Design Thinking Applied to Financial Fraud Prevention in Organizations

Jessica Wu Su[1]; Sergio Fernando Espinoza Abanto[1]; Roberto Enrique Gálvez Flores[1]; Roxanna Elvira Ardiles Carvo[1]

[1]Facultad de Ciencias Empresariales, Carrera de Contabilidad y Finanzas, Universidad de Lima, Perú

20222826@aloe.ulima.edu.pe, 20220899@aloe.ulima.edu.pe, rgalvezf@ulima.edu.pe, rardiles@ulima.edu.pe

Abstract- ***This paper analyzes the contribution of Design Thinking to the elaboration of financial-fraud prevention strategies in organizations. Current prevention mechanisms rely mainly on technical instruments that, despite achieving high accuracy, face real difficulties in organizational adoption. Following a systematic review guided by the PRISMA protocol, 120 records were examined in Scopus and Web of Science, of which 22 were retained after applying inclusion, exclusion, and quality criteria. Findings show that financial fraud is often addressed as an isolated technical or behavioral problem, and that understanding and trust remain unresolved barriers to the adoption of detection systems. Based on these findings, a conceptual framework is proposed linking the empathize, define, ideate, prototype, test and learn stages of Design Thinking with technical, organizational, and regulatory requirements identified as recurrent gaps. The study concludes that a human-centered design approach has the potential to help translate accurate but opaque detection tools into solutions organizations can understand, trust, and adopt.***

Keywords- ***design thinking, financial fraud, fraud prevention, human-centered design, explainable AI, compliance.***

Design Thinking aplicado al Fraude Financiero en las Organizaciones

Resumen- El presente artículo analiza la contribución del design thinking en la elaboración de las estrategias de prevención del fraude financiero en las organizaciones. Los mecanismos actuales de prevención se apoyan principalmente en instrumentos técnicos que, si bien alcanzan una alta precisión, enfrentan dificultades reales de adopción dentro de las organizaciones. A partir de una revisión sistemática guiada por el protocolo PRISMA, se examinaron 120 registros de Scopus y Web of Science, de los cuales se retuvieron 22 tras aplicar criterios de inclusión, exclusión y calidad. Los hallazgos muestran que el fraude financiero suele abordarse como un problema técnico o conductual de forma aislada, y que la comprensión junto con la confianza siguen siendo barreras no resueltas para la adopción de sistemas de detección. A partir de estos hallazgos, se propone un marco conceptual que vincula las etapas de empatizar, definir, idear, prototipar, probar y aprender del design thinking con requisitos técnicos, organizacionales y normativos identificados como vacíos recurrentes. Se concluye que un enfoque de diseño centrado en las personas tiene el potencial de ayudar a traducir herramientas de detección precisas, pero complejas, en soluciones que las organizaciones puedan comprender, confiar y adoptar.

Palabras clave- design thinking, fraude financiero, prevención de fraude, diseño centrado en el usuario, IA explicable, cumplimiento normativo.

I. INTRODUCCIÓN

El fraude financiero se ha consolidado como una de las amenazas más persistentes para la estabilidad de las organizaciones del sistema financiero y de servicios digitales. El avance de la digitalización de pagos, la banca móvil y las plataformas fintech amplió, al mismo tiempo, el acceso a servicios financieros, así como la exposición al fraude. Esto se debe a que estos canales permiten operar con mayor anonimato, fragmentar transacciones y mover fondos de origen ilícito con rapidez [1]. Frente a este escenario, las empresas han respondido con el diseño, implementación y gestión de sistemas de control. Entre ellos, mecanismos como controles basados en reglas y análisis de grandes volúmenes de datos. Por ejemplo, herramientas como el big data, el machine learning y el análisis de información digital permiten transformar data compleja en información útil para la toma de decisiones [23]. En los últimos años, también han incorporado modelos de aprendizaje automático capaces de clasificar transacciones fraudulentas con niveles de precisión que superan el 99% [2].

Junto a estos mecanismos, viene también el machine learning para la clasificación de transacciones fraudulentas. Varios de ellos han conseguido niveles de precisión de aproximadamente 99% [2]. Sin embargo, incluso los modelos más precisos tienden a tener limitaciones a causa de su complejidad y dependencia de datos con los que fueron entrenados, reduciendo así su aplicación en escenarios reales [2]. Este problema persiste cuando las soluciones, que son teóricamente sólidas, no logran incorporarse en las operaciones de las organizaciones. Esta distancia entre el desempeño técnico y el uso efectivo da origen al presente estudio.

Por otro lado, el design thinking consiste en una metodología de innovación centrada en las personas, que comprende etapas de empatía y definición del problema hasta su validación. En diferentes escenarios, este se ha propuesto como una forma de reducción para la brecha que existe por el desarrollo de una solución técnica y su adopción en la práctica. Por ejemplo, se ha utilizado para diseñar intervenciones de salud móvil [3] y rediseñar la experiencia de usuario de una aplicación fintech [4]. Además, su adopción en un banco ha modificado el comportamiento creativo de sus empleados [5].

No obstante, un mapeo bibliométrico de 137 registros sobre inteligencia artificial y prevención del fraude financiero encontró que predominan las investigaciones de carácter técnico. En cambio, las ciencias sociales, la ética y el diseño organizacional reciben poca atención [6]. Ninguno de esos registros vincula de forma explícita el design thinking con la prevención del fraude financiero, lo que evidencia un vacío de investigación concreto. Por esta razón, la revisión recopila estudios de áreas relacionadas de ambos campos, cuyos aportes ofrecen fundamentos conceptuales para explorar cómo podrían integrarse.

Este trabajo tiene como objetivo analizar cómo la aplicación potencial de metodologías de design thinking contribuye a diseñar e implementar estrategias de prevención del fraude financiero que sean efectivas, viables técnicamente y adoptables en contextos organizacionales. La investigación adopta un enfoque cualitativo y se desarrolla a partir de una revisión sistemática de la literatura, siguiendo los lineamientos del protocolo PRISMA.

II. MARCO TEÓRICO

A. Fraude financiero

El fraude financiero comprende diversas conductas orientadas a obtener un beneficio económico ilegítimo, por medio del engaño, la manipulación de información o el abuso de confianza dentro del sistema financiero. Buena parte de los estudios, que consideran los aspectos criminológicos y psicológicos, describen el fraude como un evento no solo técnico, sino como un fenómeno cognitivo: las víctimas de fraude en redes de telecomunicaciones toman decisiones influidas por sesgos heurísticos del denominado Sistema 1, que una intervención racional del Sistema 2 no siempre logra corregir a tiempo [7]. Esta dimensión conductual se complementa con una dimensión organizacional, en la que la prevención depende de la coordinación entre auditoría interna, gestión de riesgos, sistemas de denuncia y analítica de datos [1]; y, con una dimensión de red, evidenciada al modelar cómo

colapsan las inversiones cuando un fraude se propaga entre inversores conectados [8].

Un componente técnico central en la prevención contemporánea del fraude es la capacidad de los modelos predictivos para clasificar transacciones sospechosas con precisión. Se reporta un modelo de ensamblaje apilado capaz de superar el 99% de precisión en la detección de fraude con tarjetas de crédito [2], y se propone un procedimiento orientado a la detección ética de fraude en la contratación pública [9]. Ambas propuestas, no obstante, reconocen que la complejidad de sus decisiones -la dificultad para explicar por qué un modelo analiza y clasifica una operación como fraudulenta- limita la confianza que depositan en ellas los analistas y auditores que deben utilizarlas en su trabajo diario. Esta tensión entre precisión algorítmica e interpretabilidad se retoma en profundidad en el apartado siguiente.

B. Design Thinking

El design thinking es una metodología de resolución de problemas que parte de la comprensión empática de las necesidades de los usuarios para, a partir de ahí, definir el problema, generar múltiples alternativas de solución (ideación), construir prototipos de baja o alta fidelidad y someterlos a validación iterativa. Se han sintetizado principios de equidad, transparencia, rendición de cuentas y privacidad como base para orientar el diseño de sistemas de inteligencia artificial que empoderen al usuario en lugar de limitarse a automatizar una tarea [10]. A partir de 75 registros de salud móvil se identificó un proceso integrado denominado 'Pensamiento de Diseño Conductual', compuesto por cinco pasos -empatizar, definir, idear, prototipar y probar- que combina el diseño centrado en el usuario con principios de la ciencia del comportamiento [3].

Fuera del dominio financiero, el design thinking ha mostrado resultados positivos en contextos organizacionales complejos. Mediante una consulta Delphi con 14 consultores se desarrolló y validó una caja de herramientas de design thinking orientada a que las pequeñas y medianas empresas superen barreras de recursos y escepticismo en el liderazgo [11]. Otro caso se refleja dentro de un banco italiano, se demostró que la adopción de design thinking desde el área de recursos humanos modificó las actitudes creativas de los trabajadores [5]. Sin embargo, se señala que el proceso de encuadre (framing) propio del design thinking no es neutro. El motivo radica en que la retroalimentación de los interesados atraviesa un filtro influido por discursos dominantes dentro del equipo de diseño. Dado ello, su aplicación exige prestar atención crítica a los sistemas de valores subyacentes [12].

C. IA explicable

La inteligencia artificial explicable (XAI, por sus siglas en inglés) agrupa un conjunto de técnicas y principios de diseño que permiten a un modelo predictivo justificar sus decisiones ante quien debe utilizarlas, en vez de operar como una caja negra. En la detección de fraude, por ejemplo, se han propuesto principios de diseño para alinear las tareas de los analistas de fraude bancario con métodos de IA explicables. El estudio evidencia que un ejercicio deliberado de empatía con el usuario experto mejora su confianza en las predicciones del modelo [13]. Asimismo, los enfoques recientes de XAI aplicados a la detección de fraudes financieros muestran que es posible combinar un elevado desempeño predictivo con explicaciones locales y globales adaptadas a los requerimientos de distintos grupos de interés [24]. En la misma línea, se ha desarrollado una metodología de diseño participativo para calibrar la confianza entre humanos y sistemas de inteligencia artificial. Su propósito es evitar dos aspectos: minimizar la desconfianza excesiva de las recomendaciones automatizadas o aceptarlas sin cuestionarlas [14]. Estos trabajos plantean que la explicabilidad debe formar parte del diseño, en vez de añadirse como una característica técnica más. Por ello, el uso efectivo de los sistemas más precisos de detección de fraude depende de la comprensión de las decisiones de quienes lo utilizan.

D. Compliance

Un cuarto grupo de propuestas plantea que las normas legales no deben aplicarse al final del proceso, sino que deben incorporarse desde el inicio del desarrollo (compliance-by-design). Este se aprecia, por ejemplo, en las monedas digitales de bancos centrales que funcionan sin conexión a internet, donde se busca equilibrar la privacidad de los usuarios con las reglas para hacer frente al lavado de dinero y el financiamiento del terrorismo [15]. En otro sector, una universidad canadiense pasó de enfocarse únicamente en cumplir la ley a adoptar un modelo de diseño colaborativo centrado en la experiencia de las personas [17]. Por su parte, en el desarrollo de un sistema de visión computacional para verificar el uso de equipo de protección personal se aplicó Lean UX mediante mapas de empatía, prototipos de interfaz y evaluaciones de usabilidad, con el que se obtuvo una puntuación de 87,6 sobre 100 en usabilidad [18]. En conjunto, estos trabajos sugieren que considerar desde el inicio los requerimientos y las perspectivas de quienes utilizarán un sistema de cumplimiento puede favorecer su adopción en la organización, y a su vez mejorar sus resultados.

III. METODOLOGÍA

La presente investigación adopta un enfoque cualitativo mediante la técnica de Revisión Sistemática de Literatura (SLR, por sus siglas en inglés), con el objetivo de recopilar, analizar y sintetizar de manera rigurosa los estudios académicos existentes sobre la aplicación de design thinking para la prevención del fraude financiero en las organizaciones. Se aplicó la metodología PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) como estándar metodológico internacional, que establece pasos y elementos de reporte que garantizan la transparencia y replicabilidad del proceso de identificación y selección de estudios.

A. Planificación de la investigación y ecuación de búsqueda

El tema central de la investigación es la aplicación de design thinking para la prevención del fraude financiero en las organizaciones y la pregunta de investigación planteada es ¿de qué forma la aplicación de design thinking contribuye a mejorar la efectividad y adopción de estrategias de prevención de fraude financiero? La búsqueda ejecutada a partir de esta pregunta se realizó el 14 de julio de 2026 de manera independiente por dos revisores. Asimismo, se aplicaron las ecuaciones de búsqueda

para las bases de datos Scopus y Web of Science, fórmulas que se aprecian en las Tabla 1 y 2, respectivamente.

TABLA 1
FÓRMULA DE BÚSQUEDA PARA SCOPUS

Fórmula de búsqueda para Scopus
(design thinking OR human-centered design OR user-centered design OR service design OR participatory design OR co-design) AND (management OR prevention OR detection OR mitigation OR control OR monitoring OR identification OR risk management OR fraud management OR fraud prevention OR fraud detection) AND (financial fraud OR banking fraud OR bank fraud OR digital banking fraud OR fintech fraud OR financial scams OR regulatory compliance OR anti-fraud OR antifraud OR anti-money laundering OR AML OR know your customer OR KYC)

TABLA 2
FÓRMULA DE BÚSQUEDA PARA WEB OF SCIENCE

Fórmula de búsqueda para Web of Science
(design thinking OR human-centered design) AND (management OR prevention OR detection OR mitigation OR control) AND (financial fraud OR banking fraud OR digital banking fraud OR fintech fraud OR insurance fraud OR financial crime OR financial misconduct OR financial scams OR financial deception OR financial risk OR financial compliance OR anti-fraud OR anti-money laundering)

B. Criterios de selección

Se establecieron criterios de inclusión y exclusión aplicados en dos momentos del proceso: primero sobre el título y el resumen, y posteriormente sobre el texto completo de los registros preseleccionados. La Tabla 3 resume estos criterios.

TABLA 3
CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

N°	Inclusión	Exclusión
1	Documento completo y disponible	Disponibilidad parcial del documento
2	Publicación de acceso abierto	Acceso restringido
3	Publicado entre 2020 y 2026	Publicado antes de 2020
4	Idioma español o inglés	Idioma distinto a español/inglés
5	Relación con el tema	Fuera de contexto temático

Adicionalmente, los registros que superaron el filtro de título y resumen fueron evaluados mediante los criterios presentados en la Tabla 4, con el fin de valorar la calidad de las fuentes y la relevancia de sus aportes -relación con el tema de investigación- para el presente estudio antes de proceder a la lectura completa y tomar la decisión final de inclusión.

TABLA 4
CRITERIOS DE CALIDAD

N°	Criterios
1	¿El artículo presenta con claridad su contenido y análisis?
2	¿Las técnicas utilizadas se describen con suficiente precisión?
3	¿Se reconocen las limitaciones de los hallazgos o del alcance del estudio?
4	¿Los resultados presentados respaldan las conclusiones?

C. Proceso de identificación y cribado

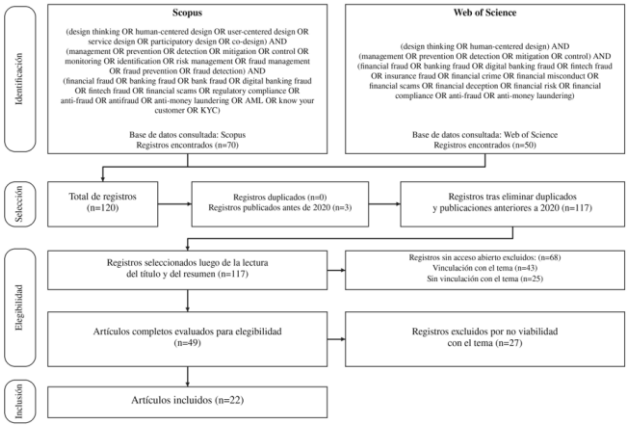


Fig. 1: Gráfico PRISMA

Tal como se muestra en el gráfico PRISMA de la Figura 1, la búsqueda se realizó en las bases de datos Scopus y Web of Science, obteniendo 70 y 50 registros, respectivamente. La revisión en su conjunto no evidenció registros duplicados entre ambas bases de datos, por lo que se mantuvieron los 120 artículos. No obstante, se identificaron 3 documentos con fecha de publicación anterior a 2020, fuera del marco temporal establecido (2020-2026).

Del total de artículos, se excluyeron 98 y se incluyeron 22. Dentro del total de exclusiones, 68 corresponden a documentos sin acceso abierto o cuyo texto completo no pudo obtenerse a través de los repositorios institucionales disponibles, y otros 27 por falta de relación con la investigación. Asimismo, de los 68 registros excluidos por razones de acceso, se realizó un análisis más detallado de la lectura de los resúmenes. Se identificó que 43 documentos guardaban relación con esta investigación, mientras que los 25 restantes no tenían vinculación con el tema.

Por otro lado, la exclusión de publicaciones sin acceso al texto completo constituye una limitación del estudio. De los 68 registros excluidos por esta razón, 43 guardaban relación con el tema, por consiguiente, los 22 estudios incluidos representan el 33,8 % de los 65 registros pertinentes identificados.

D. Construcción de un marco de trabajo

A partir de la síntesis temática de los 22 registros seleccionados, se identificaron dimensiones recurrentes en las áreas de investigación relacionadas con el design thinking y la prevención del fraude financiero. Estas dimensiones fueron agrupadas y articuladas en un marco de trabajo que integra factores técnicos, organizacionales y normativos. El modelo propuesto busca organizar los principales hallazgos de la revisión y orientar la implementación de estrategias de prevención en las organizaciones.

IV. RESULTADOS

A. Análisis de la literatura seleccionada

Los documentos utilizados en esta investigación provienen de las bases de datos Scopus y Web of Science. Las fuentes se concentran entre 2020-2026 con el fin de asegurar que la investigación refleje información actual. En

la Figura 2, se aprecia que entre 2023 y 2025 se publicaron 15 documentos (68%) del total revisado.

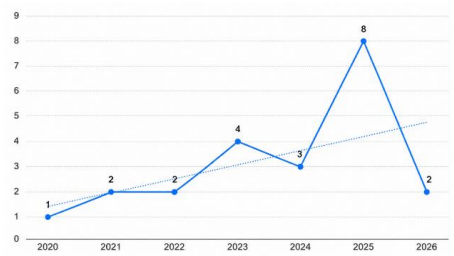


Fig. 2: Cantidad de publicaciones por año

En cuanto a los países de origen de las publicaciones, la Figura 3 muestra que hay una mayor concentración de estudios provenientes de Reino Unido (23%) seguida de Alemania, Estados Unidos y Suiza (18% cada uno), mientras que el resto de los países se muestra en una menor proporción. Los demás países presentan una menor proporción, a su vez, no se identificaron publicaciones de origen latinoamericano entre los 22 estudios incluidos.

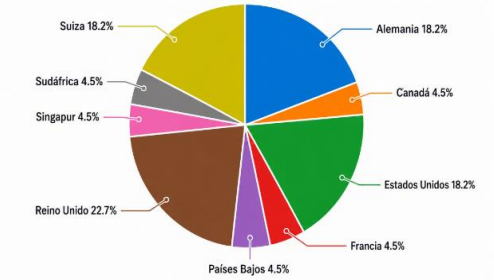


Fig. 3: País de origen de las publicaciones

Por otro lado, los estudios se clasificaron en 4 áreas según el tema principal que abordaban, reflejados en la Figura 4. Se aprecia que el área de investigación más destacada en las publicaciones es Design Thinking (41%) seguido por Detección y Prevención de fraude (23% cada una) y finalmente Compliance (13%).

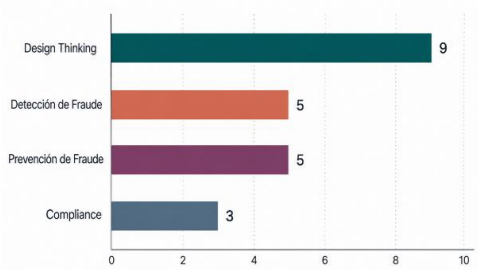


Fig. 4: Área de investigación de las publicaciones

B. El fraude financiero como problema sistémico

Los documentos del área de Prevención de Fraude coinciden en que el fenómeno no puede reducirse a un problema exclusivamente técnico. Las trayectorias cognitivas de las víctimas de fraude en redes de telecomunicaciones permiten proponer un marco que vincula tipos específicos de sesgo cognitivo con tipos de fraude y posibles contramedidas de diseño [7]. A partir de la revisión de 90 registros sobre gobiernos regionales de Indonesia, se muestra que la auditoría interna, la gestión de riesgos, el sistema de denuncias y la analítica de datos suelen operar de forma fragmentada, y que ese desajuste de habilidades explica buena parte de los fallos preventivos observados [1]. Mediante un análisis empírico correlacional basado en la Teoría del Razonamiento Conductual, se identifica que la creencia, la confianza, la autoeficacia y la motivación hedónica del usuario incrementan de forma significativa su intención de adoptar comportamientos preventivos frente al fraude digital, siendo esta intención el predictor más consistente del comportamiento observado [19]. Por su parte, mediante simulación computacional se modela cómo se propagan los colapsos de inversión por fraude en redes sociales, encontrando que una estrategia de protección dirigida a los nodos más influyentes de la red resulta más eficiente que una protección uniforme o aleatoria [8].

En conjunto, estos cuatro estudios describen un problema con al menos tres capas, cognitiva, organizacional y de red social, que rara vez se aborda de manera integrada. Asimismo, un análisis bibliométrico de 137 registros revisados por pares entre 2015 y 2025 confirma que el avance en inteligencia artificial y prevención del fraude sigue siendo en su mayoría en aspectos técnicos, con una participación aún limitada en las ciencias sociales, la ética y el diseño organizacional [6].

C. Detección de fraude: soluciones técnicas y sus límites

Los estudios del área de Detección de Fraude ponen de relieve una tensión entre la precisión de los modelos y la posibilidad de interpretar sus resultados. Como ejemplo, un modelo de ensamblaje apilado combina XGBoost y redes neuronales profundas, y utiliza SMOTE para balancear los datos. Aunque logra una precisión promedio alta al detectar fraude con tarjetas de crédito, presenta limitaciones por su complejidad computacional y su dependencia de los datos utilizados [2]. Por otra parte, el pipeline PRO-Trust plantea un enfoque de detección ética del fraude en la contratación pública. Este aborda cuatro desafíos identificados mediante una revisión sistemática de la literatura acompañada con la validación de auditores expertos: falta de transparencia, limitaciones de explicabilidad, ausencia de supervisión humana y falta de control estratégico [9].

La explicabilidad se aborda también desde el diseño mismo del sistema. Existen un conjunto de principios de diseño que alinea las tareas de los analistas de fraude bancario con métodos de IA explicable [13]. Asimismo, una propuesta anterior recoge requisitos basados en escenarios elaborados con expertos en fraude bancario para conocer qué necesitan los analistas al revisar casos en su trabajo diario [20]. Complementando esta línea, se aplicaron herramientas clave del diseño operacional de soluciones XAI (SAGE por sus siglas en inglés) junto con un diseño basado en escenarios sobre datos reales de fraude con tarjetas. Los resultados revelan vacíos en el diseño de los modelos XAI existentes, generando explicaciones más ajustadas a los requisitos de uso en situaciones reales [21].

Los estudios de este bloque permiten identificar un patrón común. Los modelos técnicos obtienen buenos resultados en las métricas convencionales de precisión, recall o

F1-score. No obstante, con frecuencia enfrentan dificultades para ser interpretados y generar confianza en el usuario final. Este contraste entre el rendimiento técnico y la adopción en la práctica define, precisamente, el punto de entrada al design thinking.

D. Design Thinking dentro y fuera del fraude financiero

Fuera del dominio financiero, dos registros trabajan los principios generales de diseño centrado en el humano que sustentan al design thinking. Un conjunto de principios de equidad, transparencia, rendición de cuentas y privacidad orienta a los sistemas de inteligencia artificial para empoderar al usuario [10], mientras que un marco de diseño participativo, desarrollado y evaluado en dos etapas se orienta a calibrar la confianza en la colaboración entre humanos y sistemas de IA [14]. Mediante una revisión de alcance sistemática (PRISMA-ScR) sobre 75 registros entre 2012 y 2021, se valida un ciclo de cinco pasos que integra design thinking con ciencia del comportamiento para el desarrollo de intervenciones de salud móvil: empatizar, definir, idear, prototipar y probar [3].

Dentro del dominio financiero, se rediseña la interfaz de transacciones de una aplicación fintech a partir de entrevistas y pruebas de usabilidad con siete participantes, obteniendo un prototipo que facilita el control del usuario durante las operaciones [4]. Por ejemplo, un estudio de caso en un banco italiano documentó que la adopción del design thinking a través del área de recursos humanos aumentó la confianza de los empleados en el proceso creativo y su participación proactiva [5]. Del mismo modo, a través de entrevistas y una consulta Delphi con 14 consultores experimentados, alineada con la norma ISO 56001:2024, se desarrolló y validó una caja de herramientas de design thinking que buscaba apoyar a pequeñas y medianas empresas superar barreras de recursos limitados y escepticismo en el liderazgo [11].

Un análisis cualitativo de dos equipos de diseño que trabajaron con una comunidad de personas mayores encontró que el proceso de encuadre (framing) no era neutral. Dado que la retroalimentación de los interesados quedaba filtrada por los discursos dominantes dentro de cada equipo [12]. Esta tensión entre el potencial innovador del design thinking y los sesgos que puede introducir al interpretar las necesidades de otros, conduce al siguiente bloque, dedicado al cumplimiento normativo y la adopción organizacional.

E. Compliance-by-design y adopción organizacional

Cuatro registros abordan la relación entre cumplimiento normativo y diseño centrado en el usuario. En el sector agrícola argentino, el cumplimiento puede servir como punto de partida para que un agricultor adopte un sistema de apoyo a la decisión diseñado con estrategias de design thinking. De este modo, funciona como incentivo y no solo como una obligación externa [16]. Otro estudio combina entrevistas, datos operativos y sprints de codiseño para examinar la transformación de los servicios de ajustes académicos de una institución de educación superior canadiense. Estos servicios pasaron de un modelo centrado en el cumplimiento a otro de codiseño centrado en las personas, con mejoras en los tiempos de espera y en la satisfacción de los usuarios [17].

Adicionalmente, se diseñó un marco conceptual de compliance-by-design que organiza las opciones de diseño de privacidad para monedas digitales de bancos centrales que funcionan sin conexión. Este marco busca equilibrar la privacidad del usuario con los requisitos regulatorios contra el lavado de activos y el financiamiento del terrorismo [15]. Por otro lado, en el sector manufacturero, una investigación empleó Lean UX, es decir, mapas de empatía y prototipos de interfaz de alta fidelidad, con el objetivo de crear un sistema de visión computacional que supervise el cumplimiento del uso de equipo de protección personal. En la evaluación de usabilidad, el sistema obtuvo 87,6 puntos sobre 100 en la escala SUS [18]. Estos trabajos aportan la dimensión normativa y organizacional, las cuales son necesarias para responder al objetivo general, complementando también los hallazgos técnicos del área C y los metodológicos del área D.

F. Viabilidad técnica versus viabilidad organizacional

Al cruzar los hallazgos de las áreas C, D y E, permiten distinguir la viabilidad técnica de una solución de las condiciones necesarias para que una organización la adopte. Por un lado, los modelos de detección pueden alcanzar un buen desempeño [2], pero quienes lo utilizan también necesitan comprender sus resultados [13]. Por ello, un modelo más complejo no es necesariamente el más adoptable. En la misma línea, la sofisticación técnica tampoco asegura que responda a las necesidades reales del usuario final, especialmente cuando el diseño centrado en el usuario para IA explicable sigue desarrollándose de manera fragmentada [22].

A esto se suma, una diferencia entre la medición de la usabilidad y lograr la aceptación dentro de una organización. En concreto, un sistema de visión computacional en manufactura obtuvo 87,6 puntos en la escala SUS [18], mientras que las pequeñas y medianas empresas enfrentan escepticismo de sus líderes ante una caja de herramientas de design thinking [11]. Por eso, aunque se trata de contextos distintos, ambos casos ayudan a precisar qué debe equilibrarse en una estrategia de prevención del fraude, es decir, la solidez técnica y las posibilidades reales de adopción, sin priorizar automáticamente una dimensión sobre la otra.

G. Vacíos y proyección hacia un marco integrado

Ninguno de los estudios revisados aplica directamente el design thinking a la prevención del fraude financiero. Además, el mapeo bibliométrico confirma la poca participación de las ciencias sociales y el diseño en este campo [6], lo que representa una oportunidad clara para futuras investigaciones.

Por otro lado, aún persisten algunos problemas importantes como la dificultad para entender cómo funcionan los modelos de inteligencia artificial y el desafío de adaptar la rapidez del proceso de diseño a las exigencias normativas del sector financiero.

V. DISCUSIÓN DE RESULTADOS

A. Fraude financiero como fenómeno multidimensional

El fraude financiero se entiende como un problema que trasciende más allá de la dimensión técnica. Los hallazgos muestran que el fenómeno combina tres capas interconectadas. En la capa cognitiva, los sesgos heurísticos hacen que los usuarios sean más vulnerables a ciertos engaños [7]. En la organizacional, la falta de coordinación entre auditoría, gestión de riesgos y sistemas de detección puede generar fallas en la

prevención [1]. Por último, en la dimensión de red social, el daño puede extenderse y amplificarse a través de las conexiones entre inversores [8]. Considerar estas dimensiones permite entender por qué un modelo con un alto desempeño de clasificación [2] no garantiza, por sí solo, una prevención efectiva dentro de las organizaciones. Sin embargo, al analizar estas dimensiones de manera separada, la literatura deja un vacío conceptual que podría abordarse bajo un enfoque más integrado.

B. Explicabilidad como barrera crítica de adopción

La precisión de un algoritmo no siempre es suficiente para generar confianza en quienes deben utilizarlo. Incluso los modelos de detección de fraude más sofisticados [2, 9] pueden despertar dudas entre los analistas cuando su funcionamiento resulta difícil de interpretar, por más que sean considerados precisos. En ese contexto, los métodos de inteligencia artificial explicable cobran especial relevancia, ya que, al alinearse con las tareas de estos profesionales, pueden mejorar la confianza en las predicciones del modelo [13]. En el sector financiero, la explicabilidad es un aspecto relevante para la transparencia, fortalecer la confianza y favorecer un uso más responsable de estos modelos [25]. Asimismo, el diseño participativo, que busca calibrar esa confianza [14], también ofrece una base para acercar lo que predice el modelo a lo que el usuario puede comprender y verificar.

C. Design thinking como vía de integración

Si bien no se identificaron antecedentes que vinculan explícitamente design thinking con prevención del fraude financiero, las casuísticas en diversos ámbitos ofrecen evidencia de su potencial. Tal es el caso de su aplicación en la salud móvil, se comprobó una serie de cinco pasos que combina empatía con ciencia del comportamiento [3], mientras que en fintech se ha utilizado para rediseñar interfaces orientadas a facilitar el control del usuario [4]. Dentro de la banca, su adopción a través del área de recursos humanos modificó las actitudes creativas en los empleados [5]. A su vez, en pequeñas y medianas empresas validó cajas de herramientas que permiten superar barreras de recursos [11]. Estos precedentes sugieren que un enfoque que surja de la empatía por los usuarios afectados por el fraude, analistas, auditores, ejecutivos de cumplimiento, podría facilitar que la sofisticación técnica se traduzca en soluciones con mayor posibilidad de adopción dentro de las organizaciones.

D. Cumplimiento normativo como requisito estratégico

Incorporar el cumplimiento normativo desde el inicio del diseño, en lugar de dejarlo para una revisión final, puede mejorar la implementación de las soluciones. El enfoque compliance-by-design se observa, por ejemplo, en las monedas digitales de bancos centrales, donde se busca equilibrar la privacidad con las exigencias regulatorias [15]. También, aparece en sistemas agrícolas, en los que el cumplimiento puede impulsar la adopción en lugar de percibirse solo como una obligación [16]. En una institución de educación superior canadiense, se documentó el paso de un modelo centrado en el cumplimiento hacia el codiseño con las personas usuarias [17]. Por su parte, la aplicación de métodos Lean UX en manufactura obtuvo una puntuación de usabilidad de 87,6 sobre 100 [18]. En conjunto, estos casos sugieren que integrar los requisitos desde el diseño puede ayudar a orientar la innovación, sin convertir el cumplimiento en una barrera.

E. Sincronización de variabilidades: técnica, organizacional y regulatoria

Los resultados señalan que la precisión [2], la interpretabilidad [13] y la usabilidad dentro de la organización [18] no necesariamente avanzan al mismo ritmo. En particular, un modelo más complejo no garantiza que sus decisiones sean más sencillas de explicar. Del mismo modo, el nivel de detalle técnico no asegura que el sistema responda a las necesidades del usuario final. Es más, una usabilidad medida favorablemente puede resultar insuficiente si se mantiene el escepticismo del liderazgo y las tres dimensiones no se coordinan entre ellas [11]. Por lo tanto, el marco conceptual propuesto busca relacionarlas desde la empatía con el usuario experto hasta la especificación de requisitos normativos. Así, se reconoce que ningún componente garantiza por sí solo la efectividad del sistema. En ese orden de ideas, su alineación contribuiría a una estrategia de prevención técnicamente sólida, viable para la organización y conforme con la normativa.

VI. PROPUESTA DE VALOR

Por lo general, los mecanismos para prevenir el fraude financiero se diseñan y evalúan individualmente. Los aspectos técnicos, organizacionales y normativos siguen caminos independientes, por lo que casi nunca se comprueba de forma integrada si una solución es precisa y fácil de adoptar antes de ponerla en funcionamiento [1, 2, 13, 15].

Debido a esta separación es que se dan los fallos preventivos recurrentes. Por un lado, existen modelos muy precisos que no logran generar confianza en las personas que deben utilizarlos [2, 13]. Por otro lado, las exigencias regulatorias suelen revisarse cuando la herramienta ya está construida, lo que genera costos adicionales [15, 16]. Para resolver estos problemas, se proponen tres cambios en el diseño de las estrategias preventivas.

El primer cambio consiste en exigir que todo modelo de detección cumpla un umbral de precisión y un nivel mínimo de explicabilidad verificado por un responsable designado. Así, la alineación entre las tareas de los analistas y los métodos de inteligencia artificial explicable, junto con la calibración de la confianza en los sistemas automatizados, pasarían de ser orientaciones de diseño a controles obligatorios y verificables [13, 14].

El segundo cambio se basa en la asignación de una unidad específica de la tarea de convertir cada obligación regulatoria aplicable en una condición de diseño comprobable desde el inicio. Así, el cumplimiento regulatorio se evalúa durante el desarrollo y no solo al final, tomando como referencia experiencias aplicadas en banca central y manufactura [15, 18].

Por último, se propone establecer un punto de control antes de llevar el sistema a producción. Ningún prototipo avanzaría sin la conformidad del comité de diseño, del responsable de explicabilidad y de la unidad de cumplimiento normativo. Con ello, las dimensiones técnica, organizacional y legal se evaluarían de forma conjunta y no como fases individuales [11, 18].

TABLA 5
MODELO VISUAL DE FRAMEWORK

Fase	Actividad central	Producto
Empatizar	Entrevistas con analistas, auditores, usuarios y cumplimiento	Mapa de necesidades y riesgos
Definir	Formular el problema de fraude y los requisitos regulatorios	Declaración integrada del problema
Idear	Generar soluciones técnicas y organizacionales	Alternativas de control
Prototipar	Construir interfaces, alertas y flujos de revisión	Prototipo antifraude
Probar	Evaluar precisión, explicabilidad, usabilidad y cumplimiento	Decisión de implementación
Aprender	Monitorear resultados y retroalimentar el diseño	Mejora continua

VII. CONCLUSIONES

El presente estudio buscó analizar cómo el design thinking contribuye a mejorar la efectividad y la adopción de las estrategias contra el fraude financiero. A partir de los hallazgos, se propone un marco que reúne desde el inicio aspectos que la literatura suele tratar de forma aislada. Entre ellos tenemos la necesidad de explicar los resultados de los algoritmos para generar confianza y la integración del cumplimiento normativo desde las fases de diseño.

En primer lugar, las fallas en las estrategias actuales no se deben a la falta de tecnología. La literatura muestra que las dimensiones cognitivas hasta la de red suelen abordarse por separado y sin alinearse claramente con los objetivos del sistema. Esta fragmentación explica el porqué de estos fallos de prevención aun cuando se utilizan herramientas técnicamente avanzadas.

En segundo lugar, la etapa inicial del design thinking, que incluye desde la fase de empatía hasta la ideación, permite integrar todos estos componentes en un solo diagnóstico. Aunque ningún estudio revisado aplicó estas etapas directamente al fraude financiero, las experiencias en áreas como salud móvil y tecnología financiera demuestran que esta integración es metodológicamente viable.

En tercer lugar, la viabilidad técnica no siempre avanza al mismo ritmo que la organizacional. Un modelo puede ser muy preciso para detectar fraudes, pero difícil de entender o de usar en las labores diarias. Por eso, la precisión, la explicabilidad y la usabilidad deben contemplarse desde el inicio del proceso, pues si se atienden al final, terminan tratándose como simples arreglos superficiales.

En cuarto lugar, la revisión permitió estructurar el "Marco de Prevención de Fraude Centrado en el Diseño", una propuesta que articula los factores técnicos, normativos y organizacionales. Su principal aporte es coordinar el diagnóstico, la definición de requisitos y la prueba de prototipos dentro de un mismo proceso, evitando que estas tareas se ejecuten de manera aislada o desconectada.

En su conjunto, los resultados sugieren que el design thinking permite pasar de una gestión del riesgo reactiva y fragmentada a un proceso de diseño integral. Sin embargo, al tratarse de un aporte conceptual proveniente de investigaciones en otros sectores, su verdadero valor dependerá de su validación en la práctica.

VIII. RECOMENDACIONES

Es importante que las organizaciones del sector financiero consideren integrar el marco de prevención de fraude centrado en el design thinking a sus procesos de innovación como forma de prevención. Para llevarlo a la práctica, podrían formar equipos multidisciplinarios con analistas de fraude, auditores, especialistas en cumplimiento y diseñadores. Así, el diagnóstico convergente, la especificación con doble criterio y el prototipado con doble validación se trabajarían de forma coordinada, en vez de quedar como fases separadas entre las áreas técnica, de negocio y de cumplimiento. Las tres etapas formarían parte de un procedimiento único, gestionado de manera conjunta.

Además, las organizaciones que desarrollan o adquieren sistemas de detección de fraude basados en inteligencia artificial deberían exigir, desde la etapa de definición de requisitos, metas de explicabilidad verificables junto con las metas de desempeño predictivo. De igual manera, es necesario invertir en programas de capacitación para que los analistas de fraude puedan interpretar las predicciones de estos sistemas y confiar en ellas. Estas medidas ayudarían a reducir la brecha entre la sofisticación técnica y la confianza operativa identificada en la revisión. Así se evitaría que modelos de alta precisión terminen subutilizados por falta de entendimiento.

De igual forma, también es necesario que las áreas de compliance formen parte del proceso desde un inicio. De esta forma, su contribución permitiría convertir los requisitos regulatorios en condiciones de diseño comprobables antes de invertir en el desarrollo completo de una solución. La aplicación de esto permitiría que las organizaciones puedan anticipar problemas normativos que, de otra forma, podrían detectarse cuando la solución técnica ya estuviera desarrollada.

Para futuras investigaciones, se recomienda validar empíricamente el marco propuesto en un caso real empresarial. También convendría ampliar la búsqueda bibliográfica en más bases de datos para no depender únicamente de estudios de acceso abierto y realizar estudios bajo contextos latinoamericanos aplicando un diseño cuasiexperimental con el objetivo de identificar cómo influye la explicabilidad en la adopción de herramientas contra el fraude. Finalmente, realizar estudios a largo plazo permitiría comprobar si los beneficios iniciales se mantienen a medida que cambian las modalidades de fraude financiero.

REFERENCIAS

[1] I. Putra, U. Sulistiyo, E. Diah, S. Rahayu and S. Hidayat, "The influence of internal audit, risk management, whistleblowing system and big data analytics on the financial crime behavior prevention," Cogent Economics & Finance, vol. 10, no. 1, Art. no. 2148363, 2022, doi: 10.1080/23322039.2022.2148363.

[2] N. A. Ahmed and F. Al-Turjman, "A stacking ensemble approach integrating XGBoost and deep neural networks with SMOTE for financial fraud detection," Journal of Advances in Information Technology, vol. 17, no. 5, pp. 884–894, 2026, doi: 10.12720/jait.17.5.884-894.

[3] P. Voorheis, A. Zhao, K. Kuluski, Q. Pham, T. Scott, P. Sztur, N. Khanna, M. Ibrahim and J. Petch, "Integrating behavioral science and design thinking to develop mobile health interventions: Systematic scoping review," JMIR mHealth and uHealth, vol. 10, no. 3, Art. no. e35799, 2022, doi: 10.2196/35799.

[4] A. F. Doni, Y. D. P. Negara, E. R. Wulandari and M. Z. Mustofa, "Redesign prototype of fintech application," E3S Web of Conferences, vol. 328, Art. no. 04002, 2021, doi: 10.1051/e3sconf/202132804002.

[5] M. Melazzini and G. Carella, "Nurture employees' creative behaviors: Unveiling the impact of design thinking on human organizational behavior," Proceedings of the Design Society, vol. 4, pp. 295–304, 2024, doi: 10.1017/pds.2024.32.

[6] L. Moura, A. Barcaui and R. Payer, "AI and financial fraud prevention: Mapping the trends and challenges through a bibliometric lens," Journal of Risk and Financial Management, vol. 18, no. 6, Art. no. 323, 2025, doi: 10.3390/jrfm18060323.

[7] F. Xu, A. Liu and X. Li, "Victimization mechanisms and countermeasures in telecom network fraud: A dual-system theoretical perspective," Frontiers in Psychology, vol. 16, Art. no. 1637935, 2025, doi: 10.3389/fpsyg.2025.1637935.

[8] J. Jin, H. Liu, Y. Han and A. Zhu, "Modeling strategies to protect investors from financial fraud collapses on social networks," International Journal of Modern Physics B, vol. 37, no. 2, Art. no. 2350014, 2023, doi: 10.1142/S0217979223500145.

[9] I. G. B. Sampaio, E. de Oliveira Andrade, S. de Souza Barbosa Fontes, F. C. Bernardini and J. Viterbo, "Trustworthy AI in public administration: The PRO-Trust pipeline for ethical fraud detection in public procurement," Government Information Quarterly, vol. 43, no. 3, Art. no. 102157, 2026, doi: 10.1016/j.giq.2026.102157.

[10] U. A. Usmani, A. Happonen and J. Watada, "Human-centered artificial intelligence: Designing for user empowerment and ethical considerations," in 2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), 2023, pp. 1–7, doi: 10.1109/HORA58378.2023.10156761.

[11] F. Demir, I. Saur-Amaral and D. F. Polónia, "Enabling innovation capabilities: A design thinking toolbox for SME strategic transformation," Administrative Sciences, vol. 15, no. 10, Art. no. 384, 2025, doi: 10.3390/admsci15100384.

[12] D. Minné, N. Conrad, T. S. Douglas and T. Mutsvangwa, "Negotiating boundaries: Framing and sense-making in a design thinking project with an elderly community," South African Journal of Higher Education, vol. 37, no. 1, pp. 243–265, 2023, doi: 10.20853/37-1-5678.

[13] D. Cirqueira, M. Helfert and M. Bezbradica, "Towards design principles for user-centric explainable AI in fraud detection," in Artificial Intelligence in HCI, Lecture Notes in Computer Science, vol. 12797, 2021, pp. 21–40, doi: 10.1007/978-3-030-77772-2_2.

[14] M. Naiseh, A. Simkute, B. Zieni, N. Jiang and R. Ali, "C-XAI: A conceptual framework for designing XAI tools that support trust calibration," Journal of Responsible Technology, vol. 17, Art. no. 100076, 2024, doi: 10.1016/j.jrt.2024.100076.

[15] P. Michalopoulos, O. Olowookere, N. Pocher, J. Sedlmeir, A. Veneris and P. Puri, "Privacy and compliance design options in offline central bank digital currencies," IEEE Transactions on Network and Service Management, vol. 22, no. 5, pp. 3748–3763, 2025, doi: 10.1109/TNSM.2025.3575367.

[16] F. J. Baumont De Oliveira, A. Fernandez, J. E. Hernández and M. del Pino, "Design thinking and compliance as drivers for decision support system adoption in agriculture," International Journal of Decision Support System Technology, vol. 15, no. 2, pp. 1–16, 2023, doi: 10.4018/IJDSST.315643.

[17] S. Crowe and A. Ghoneim, "From compliance to co-design: Transforming accommodation services at a Canadian college through a people-centred service design and change management approach," Canadian Journal of Higher Education, vol. 55, no. 4, pp. 148–166, 2025, doi: 10.47678/cjhe.v55i4.190519.

[18] L. A. Trujillo-Lopez, R. A. Raymundo-Guevara and J. C. Morales-Arevalo, "User-centered design of a computer vision system for monitoring PPE compliance in manufacturing," Computers, vol. 14, no. 8, Art. no. 312, 2025, doi: 10.3390/computers14080312.

[19] L. Puri, A. Kumar and R. Singh, "What drives or discourages fraud-safe behavior in digital transactions? A BRT perspective," Acta Psychologica, vol. 260, Art. no. 105675, 2025, doi: 10.1016/j.actpsy.2025.105675.

[20] D. Cirqueira, D. Nedbal, M. Helfert and M. Bezbradica, "Scenario-based requirements elicitation for user-centric explainable AI: A case in fraud detection," in Machine Learning and Knowledge Extraction, Lecture Notes in Computer Science, vol. 12279, 2020, pp. 321–341, doi: 10.1007/978-3-030-57321-8_18.

[21] E. Mill, W. Garn and C. Turner, "Real-world efficacy of explainable artificial intelligence using the SAGE framework and scenario-based design," Applied Artificial Intelligence, vol. 38, no. 1, Art. no. 2430867, 2024, doi: 10.1080/08839514.2024.2430867.

[22] S. Hong and W. Park, "Developing user-centered system design guidelines for explainable AI: A systematic literature review," Artificial Intelligence Review, vol. 58, no. 12, Art. no. 386, 2025, doi: 10.1007/s10462-025-11363-y.

[23] J. B. Vega Criollo, D. M. Anticona-Valderrama and J. B. Chumpe Agesto, "Sentiment analysis as a management tool: a systematic review," *Proceedings of the LACCEI International Multi-Conference for Engineering, Education and Technology*, 2025, doi: 10.18687/LEIRD2025.1.1.1053.

[24] J. Černevičienė and A. Kabašinskas, "Explainable artificial intelligence (XAI) in finance: a systematic literature review," Artificial Intelligence Review, vol. 57, Art. no. 216, 2024, doi: 10.1007/s10462-024-10854-8

[25] Y. Zhou, H. Li, Z. Xiao and J. Qiu, "A user-centered explainable artificial intelligence approach for financial fraud detection," Finance Research Letters, vol. 58, Part A, Art. no. 104309, 2023, doi: 10.1016/j.frl.2023.104309.