	Mes 2	Mes 3	Mes 4
1	Planificación del proyecto	✓			
	Diagnóstico y levantamiento de información	✓			
2	Identificación de riesgos en IA y datos	✓	✓		
	Análisis de brechas (gap analysis)		✓		
3	Diseño del modelo de gobernanza de datos		✓	✓	
	Definición de controles y medidas de seguridad		✓	✓	
4	Elaboración de políticas y procedimientos			✓	
	Documentación (manuales, lineamientos)			✓	
5	Implementación piloto en área seleccionada			✓	✓
	Capacitación del personal			✓	✓
6	Evaluación de resultados				✓
	Ajustes y mejoras del modelo				✓
7	Elaboración de informe final				✓
	Presentación de resultados				✓

Fuente: Elaboración propia (2026)

6.6 PRESUPUESTO DE EJECUCIÓN

En este apartado se presenta una estimación ampliada de los recursos financieros requeridos para la implementación del modelo de gobernanza y protección de datos personales en soluciones de inteligencia artificial en el sistema financiero hondureño.

Tabla 12. Presupuesto de ejecución.

Categoría	Concepto	Descripción	Costo (L)
Recurso humano	Consultor en ciberseguridad / IA	Diseño, análisis y supervisión del proyecto	L80,000.00
	Analista de cumplimiento	Evaluación normativa y controles	L40,000.00
	Soporte técnico / TI	Apoyo en implementación	L20,000.00
Tecnología	Herramientas de análisis	Software para análisis de datos, IA y riesgos	L50,000.00
	Licencias y servicios	Plataformas, nube o herramientas básicas	L20,000.00
Capacitación	Talleres	Capacitación en protección de datos e IA	L25,000.00
	Materiales	Guías, manuales y documentación de apoyo	L3,000.00
Operativos	Transporte y logística	Reuniones, visitas a instituciones	L15,000.00
	Documentación	Impresiones, informes finales	L10,000.00
Total			**L263,000.00**

Fuente: Elaboración propia (2026)

REFERENCIAS BIBLIOGRÁFICAS

(BIS), B. d. (2024). *Regulating AI in the Financial Sector*. Obtenido de BIS: https://www.bis.org/fsi/publ/insights63.pdf

Advogados, L. (2024). *What you need to know about data protection in Latin America.* São Paulo: Lefosse Advogados.

Aldboush, H. H., & Ferdous, M. (10 de Julio de 2023). Obtenido de Generando confianza en la tecnología financiera: un análisis de las consideraciones éticas y de privacidad en la intersección del Big Data, la IA y la confianza del cliente.: https://www.mdpi.com/2227-7072/11/3/90

Alexandre Veronese, A. N. (19 de agosto de 2021). Regulatory paths for artificial intelligence in latin american countries with data protection law frameworks: limits and possibilities of integrating policies. *Revista Latinoamericana de Economía y Sociedad Digital*, 371-384. Obtenido de Latinoamericana de Economía y Sociedad Digital: https://revistalatam.digital/article/210207-2/

AlSur. (2024). *The Regulatory Pathways for AI in Latin America: Collection of study cases in Brazil, Mexico, Peru and Colombia.* Buenos Aires: AlSur. Obtenido de https://www.alsur.lat/sites/default/files/2024-09/ALSUR%20-%20IA%20en%20Latam%20%5BENG%5D.pdf

Ashrafuzzaman, M., Parveen, R., Sumiya, M. A., & Rahman, A. (2025). AI-POWERED PERSONALIZATION IN DIGITAL BANKING: A REVIEW OF CUSTOMER BEHAVIOR ANALYTICS AND ENGAGEMENT. *American Journal of Interdisciplinary Studies*, 40-71. doi:10.63125/z9s39s47

Awwal-Bolanta, O., & Anakanire, O. C. (2024). Artificial Intelligence and Data Privacy: Evaluation of The Innovations, Legal Frameworks and Technological Protection. *Journal of Law and Global Policy (JLGP)*, 36-49. doi:10.56201/JLGP.v9.no2.2024.pg36.49

Banco Central de Honduras & Comisión para la Defensa y Promoción de la Competencia. (2017). *Identificación de Barreras Regulatorias a la Competencia en Honduras.* Tegucigalpa: Banco Central de Honduras. Obtenido de https://www.bch.hn/varios/MIF/Documentos/Documento%20Barreras%20Regulatorias.pdf

BCH, CNBS, & ACDI/VOCA. (2021). *Barreras Regulatorias en la Industria de Tecno-Finanzas en Honduras*. Obtenido de BCH: https://www.bch.hn

CNBS. (2024). *Documentos FinTech*. Obtenido de Comisión Nacional de Bancos y Seguros: https://www.cnbs.gob.hn/fintech/documentos-fintech-cnbs/

Comisión Nacional de Bancos y Seguros. (2023). *Regulación Fintech Honduras*. Obtenido de Comisión Nacional de Bancos y Seguros: https://www.cnbs.gob.hn/documentos-fintech/regulacion-fintech-honduras/

Competencia, B. C. (2017). *Identificación de Barreras Regulatorias a la Competencia en Honduras.* Tegucigalpa: Banco Central de Honduras. Obtenido de https://www.bch.hn/varios/MIF/Documentos/Documento%20Barreras%20Regulatorias.pdf

Creswell, J. W. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches.* Thousand Oaks, CA: SAGE Publications.

Crisanto, J. C., Prenio, J., Yong, J., & Leuterio, C. B. (s.f.). *Regulating Al in the financial sector: recent developments and main challenges*. Obtenido de Bank for International Settlements: https://www.bis.org/fsi/publ/insights63.htm

Hernández-Sampieri, R. F.-C. (2014). *Metodología de la investigación.* México: McGraw-Hill.

Honduras, R. F. (2023). *Regulación Fintech Honduras.* Tegucigalpa: Comisión Nacional de Bancos y Seguros. Obtenido de https://www.cnbs.gob.hn/documentos-fintech/regulacion-fintech-honduras/

Internacional, A. d. (18 de septiembre de 2024). *Guía comercial de Honduras*. Obtenido de nternational Trade Administration: https://www.trade.gov/country-commercial-guides/honduras-digital-economy

Irfan, M., Yasin, A., Hussain, R. A., Bashir, N., & Munir, B. (30 de septiembre de 2024). ARTIFICIAL INTELLIGENCE, DATA PROTECTION AND TRANSPARENCY: A COMPARATIVE STUDY OF GDPR AND CCPA. *Journal of Media Horizons*. doi:10.5281/zenodo.15210292

ISO/IEC. (2022). ISO/IEC 27001:2022 – Information security management systems. *International Organization for Standardization*, https://www.iso.org/standard/82875.html.

Jim, M. M., Hasan, M., & Munira, M. S. (29 de diciembre de 2024). *The Role Of AI In Strengthening Data Privacy For Cloud Banking*. Obtenido de Frontiers in Applied Engineering and Technology: https://journal.aimintlllc.com/index.php/FAET/article/view/39/

Mbah, G. O. (diciembre de 2024). Data privacy in the era of AI: Navigating regulatory landscapes for global businesses. *International Journal of Science and Research Archive*, 2040-2058. doi:10.30574/ijsra.2024.13.2.2396

OECD. (2021). *OECD Privacy Guidelines*. Obtenido de Organisation for Economic Co-operation and Development: https://www.oecd.org/privacy

Reyes, M. A. (s.f.). *Central American Journals Online*. Obtenido de La Revista de Derecho: https://camjol.info/index.php/LRD/article/view/19394

Richard, S., & Blake, H. (octubre de 2024). *Data Privacy Challenges in AI-Driven Financial Services*. Obtenido de ResearchGate: https://www.researchgate.net/publication/389466331_Data_Privacy_Challenges_in_AI-Driven_Financial_Services

Ridzuan, N. N., Masri, M., Anshari, M., Fitriyani, N. L., & Syafrudin, M. (21 de Julio de 2024). *AI in the Financial Sector: The Line between Innovation, Regulation and Ethical Responsibility*. Obtenido de Information: https://www.mdpi.com/2078-2489/15/8/432

Rojas, L., & De León, I. (2020). *Barreras Regulatorias en la Industria de Tecno-Finanzas en Honduras*. Obtenido de BCH: https://www.bch.hn/varios/MIF/Documentos/Documento%20Barreras%20Regulatorias.pdf

Seguros, C. N. (2024). *Hub de Innovación Financiera de Honduras*. Obtenido de Comisión Nacional de Bancos y Seguros: https://www.cnbs.gob.hn/hub-de-innovacion-financiera-de-honduras/

Selvam, M. (2025). Ethical Al for Personalized Banking: Addressing Bias and Fairness Challenges. *LatIA*, 361. doi:10.62486/latia2025361

Selvam, M. (mayo de 2025). Ethical Al for Personalized Banking: Addressing Bias and Fairness Challenges. *LatIA*. doi:10.62486/latia2025361

Srivastava, S., & Sharma, S. (enero de 2024). *CUSTOMER TRUST AND DATA PRIVACY IN DIGITAL BANKING SERVICES - A STUDY IN CONTEXT OF ARTIFICAL INTELLIGENCE*. Obtenido de ShodhKosh: Journal of Visual and Performing Arts: https://www.granthaalayahpublication.org/Arts-Journal/ShodhKosh/article/view/3505

European, Union. (2016). General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679. *EUR-Lex*, https://eur-lex.europa.eu/eli/reg/2016/679/oj.

Groves, R. M. (2006). Nonresponse rates and nonresponse bias in household surveys. Public Opinion Quarterly, 70(5), 646–675. https://doi.org/10.1093/poq/nfl033

Kelley, K., Clark, B., Brown, V., & Sitzia, J. (2003). Good practice in the conduct and reporting of survey research. International Journal for Quality in Health Care, 15(3), 261–266. https://doi.org/10.1093/intqhc/mzg031

Carmines, E. G., & Zeller, R. A. (1979). Reliability and validity assessment. Sage Publications. https://doi.org/10.4135/9781412985642

Flannelly, K. J., Flannelly, L. T., & Jankowski, K. R. B. (2014). Independent, dependent, and other variables in healthcare and chaplaincy research. Journal of Health Care Chaplaincy, 20(4), 161–170. https://doi.org/10.1080/08854726.2014.959374

Joshi, A., Kale, S., Chandel, S., & Pal, D. K. (2015). Likert scale: Explored and explained. British Journal of Applied Science & Technology, 7(4), 396–403. https://doi.org/10.9734/BJAST/2015/14975

Ashta, A., & Herrmann, H. (2021). Artificial intelligence and fintech: An overview of opportunities and risks for financial services. Strategic Change, 30(3), 211–222. https://doi.org/10.1002/jsc.2403

Dwivedi, Y. K., Hughes, L., Ismagilova, E., et al. (2021). Artificial intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International Journal of Information Management, 57, 101994. https://doi.org/10.1016/j.ijinfomgt.2019.08.002

Gomber, P., Koch, J.-A., & Siering, M. (2018). Digital finance and fintech: Current research and future research directions. Journal of Business Economics, 87(5), 537–580. https://doi.org/10.1007/s11573-017-0852-x

Ryll, L., Seidens, S., & Ryll, L. (2020). Artificial intelligence in financial services: Opportunities and challenges. Journal of Financial Transformation, 51, 24–32.

Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., & Floridi, L. (2018). Artificial intelligence and the ‘good society’: The US, EU, and UK approach. Science and Engineering Ethics, 24(2), 505–528. https://doi.org/10.1007/s11948-017-9901-7

Diakopoulos, N. (2016). Accountability in algorithmic decision making. Communications of the ACM, 59(2), 56–62. https://doi.org/10.1145/2844110

Kuner, C., Bygrave, L. A., & Docksey, C. (2020). The EU General Data Protection Regulation (GDPR): A commentary. Oxford University Press.

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. International Data Privacy Law, 7(2), 76–99. https://doi.org/10.1093/idpl/ipx005

Zarsky, T. Z. (2016). The trouble with algorithmic decisions: An analytic road map to examine efficiency and fairness in automated and opaque decision making. Science, Technology & Human Values, 41(1), 118–132. https://doi.org/10.1177/0162243915605575

Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A., Galanos, V., Ilavarasan, P. V., Janssen, M., Jones, P., Kar, A. K., Kizgin, H., Kronemann, B., Lal, B., Lucini, B., … Williams, M. D. (2021). Artificial intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International Journal of Information Management, 57, 101994. https://doi.org/10.1016/j.ijinfomgt.2019.08.002

Groves, R. M. (2006). Nonresponse rates and nonresponse bias in household surveys. Public Opinion Quarterly, 70(5), 646–675. https://doi.org/10.1093/poq/nfl033

Sedgwick, P. (2014). Cross sectional studies: Advantages and disadvantages. BMJ, 348, g2276. https://doi.org/10.1136/bmj.g2276

Banco Central de Honduras, Comisión Nacional de Bancos y Seguros, & ACDI/VOCA. (2021). Barreras regulatorias en la industria de tecno-finanzas en Honduras. Banco Central de Honduras.

Crisanto, J. C., Leuterio, C. B., Prenio, J., & Yong, J. (2024). Regulating AI in the financial sector: Recent developments and main challenges (FSI Insights No. 63). Bank for International Settlements.

GLOSARIO

En esta sección se presentan los principales términos utilizados en la investigación, con el propósito de facilitar la comprensión de los conceptos técnicos abordados a lo largo del estudio.

Auditoría de seguridad:

Proceso sistemático mediante el cual se evalúan los sistemas de información con el objetivo de identificar vulnerabilidades y verificar el cumplimiento de políticas y controles de seguridad.

Control de acceso:

Mecanismo que permite restringir el acceso a sistemas o información únicamente a usuarios autorizados, garantizando la seguridad de los datos.

Datos personales:

Información que identifica o puede identificar a una persona natural, como nombre, número de identidad, dirección o información financiera.

Evaluación de impacto en privacidad (DPIA):

Proceso que permite identificar, analizar y mitigar los riesgos asociados al tratamiento de datos personales, especialmente en sistemas que utilizan inteligencia artificial.

Gobernanza de datos:

Conjunto de políticas, procesos y estándares que regulan la gestión, calidad, seguridad y uso adecuado de los datos dentro de una organización.

Incidente de seguridad:
Evento que compromete la confidencialidad, integridad o disponibilidad de la información.

Inteligencia artificial (IA)

Tecnología que permite a los sistemas realizar tareas que requieren inteligencia humana, como análisis de datos, aprendizaje automático y toma de decisiones automatizadas.

Riesgo:

Probabilidad de que una amenaza explote una vulnerabilidad, generando un impacto negativo en la organización.

Seguridad de la información:

Conjunto de medidas orientadas a proteger la información, garantizando su confidencialidad, integridad y disponibilidad.

Tratamiento de datos:

Cualquier operación realizada sobre datos personales, como recolección, almacenamiento, uso, transferencia o eliminación.

ANEXOS

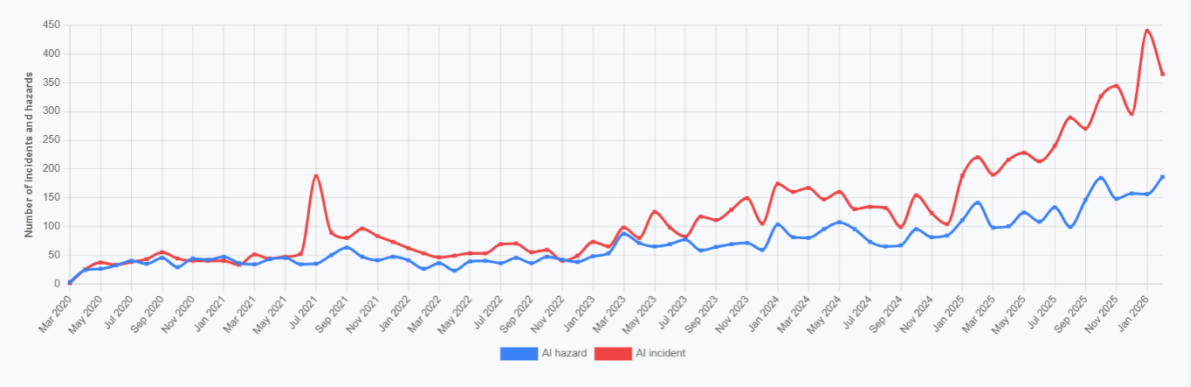


Figura 21. Evolución de incidentes y riesgos asociados a la inteligencia artificial según su gravedad (2020–2026).

Fuente: OECD (2024). OECD.AI Incidents Monitor. https://oecd.ai/en/incidents