INTEGRACIÓN

DE LA INTELIGENCIA ARTIFICIAL EN LOS SISTEMAS DE CONTROL INTERNO DE LAS ORGANIZACIONES

REVISTA UGC | Revista científica de la Universidad del Golfo de California
Volumen 3 | S2 | Junio - 2025

INTEGRATION OF ARTIFICIAL INTELLIGENCE IN THE INTERNAL CONTROL SYSTEMS OF ORGANIZATIONS

Johana Natali Quintuña-Quintuña[1]
E-mail: johana.quintuna.95@est.ucacue.edu.ec
ORCID: https://orcid.org/0009-0004-1935-1537
Verónica Paulina Moreno-Narváez[1]
E-mail: veronica.moreno@ucacue.edu.ec
ORCID: https://orcid.org/0000-0002-6137-2460
[1] Universidad Católica de Cuenca. Ecuador.

Cita sugerida (APA, séptima edición)

Quintuña-Quintuña, J. N., & Moreno-Narváez, V. P. (2025). Integración de la inteligencia artificial en los sistemas de control interno de las organizaciones. *Revista UGC, 3(S2), 261-272.*

Fecha de presentación: 13/04/2025 **Fecha de aceptación:** 09/05/2025 **Fecha de publicación:** 01/06/2025

RESUMEN

La auditoría moderna ha incorporado herramientas de inteligencia artificial (IA) y aprendizaje automático (ML) para mejorar la detección de fraudes y la gestión de riesgos. Sin embargo, en las pequeñas y medianas empresas (PYMES) de Guayaquil, la adopción de estas tecnologías es limitada. Por ello, este estudio tiene como objetivo diseñar estrategias que integren la inteligencia artificial en los sistemas de control para la detección de fraudes en las PYMES de la ciudad de Guayaquil. Se empleó un enfoque mixto con un diseño correlacional y transversal. Los resultados revelan que el fraude financiero es el más recurrente en las PYMES analizadas. Los principales obstáculos para la implementación de IA y ML incluyen la falta de conocimientos técnicos, la dificultad de integración con sistemas existentes y la ausencia de datos de calidad. Estos hallazgos evidencian la necesidad de estrategias que aborden estas barreras para facilitar la adopción efectiva de tecnologías avanzadas en la gestión de riesgos.

Palabras clave:

Inteligencia artificial, auditoria, gestión de riesgos, fraude, automatización.

ABSTRACT

Modern auditing has incorporated artificial intelligence (AI) and machine learning (ML) tools to improve fraud detection and risk management. However, in small and medium-sized enterprises (SMEs) in Guayaquil, the adoption of these technologies is limited. Therefore, this study aims to design strategies that integrate artificial intelligence into control systems for fraud detection in SMEs in the city of Guayaquil. A mixed approach with a correlational and cross-sectional design was used. The results reveal that financial fraud is the most recurrent in the SMEs analyzed. The main obstacles to the implementation of AI and ML include lack of technical knowledge, difficulty of integration with existing systems, and lack of quality data. These findings highlight the need for strategies that address these barriers to facilitate the effective adoption of advanced technologies in risk management.

Keywords:

Artificial intelligence, auditing, risk management, fraud, automation.

INTRODUCCIÓN

La integración de la inteligencia artificial (IA) en los sistemas de control interno de las organizaciones es una tendencia global que busca fortalecer la transparencia y la eficiencia en la gestión de riesgos. A medida que las empresas enfrentan desafíos cada vez más complejos en términos de seguridad financiera y cumplimiento normativo, la adopción de soluciones basadas en IA se ha convertido en un factor necesario para optimizar la detección de irregularidades y mejorar la toma de decisiones.

En Europa, los fraudes en las pequeñas y medianas empresas (PYMES) representan un desafío, sobre todo en el manejo tributario del impuesto al valor agregado (IVA) y la gestión de fondos europeos. Según la Fiscalía Europea, el fraude relacionado con el IVA es una práctica común e involucra esquemas como el uso indebido de operadores intracomunitarios y la presentación de declaraciones falsas.

Asimismo, los fondos destinados a iniciativas como NextGenerationEU son blanco de irregularidades, incluyendo malversación de fondos, blanqueo de capitales y gastos ajenos a los contratos públicos. Los contratos públicos, por su parte, suelen ser manipulados a través de prácticas corruptas y alteraciones en los procesos de licitación para desviar recursos hacia intereses privados o redes delictivas.

El blanqueo de capitales, vinculado a estos delitos, se basa en estructuras complejas diseñadas para ocultar el origen ilícito de los fondos. Los grupos delictivos operan a nivel transnacional, aprovechando vacíos legales y trasladando sus actividades a jurisdicciones más permisivas (Oficina de Publicaciones de la Unión Europea, 2024).

La Fiscalía Europea ha fortalecido sus capacidades de detección gracias al incremento de denuncias por parte de particulares y autoridades nacionales. No obstante, las instituciones de la Unión Europea tienen un margen de mejora en la identificación de irregularidades. Las investigaciones se enfocan en la recuperación de activos y el procesamiento penal de los responsables, aplicando medidas preventivas como el embargo de bienes. Este esfuerzo busca mitigar el impacto económico, y frenar la influencia de grupos delictivos organizados, que consideran estas actividades de bajo riesgo y alta rentabilidad en las PYMES (Unión Europea, 2024).

En Latinoamérica, las PYMES enfrentan fraudes que ponen en riesgo su sostenibilidad y operaciones. Entre los más frecuentes se encuentra la malversación de fondos, donde empleados o directivos desvían recursos mediante la falsificación de facturas o la manipulación de registros contables para encubrir actividades ilícitas y obtener beneficios indebidos. El lavado de dinero da lugar a ocultar fondos ilegales e integrarlos en la economía formal, mientras que la evasión fiscal se basa en la declaración falsa de ingresos para evitar el pago de impuestos, afectando los recursos del Estado. Asimismo, la corrupción y el soborno erosionan la integridad empresarial, facilitando la obtención de contratos y beneficios ilícitos.

En la ciudad de Guayaquil, Ecuador, las PYMES enfrentan múltiples riesgos que amenazan su estabilidad y crecimiento. Uno de los fraudes más frecuentes es la manipulación de información financiera, donde empleados alteran registros contables para ocultar pérdidas o inflar ingresos. De forma paralela se registra el desvío de fondos mediante transacciones fraudulentas o la creación de cuentas ficticias. Otro problema recurrente es la gestión irregular de inventarios, en la que los empleados manipulan los niveles de existencia para encubrir robos o pérdidas. Se suma a esta realidad, el fraude en la facturación que consistente en la emisión de facturas por productos o servicios inexistentes, lo cual facilita la apropiación indebida de recursos. En varios casos, estos fraudes están vinculados a actos de corrupción, como sobornos o pagos a intermediarios ficticios, lo que agrava la situación financiera y reputacional de las empresas (Barriga et al., 2023).

Más allá de los fraudes internos, las PYMES en Guayaquil, por otro lado, enfrentan riesgos derivados de la transformación digital. La adopción de inteligencia artificial y nuevas tecnologías presenta desafíos notables, como la necesidad de realizar inversiones en infraestructura tecnológica, gestionar grandes volúmenes de datos con altos estándares de seguridad y privacidad, y transformar la fuerza laboral mediante la capacitación en nuevas competencias. Si bien la automatización puede optimizar procesos y mejorar la eficiencia, asimismo conlleva la eliminación de ciertas funciones laborales, lo que impacta en el empleo. Frente a estos retos, las empresas deben evaluar con cuidado los costos y beneficios para garantizar que la implementación de estas tecnologías sea sostenible y aporte valor a largo plazo (Tenes, 2023).

Sobre la base de los antecedentes expuestos, se plantea el siguiente problema de investigación: ¿cómo mejorar la detección de fraudes en las PYMES de la ciudad de Guayaquil? Por ello, el objetivo es diseñar estrategias que integren la inteligencia artificial en los sistemas de control para la detección de fraudes en las PYMES de la ciudad de Guayaquil.

Los softwares de análisis de datos, como ***Audit Command Language*** (ACL), ***Interactive Data Extraction and Analysis*** (IDEA) y T***ableau*** son esenciales en la auditoría moderna, porque facultan examinar grandes volúmenes de información para detectar patrones, anomalías y riesgos. ACL, por ejemplo, es un software especializado en procesar datos masivos, identificado por su capacidad para realizar auditorías continuas y evaluaciones de riesgos. A su vez, el software IDEA está diseñado para la extracción y análisis interactivo de datos, facilitando pruebas sustantivas, identificación de duplicados, validación de cálculos y evaluación de tendencias financieras y operativas. De

igual forma, ***Tableau***, es una herramienta que transforma datos complejos en gráficos interactivos y paneles dinámicos, mejorando la comunicación de hallazgos de manera visual e intuitiva (Instituto de Auditores Internos de España, 2023).

Así mismo, la aplicación de herramientas tecnológicas ha transformado el trabajo de los auditores, permitiéndoles mejorar la detección de fraudes y optimizar sus análisis. Modelos de ***Machine Learning*** (ML), como regresiones, árboles de decisión y redes neuronales, facilitan la identificación de patrones irregulares y la predicción de comportamientos anómalos. Por su parte, la Automatización de Procesos Robóticos (RPA) contribuye a reducir la carga de tareas repetitivas, lo que permite a los auditores enfocarse en actividades estratégicas. El análisis predictivo y los sistemas de detección de anomalías, impulsados por Inteligencia Artificial, fortalecen la capacidad de anticipar riesgos y detectar irregularidades en tiempo real (Instituto de Auditores Internos de España, 2023).

Estas innovaciones tecnológicas, que han transformado la auditoría, son reflejo de un cambio más amplio en la dinámica empresarial global, en particular durante la pandemia de COVID-19. Este evento histórico aceleró cambios considerables en los modelos de negocio, marcados por cinco tendencias que redefinieron la forma de operar de las empresas. La digitalización y el uso de tecnología se convirtieron en una prioridad, acelerando la adopción de herramientas como el teletrabajo, el comercio electrónico y la inteligencia artificial. Este impulso tecnológico permitió a las organizaciones adaptarse con eficacia a las nuevas condiciones del mercado, ajustando productos y servicios para alinearse con las restricciones de proximidad física y un mayor énfasis en la higiene y la seguridad (García et al., 2021).

Este mismo contexto, la agilidad organizacional surgió como una capacidad esencial, permitiendo a las empresas responder de manera rápida a los cambios del entorno y explorar nuevas oportunidades de mercado. Al mismo tiempo, la evolución en las interacciones con los clientes, impulsadas por el distanciamiento social, llevó a la creación de experiencias personalizadas y seguras, respaldadas por tecnologías innovadoras. Estas tendencias evidencian cómo el entorno pospandemia está moldeando la manera en que las empresas gestionan sus operaciones y enfrentan desafíos, tanto en la auditoría como en otros aspectos estratégicos de su funcionamiento (García et al., 2021).

Al respecto, la inteligencia artificial (IA) mejora la auditoría al validar grandes volúmenes de información con mayor calidad y precisión en menos tiempo, garantizando decisiones basadas en datos confiables. Automatiza tareas repetitivas, detecta errores y optimiza procesos, incrementando la eficiencia operativa. A la vez, reduce el tiempo requerido para auditorías, permitiendo a los auditores enfocarse en actividades estratégicas. Es esencial en la prevención de fraudes y gestión de riesgos, al identificar patrones de posibles irregularidades. Proporciona información precisa y oportuna, mejorando la toma de decisiones. En la planificación, facilita juicios de materialidad, minimizando riesgos y aumentando la efectividad general en un entorno empresarial dinámico (Erazo & De la A, 2023).

Asimismo, estas tecnologías optimizan procesos como el análisis de grandes volúmenes de datos para identificar patrones y riesgos, la automatización de tareas repetitivas y la evaluación predictiva de riesgos basada en datos históricos. Las herramientas de ML, como algoritmos de clasificación y regresión, dan lugar a detectar fraudes o anomalías y personalizar estrategias de auditoría según las necesidades específicas de las organizaciones. Por su parte, los sistemas de procesamiento de lenguaje natural (NLP) pueden ser empleados para analizar documentación masiva, simplificando la búsqueda de información relevante y apoyando en la generación de informes automatizados, y las plataformas de visualización de datos facilitan la interpretación y presentación de resultados de análisis de manera comprensible para las partes interesadas, contribuyendo a la toma de decisiones informadas (Calle et al., 2024).

Este orden de ideas, la inteligencia artificial (IA) mejora la eficiencia de los sistemas de control interno en las PYMES al abordar aspectos primordiales de su funcionamiento. Facilita la detección precisa y proactiva de riesgos, lo que faculta adoptar medidas correctivas oportunas. Al automatizar tareas repetitivas, reduce los errores humanos y mejora la consistencia en los controles. De igual manera, su capacidad para ofrecer monitoreo continuo en tiempo real consciente una evaluación y reacción inmediata ante desviaciones, optimizando recursos y reduciendo costos. Esto, a su vez, garantiza un acceso rápido y preciso a la información financiera necesaria para la toma de decisiones estratégicas, lo que fortalece la confianza en los procesos operativos y la calidad de los informes financieros, esenciales para la sostenibilidad empresarial.

La efectividad de este sistema depende de un diseño adecuado, de su alineación con los objetivos estratégicos de la empresa y de la capacitación del personal, lo que ayuda a mejorar la competitividad (Rivas, 2022). En un contexto más amplio, las empresas han integrado diversas herramientas de IA para fortalecer la detección y prevención de fraudes, logrando así una mayor transparencia y seguridad en sus operaciones financieras. El análisis avanzado de datos posibilita examinar grandes volúmenes de información, lo que facilita la identificación de tendencias y anomalías a través de técnicas como el análisis de varianza y la comparación de patrones históricos.

Los sistemas de detección de anomalías monitorean las transacciones en tiempo real, detectando comportamientos inusuales que podrían indicar actividades

fraudulentas. La automatización de procesos robóticos (RPA) es primordial al optimizar tareas repetitivas, permitiendo que los equipos se concentren en áreas de mayor riesgo. Al mismo tiempo, los softwares de reconocimiento de patrones y los sistemas de alerta temprana detectan señales de posibles irregularidades en los datos, fortaleciendo así la capacidad preventiva de las empresas (Valladares & Ordoñez, 2024). Un ejemplo destacado de la aplicación de inteligencia artificial (IA) en la prevención de fraudes es Kushki, una empresa fintech ecuatoriana fundada en 2016, especializada en pagos electrónicos. Kushki ha implementado tecnologías avanzadas de IA y aprendizaje automático para analizar grandes volúmenes de datos y detectar patrones de comportamiento sospechosos en tiempo real, lo que permite identificar y prevenir transacciones fraudulentas de manera eficiente. Además, la empresa utiliza técnicas como la biometría y la verificación de identidad para fortalecer la seguridad en las transacciones digitales. Estas innovaciones han posicionado a Kushki como un referente en la industria de pagos electrónicos en América Latina.

El sistema evalúa cada transacción procesada, considerando aspectos como el historial de transacciones del usuario, la geolocalización y el comportamiento del consumidor. Cuando se identifica una anomalía que se desvía de los patrones normales, el sistema bloquea de forma automática la transacción sospechosa y genera una alerta para que el equipo de seguridad de Kushki la revise. Este enfoque protege a los consumidores, y al mismo tiempo refuerza la reputación de Kushki como un proveedor confiable de servicios de pago seguro. Incluso, Kushki Shield se entrena de forma continua con datos de transacciones reales, lo que mejora su efectividad con el tiempo (Jara & Naspud, 2024).

El fraude empresarial consiste en cualquier acto intencional y deliberado destinado a engañar a una persona, empresa u organización para obtener una ventaja injusta, perjudicando derechos o intereses legítimos. Estas prácticas abarcan una amplia gama de acciones, como la manipulación de estados financieros, la malversación de fondos, la falsificación de documentos y otras conductas desleales diseñadas para privar a terceros de dinero o propiedades mediante engaños. Los responsables pueden ser miembros internos de una organización, agentes externos o incluso actores colaborativos entre diferentes entidades jurídicas (Tantalean, 2022).

El objetivo principal suele ser obtener beneficios personales, corporativos o para terceros, ignorando las implicaciones legales y éticas. Este tipo de fraudes afecta la confianza entre las partes involucradas, pone en riesgo la estabilidad económica y la reputación de las organizaciones. Para combatirlos, es básico implementar controles internos robustos, realizar auditorías frecuentes y fomentar una cultura ética basada en la transparencia y la rendición de cuentas (Tantalean, 2022). Los fraudes en entornos empresariales se clasifican en tres categorías: corrupción, fraude en estados financieros y apropiación indebida de activos. La corrupción ocurre cuando empleados utilizan su influencia de manera indebida para obtener beneficios personales, como en casos de sobornos o extorsión.

El fraude en estados financieros implica la manipulación de información contable con el propósito de presentar una situación económica irreal, ejemplos de esto son la sobrevaloración de activos o el registro ficticio de ingresos. La apropiación indebida de activos se refiere a la sustracción o uso no autorizado de recursos empresariales para beneficio personal, incluyendo esquemas como desvíos de fondos mediante recibos falsos, robo de bienes o alteración de cheques, aunque los hechos de corrupción son menos frecuentes, en ocasiones suelen ser los más costosos (Lisicki Litvin & Asociados, 2020).

En las PYMES, la detección de fraudes es esencial para proteger su integridad financiera, y para ello se utilizan diversos métodos que combinados pueden ser altos efectivos. La verificación de documentos asegura que facturas y otros registros cumplan con los requisitos tributarios y que los proveedores sean legítimos, evitando tratar con empresas ficticias. El control de inventario, mediante el registro y monitoreo de los movimientos, garantiza que los productos ingresen y salgan según lo reportado. Las auditorías internas permiten evaluar de forma oportuna la eficacia de los controles internos y detectar irregularidades en las transacciones financieras. La supervisión y segregación de funciones, al dividir responsabilidades entre empleados y aumentar la vigilancia en áreas críticas como compras y contabilidad, reduce la mayor parte de las oportunidades de fraude (Chiriguaya & Mejia, 2022).

Un riguroso registro de transacciones, incluyendo la documentación de gastos y el control de fondos menores, facilita la identificación de actividades sospechosas. Del mismo modo, el análisis de transacciones puede revelar patrones de gastos inusuales que indican posibles irregularidades. La capacitación y concienciación del personal en ética empresarial y riesgos de fraude fomenta un ambiente donde se reportan conductas sospechosas. La implementación de políticas de control interno y protocolos claros para la gestión de compras y pagos mitiga los riesgos asociados (Chiriguaya & Mejia, 2022).

MATERIALES Y MÉTODOS

La investigación se diseñó con un enfoque metodológico riguroso, conforme a principios sistemáticos para analizar fenómenos en su contexto natural, tal como propone los trabajos de Hernández y Mendoza (2018).

Se adoptó un diseño no experimental, lo que permitió estudiar las variables sin intervenir en su entorno, garantizando así una observación objetiva y precisa. Este enfoque fue complementado con una metodología mixta,

en la que se combinó el análisis cuantitativo con la investigación cualitativa, favoreciendo una comprensión amplia del fenómeno en estudio. Mientras que las herramientas cuantitativas proporcionaron datos objetivos, las entrevistas y análisis descriptivos ofrecieron una visión más profunda y contextualizada.

El diseño transeccional, utilizado en el estudio, permitió obtener datos en un solo momento temporal, lo que brindó una representación precisa y actual de la situación de las PYMES en Guayaquil. Al centrarse en las interacciones y la incidencia de las variables críticas en el contexto de los sistemas de control interno, se logró una evaluación de la problemática sin alterar las condiciones previas. Este diseño fue adecuado para describir y evaluar de manera puntual los procesos y sistemas en funcionamiento dentro de estas empresas. El enfoque descriptivo y explicativo de la investigación permitió detallar el uso de tecnologías como la inteligencia artificial y el machine learning en la mejora de la gestión de riesgos dentro de las PYMES de Guayaquil.

Mediante análisis estadísticos, se exploraron las aplicaciones y los impactos de estas tecnologías, destacando su rol en la automatización de procesos, la mejora en la detección de fraudes y la optimización de los controles internos, ofreciendo una visión integral sobre la eficiencia y efectividad de las prácticas empresariales en el contexto local.

Se emplearon los métodos histórico-lógico, analítico-sintético y sistemático para estructurar y contextualizar los datos. Los métodos histórico-lógico permitió ubicar los datos en su evolución temporal, facilitando la comprensión de cómo las prácticas de detección de fraudes en las PYMES de Guayaquil han cambiado. Por su parte, los métodos analítico-sintético y sistemático ayudaron a descomponer y organizar la información, asegurando la coherencia y precisión del análisis.

En la recolección de datos, se utilizó una encuesta estructurada que permitió conocer la percepción de los profesionales en áreas contables, financieras y de auditoría que laboran en las PYMES de Guayaquil sobre el uso de herramientas tecnológicas para la detección de fraudes. El cuestionario, compuesto por 22 ítems, proporcionó información relevante sobre el impacto de estas herramientas en los sistemas de control interno.

En lo que respecta al universo de estudio, se desconoce el número exacto de pequeñas y medianas empresas (PYMES) en Guayaquil, ya que el Instituto Nacional de Estadística y Censos (2022), no proporciona cifras específicas para esta ciudad. Sin embargo, según el Registro Estadístico de Empresas (REEM), en 2022 existían 1.239.822 empresas activas en Ecuador. De estas, el 92,4% eran microempresas y el 7,4% pequeñas empresas. Aunque no se dispone de datos precisos para Guayaquil, se estima que una proporción significativa de estas PYMES opera en la ciudad.

Para la selección de los participantes en el estudio, se empleó un muestreo por conveniencia, eligiendo 37 PYMES ubicadas en Guayaquil. El análisis de los datos obtenidos se realizó utilizando el software estadístico JASP, que facilitó la ejecución de análisis descriptivos. Esto permitió identificar patrones y relaciones relevantes en los datos, así como generar representaciones gráficas que contribuyeron a la interpretación y comunicación efectiva de los resultados.

RESULTADOS Y DISCUSIÓN

A continuación, se presentan los resultados obtenidos en el estudio, los cuales han sido procesados y analizados de manera detallada para ofrecer una visión clara y precisa de las variables estudiadas, así como las relaciones y patrones identificados

Cargos: En el análisis de las empresas encuestadas, se identificó que el cargo más frecuente es otro, representando el 43,24% del total. Esto sugiere una diversidad de funciones que no se ajustan a las categorías específicas predefinidas. El segundo cargo más común es el de contador, con un 35,14%. Los cargos de auditor y director financiero tienen una representación equivalente del 8,11% cada uno. El cargo de asesor financiero es el menos frecuente, correspondiendo al 5,41% de los encuestados.

Nivel de conocimiento sobre herramientas de IA y ML: la mayoría, representada por el 40.54% declara un nivel de conocimiento medio sobre herramientas de IA y ML. El 29.73% reporta un nivel bajo, mientras que un 13.51% indica tener un conocimiento alto. Por otro lado, el 10.81% afirma no tener ningún conocimiento sobre estas herramientas, y solo el 5.41% manifiesta tener un conocimiento muy alto. Estos datos apuntan que, si bien existe cierto grado de familiaridad con estas tecnologías, los niveles avanzados de conocimiento son poco comunes entre los encuestados.

El nivel de adopción de herramientas de IA o ML: el nivel de adopción de herramientas de inteligencia artificial (IA) o aprendizaje automático (ML) en las empresas encuestadas muestra un avance moderado, con una tendencia hacia una posible mayor implementación en el futuro. Según los datos presentados en la figura 1, el 37.84% de las empresas no utiliza a la actualidad estas herramientas, mientras que un 35.14% no las ha implementado, más si tiene la intención de hacerlo. El 16.22% las emplea de manera limitada, y solo un 10.81% ha adoptado estas tecnologías de forma extensiva.

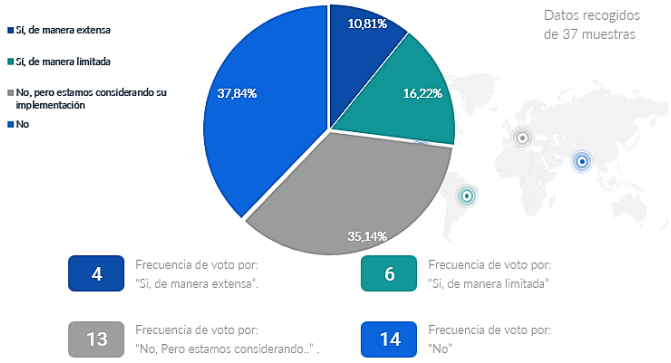

Figura 1. Herramientas de inteligencia artificial en los sistemas de control interno.

El 27.03% de las empresas usa IA en control interno, el 35.14% planea implementarla y el 37.84% no la utiliza.

Tipos de algoritmos son más útiles para la detección de fraudes: el conocimiento sobre los tipos de algoritmos más útiles para la detección de fraudes en las empresas encuestadas es limitado, lo que podría representar un obstáculo para la implementación efectiva de estas tecnologías. Según los datos obtenidos, el 56.76% de los encuestados no está seguro sobre qué tipo de algoritmos resultan más adecuados, lo que evidencia una falta de conocimiento generalizado en este ámbito.

Entre quienes identifican alguna preferencia, el 16.22% considera que los algoritmos supervisados, como la regresión o los árboles de decisión, son los más útiles, mientras que un porcentaje igual (16.22%) menciona las redes neuronales profundas. Por otro lado, el 10.81% destaca la utilidad de los algoritmos no supervisados, como el *clustering* o la detección de anomalías.

IA/ML vs. métodos tradicionales detección de fraudes: la figura 2 refleja una percepción es su mayoría favorable hacia el uso de inteligencia artificial (IA) y aprendizaje automático (ML) en la detección de fraudes en comparación con los métodos tradicionales. Un 48.65% de los encuestados considera que estas herramientas son algo más eficientes, mientras que un 24.32% las califica como más eficientes. Otro 24.32% opina que su desempeño es similar al de los métodos convencionales, y solo un 2.70% cree que son menos eficientes.

Se evidencia una tendencia positiva hacia la adopción de IA y ML en la detección de fraudes, lo que demuestra que las empresas reconocen su potencial para mejorar la identificación de anomalías y minimizar riesgos. No obstante, la proporción de encuestados que perciben una eficiencia similar a la de los métodos tradicionales indica la necesidad de mayor información y evidencia empírica sobre los beneficios concretos de estas tecnologías en el ámbito empresarial.

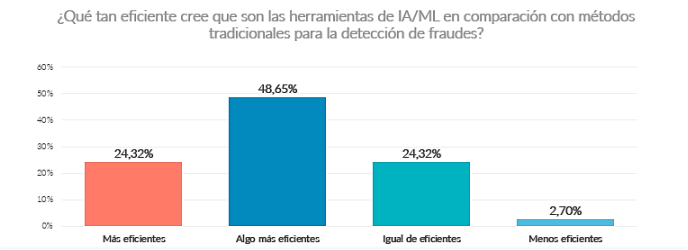

Figura 2. La eficiencia de las herramientas de IA/ML con los métodos tradicionales en la detección de fraudes.

El 72.97% cree que las herramientas de IA/ML son más eficientes que los métodos tradicionales, mientras que el 24.32% las considera igual de eficientes y el 2.70% menos eficientes.

Desafíos empresariales en implementación de IA/ML: los principales desafíos que enfrentan las empresas en la implementación de inteligencia artificial (IA) y aprendizaje automático (ML) están relacionados con factores técnicos, operativos y financieros.

Según los datos presentados en la tabla 1, la falta de conocimientos técnicos es el obstáculo más destacado, señalado por el 35.14% de los encuestados. Esto indica que la escasez de personal capacitado y la falta de formación en estas tecnologías representan una barrera importante para su adopción. en segundo lugar, el 27.03% identifica la integración con los sistemas actuales como un desafío determinante, lo que indica posibles dificultades en la compatibilidad tecnológica y en la adaptación de procesos empresariales a nuevas herramientas basadas en IA/ML.

Por otro lado, tanto el alto costo de implementación como la resistencia al cambio son percibidos como barreras por el 18.92% de los encuestados. Estos resultados reflejan que, aun cuando existiendo la necesidad de conocimientos técnicos, los factores económicos y la disposición organizacional influyen en la adopción de estas tecnologías.

Tabla 1. Principales desafíos en la implementación de IA/ML en la empresa.

Opciones	Frecuencia	Porcentaje
Falta de conocimientos técnicos	13	35.14
Alto costo de implementación	7	18.92
Integración con sistemas actuales	10	27.03
Resistencia al cambio	7	18.92
Total	37	100

Los desafíos para implementar IA/ML son falta de conocimientos, integración, costo y resistencia al cambio.

Procesos importantes para automatización con IA/ML: los procesos empresariales identificados como prioritarios para la automatización con inteligencia artificial (IA)

y aprendizaje automático (ML) están muy ligados a la eficiencia financiera y al fortalecimiento del control interno.

Según los datos obtenidos, la generación de informes financieros es el proceso más destacado, con un 29.73% de las respuestas, lo que demuestra que las empresas buscan agilizar la elaboración y precisión de sus reportes contables. Las auditorías internas y la evaluación de riesgos son igual de relevantes, cada una mencionada por el 24.32% de los encuestados. Esto indica una necesidad de optimizar la identificación de inconsistencias y mejorar la supervisión del cumplimiento normativo. En contraste, el monitoreo de transacciones es considerado un proceso por el 21.62%, lo que refleja la importancia de detectar anomalías en tiempo real y fortalecer la seguridad en las operaciones financieras.

Impacto de IA/ML en gestión de riesgos: el impacto de la IA y el aprendizaje ML en la gestión de riesgos es reconocido en el ámbito empresarial, con una percepción positiva sobre su potencial para fortalecer los procesos de control y toma de decisiones. Según los datos presentados en la tabla 2, el 70.27% de los encuestados considera que su impacto es relevante, lo que dice que estas tecnologías están siendo vistas como herramientas para mejorar la identificación y mitigación de riesgos.

Mientras, el 16.22% califica su impacto como transformador, lo que indica que un segmento de las empresas reconoce su utilidad, e incluso anticipa cambios sustanciales en la forma en que se gestionan los riesgos. En cambio, un 10.81% percibe un impacto moderado, lo que podría reflejar una adopción parcial o desafíos en la implementación. Solo el 2.70% considera que estas tecnologías tienen un impacto insignificante, lo que explica una baja resistencia a su uso en este sentido.

Tabla 2. Impacto de la implementación de IA/ML en la gestión de riesgos en su empresa.

Respuestas	Frecuencia	Porcentaje
Transformador	6	16.22
Significativo	26	70.27
Moderado	4	10.81
Insignificante	1	2.70
Total	37	100

Los resultados muestran que la implementación de IA/ML ha transformado de manera notable la gestión de riesgos empresariales.

Frecuencia de problemas de fraude en empresas: la frecuencia de problemas de fraude en las empresas encuestadas muestra que, a pesar de que no es un problema recurrente para la mayoría, sigue siendo una preocupación latente.

Según los datos recopilados, el 51.35% de las empresas indica que estos incidentes ocurren rara vez, mientras que un 21.62% asegura no haber enfrentado problemas de fraude. El 16.22% menciona que el fraude ocurre de modo eventual, y un 10.81% señala que enfrenta estos problemas con frecuencia.

Fraudes más comunes según empresas encuestadas: los fraudes más habituales identificados por las empresas encuestadas reflejan una mayor incidencia en el ámbito financiero, seguido de riesgos internos y tecnológicos.

El fraude financiero es el más frecuente, señalado por el 54.05% de los encuestados, lo que lo posiciona como el principal problema en las organizaciones. En segundo lugar, el fraude interno es mencionado por el 21.62%, lo que demuestra que las irregularidades en la empresa, como la malversación de fondos o la manipulación de registros, representan una preocupación. El fraude cibernético ocupa el tercer lugar, reportado por el 13.51% de las empresas, lo que destaca los riesgos asociados a la digitalización y a la seguridad de la información. Por último, un 10.81% menciona otros tipos de fraude.

Precisión en detección de fraudes empresariales: la precisión en la detección de fraudes empresariales es considerada un factor decisivo para la mayoría de las empresas encuestadas. Según los datos, el 59.46% de los encuestados considera que la precisión es muy importante, lo que resalta su relevancia en la identificación y mitigación de riesgos. Un 27.03% la califica como importante, lo que indica que, aunque se reconoce su valor, no es vista como un aspecto prioritario en todos los casos. Solo un 8.11% la define como crítica, es decir, para algunas empresas, la precisión no es la prioridad máxima en sus sistemas de detección de fraudes. Un 5.41% percibe la precisión como poco importante, lo que representa una pequeña fracción que tal vez subestima su impacto.

Integración de detección de fraudes con sistemas: la integración de la detección de fraudes con los sistemas existentes es considerada un aspecto importante por la mayoría de las empresas encuestadas, como se refleja en los datos presentados en la figura 3. Un 51.35% de los encuestados considera que esta integración es algo relevante, mientras que un 35.14% la califica como muy relevante, destacando su importancia en la mejora de los procesos de control y prevención de fraudes. Solo un 10.81% percibe esta integración como poco relevante, y un 2.70% la considera irrelevante, lo que indica que una pequeña fracción de empresas no otorga prioridad a la integración de sus sistemas de detección de fraudes.

Sistema de control interno con tecnologías emergentes para mejorar la detección de riesgos en las PYMES de Guayaquil

El sistema propuesto está diseñado para permitir que las PYMES de Guayaquil optimicen el control de sus operaciones administrativas, contables y financieras, utilizando tecnologías emergentes que faciliten la detección temprana de riesgos y una actuación precisa ante posibles

amenazas. A diferencia de otros enfoques más teóricos, esta propuesta se basa en una estructura práctica, compuesta por cinco componentes interconectados que actúan como una red de protección interna. Estos componentes se alinean con el modelo COSO de control interno, adaptado para las PYMES (ver Figura 3), y son los siguientes: la creación de un ambiente de control sólido, la evaluación y mitigación de riesgos operativos y financieros, la implementación de actividades de control efectivas, la gestión eficiente de los sistemas de información y comunicación, y la actividad de supervisión constante para asegurar la efectividad del sistema.

Figura 3. Componentes del control interno según COSO.

Un sistema robusto integra ética, análisis, procedimientos, comunicación y supervisión constante.

Componente 1: Ambiente de control

El Ambiente de Control es la base sobre la cual se construye todo el sistema de control interno en las organizaciones, y en el caso de las PYMES de Guayaquil, este componente es determinante para establecer la cultura empresarial, los valores éticos, la estructura operativa y el compromiso de la alta dirección con la transparencia y la eficiencia. En la tabla 3, se presentan los principales elementos del ambiente de control, donde se detalla su descripción, y aplicación práctica, en el uso de tecnologías emergentes como el chatbot con inteligencia artificial en WhatsApp Business, esta herramienta se implementa de forma práctica para mejorar la estructura organizativa, la gestión del talento humano y la difusión de la ética empresarial.

Tabla 3. Aplicación de Chatbot con IA en WhatsApp Business en el Ambiente de Control – PYMES de Guayaquil.

Elementos	Definición para PYMES de Guayaquil	Aplicación del Chatbot con IA (WhatsApp)	Beneficios	Usuarios en PYMES
Estructura organizativa	Define con claridad los roles, jerarquías y responsabilidades, evitando duplicación de funciones y promoviendo la eficiencia.	Consulta rápida del organigrama y funciones por WhatsApp; el chatbot responde preguntas sobre responsabilidades y estructura.	Claridad de roles, mejor flujo operativo, reducción de errores.	Empleados y nuevos colaboradores
Recursos humanos	Administra el talento humano, promueve la capacitación y controla el cumplimiento laboral interno	Automatiza recordatorios de capacitaciones, encuestas de clima laboral, y seguimiento de asistencia o cumplimiento formativo.	Ahorro de tiempo, monitoreo de desempeño, refuerzo continuo.	RR.HH., personal administrativo y operativo
Política de ética y valores	Establece normas de conducta organizacional para crear un entorno laboral sano, transparente y coherente con los valores.	Envía políticas éticas en PDF, hace preguntas de comprensión, analiza respuestas con IA y genera reportes automáticos.	Mayor cumplimiento, aprendizaje activo, trazabilidad digital.	Todos los niveles de la empresa

Alinear la cultura organizacional con las nuevas tecnologías para fortalecer la ética, liderazgo y estructura operativa desde el núcleo.

Componente 2: Evaluación de riesgos

La evaluación de riesgos es un proceso fundamental para las PYMES porque les permite identificar, valorar y mitigar los riesgos que podrían afectar su operatividad y crecimiento. En las PYMES de Guayaquil, un entorno que enfrenta fluctuaciones económicas, cambios regulatorios y nuevos desafíos tecnológicos, la evaluación de riesgos es aún más relevante.

En la tabla 4 se muestran tres elementos esenciales: identificación, valoración y plan de acción. Cada uno de estos elementos se adapta a la realidad de las PYMES locales, con metodologías simples, aunque efectivas. El uso de tecnologías emergentes como Big Data, Inteligencia Artificial y plataformas de automatización de riesgos puede potenciar este proceso, permitiendo una gestión más precisa, proactiva y adaptativa. Así, las PYMES responden a los riesgos, y aprenden a anticiparlos.

Tabla 4. Evaluación de Riesgos.

Elemento	**Descripción de elemento relacionado con las PYMES de Guayaquil**	**Tecnología Emergente**
Identificación	Se identifican riesgos financieros, regulatorios, tecnológicos y del mercado, con participación del equipo. Se usan encuestas internas, revisión de datos históricos y alertas del entorno.	Big Data e IA para analizar patrones de riesgo y fuentes externas (noticias, regulaciones).
Valoración	Se evalúa la probabilidad e impacto de los riesgos detectados, priorizando los que afectan procesos críticos. Permite tomar decisiones más rápidas y focalizadas.	Dashboards inteligentes (Power BI, Tableau) para visualización dinámica de riesgos.
Plan de acción	Se debe diseñar un plan con acciones preventivo y correctivo, asignando responsables y fechas límite. Este plan se actualiza según los cambios del entorno y desempeño del negocio.	Software de gestión de riesgos con seguimiento automatizado y alertas programadas.

Su correcta aplicación fortalece la resiliencia de las PYMES frente a un entorno cambiante y competitivo, como el de Guayaquil.

Componente 3: Actividades de control

En este componente se constituyen el núcleo operativo del sistema de control interno en las PYMES de Guayaquil. Estas actividades buscan prevenir, detectar y corregir errores o irregularidades en áreas esenciales como inventarios, cuentas por cobrar, pagos y registros financieros. En un entorno donde la informalidad, la falta de control documental y los retrasos financieros son comunes, aplicar tecnologías emergentes permite automatizar procesos críticos, reducir errores humanos y mejorar la trazabilidad de las operaciones. La tabla 5 resume cómo estas actividades deben adaptarse a la realidad de las PYMES locales, describiendo sus elementos y su relación con las cuentas involucradas, el proceso que se sigue y qué tecnología emergente potencia su ejecución eficiente.

Tabla 5. Actividades de Control en PYMES de Guayaquil con Aplicación de Tecnologías Emergentes.

Elemento del control:	**Actividades de Control**	**Tecnologías Emergentes Aplicadas**	**Proceso**
Controles preventivos.	Realizar inventarios físicos periódicos y comparar con registros contables por medio de dispositivos móviles o escáneres	Sistema de gestión de inventarios automatizado (como NetSuite) con RFID o códigos QR	El sistema se integra con tecnología RFID o códigos QR, etiquetando productos y actualizando inventarios en tiempo real al escanearlos en puntos de venta o almacenes.
Cuenta: Inventarios de productos terminados y materias primas			
Segregación de funciones	Establecer límites de crédito para los clientes y realizar seguimientos periódicos de los pagos	Software de gestión de cobranza (como Zoho Invoice) personal de contabilidad, dispositivos móviles o computadoras	El software automatiza la creación de facturas, el envío de recordatorios y la actualización de los estados de cuenta.
Cuenta: Cuentas por cobrar a clientes.			

Controles Preventivos Cuenta: Deudores diversos y cuentas por pagar.	Establecer políticas claras sobre pagos y plazos para evitar atrasos.	Software de gestión financiera integrado (como Xero)	El software permite gestionar todas las cuentas y los pagos desde una única plataforma, con recordatorios automáticos de plazos de pago.
Controles Correctivos Cuenta: Aseguramiento de la Información Financiera	Asegurar que todos los registros sean auditados y validados por un sistema independiente	Blockchain utilizada por auditores y gerentes, para registros inalterables y auditoría de transacciones financieras	Se registran todas las transacciones en la cadena de bloques, creando registros inmutables.
Controles Preventivos Cuenta: Gastos anticipados - Pagos de alquiler, seguros, etc.	Establecer un calendario de revisión y registro de los gastos anticipados en los estados financieros.	Sistemas de contabilidad en la nube (como FreshBooks). Utilizado por el personal de contabilidad.	Los pagos anticipados se registran de manera automática y se distribuyen en los períodos contables correspondientes.

Cada actividad de control se optimiza con tecnologías emergentes, mejorando eficiencia y reduciendo riesgos en PYMES.

Componente 4: Información y comunicación

Este componente busca garantizar que la información fluya de manera clara y oportuna dentro y fuera de la organización. En las PYMES de Guayaquil, la incorporación de tecnologías emergentes como plataformas en la nube, inteligencia artificial y sistemas de automatización, permite fortalecer los canales de comunicación y los reportes, reduciendo riesgos de desinformación y mejorando la capacidad de respuesta ante amenazas. En la tabla 6 se resumen los principales elementos de este componente, detallando su proceso, las tecnologías aplicadas, y los beneficios tangibles que generan para las PYMES.

Tabla 6. Aplicación de Tecnologías Emergentes en los Canales de Comunicación y Reportes de Control Interno en las PYMES de Guayaquil.

Elemento	Descripción del Proceso	Tecnología Emergente Aplicada	Beneficios
Canales de Comunicación Internos	Establecer canales claros y eficaces (intranet, correos internos, reuniones periódicas) para comunicar riesgos y actividades de control interno.	Plataformas de comunicación en la nube (Microsoft Teams)	Facilita el flujo eficiente de la información dentro de la empresa y asegura alineación entre todos los niveles.
Comunicación Externa	Mantener relaciones formales con autoridades fiscales, bancos y otras entidades externas para asegurar el cumplimiento de normativas legales y fiscales.	Blockchain para autenticación documental, correo cifrado.	Aumenta la transparencia y la confianza con stakeholders externos, fortaleciendo la reputación de la empresa.
Reportes de Control Interno	Generar reportes periódicos sobre el estado de los controles internos, riesgos identificados y acciones correctivas implementadas.	Business Intelligence (Power BI) e IA para análisis de datos	Mejora la toma de decisiones al proporcionar información clara y detallada sobre el control de riesgos

Las tecnologías emergentes mejoran la comunicación, transparencia y toma de decisiones en las PYMES de Guayaquil.

Componente 5: Actividad de supervisión

La supervisión efectiva es esencial para las PYMES de Guayaquil, permite detectar posibles fallos en el sistema de control interno y tomar las acciones correctivas necesarias a tiempo. En un entorno empresarial cambiante y marcado por múltiples riesgos, la supervisión continua y la evaluación periódica son fundamentales para garantizar la eficacia de los controles internos. Las tecnologías emergentes, como los sistemas de monitoreo en tiempo real, la auditoría

automatizada y las plataformas de análisis de datos, optimizan este proceso, permitiendo una detección rápida y un seguimiento continuo de los indicadores críticos de desempeño (KPIs).

A continuación, en la tabla 7 se resume estos elementos, detallando su proceso, los beneficios concretos que ofrecen a las PYMES y cómo se fortalece su capacidad de respuesta frente a irregularidades internas.

Tabla 7. Integración de tecnologías emergentes.

Elemento	Descripción del Proceso	Tecnologías Emergentes Aplicadas	Beneficios
Monitoreo Continuo	Implementar un sistema de monitoreo en tiempo real para detectar fallos o debilidades en el sistema de control interno (por ejemplo, auditorías automáticas).	Inteligencia Artificial (IA) y Sistemas de Monitoreo en Tiempo Real	Permite detectar irregularidades de forma rápida y tomar acciones correctivas de manera oportuna.
Auditorías Periódicas	Realizar auditorías internas de manera periódica para evaluar la efectividad del sistema de control y hacer recomendaciones de mejora.	Blockchain **software de auditoría automática**.	Asegura que los controles sean efectivos y adecuados, proporcionando una visión objetiva del sistema de control
Revisión de Indicadores (KPIs)	Desarrollar y revisar indicadores de desempeño (KPIs) para evaluar la efectividad de los controles internos, como el análisis de transacciones y desempeño.	Business Intelligence (BI) y dashboards en tiempo real	Ayuda a la alta dirección a evaluar la eficiencia del sistema de control y tomar decisiones basadas en datos.

Las tecnologías emergentes mejoran el monitoreo, auditorías y revisión de KPIs, optimizando la supervisión interna.

CONCLUSIONES

Los fraudes en las PYMES, tanto en Europa como en Latinoamérica, representan un reto que compromete la sostenibilidad y competitividad de estas empresas. Mientras que en Europa los delitos relacionados con el IVA, los fondos europeos y los contratos públicos reflejan una problemática estructural, en Latinoamérica y Ecuador, prácticas como la malversación, la falsificación de documentos y el lavado de dinero destacan como las principales amenazas.

La integración de la inteligencia artificial (IA) fortalece los sistemas de control interno mediante la automatización de tareas repetitivas, el monitoreo en tiempo real y la generación de informes precisos, mejorando así la toma de decisiones estratégicas. Al mismo tiempo, estas soluciones promueven la transparencia, la seguridad financiera y la sostenibilidad, elementos decisivos para la competitividad en un entorno empresarial dinámico.

El fraude empresarial representa una amenaza para la estabilidad económica y la reputación de las organizaciones, manifestándose en prácticas como la manipulación de estados financieros, la malversación de fondos y la falsificación de documentos. La detección y prevención requieren la implementación de controles internos sólidos, auditorías frecuentes y estrategias como la verificación de documentos, el monitoreo de inventarios y la supervisión de transacciones. La segregación de funciones y la capacitación del personal en ética empresarial refuerzan la transparencia y reducen las oportunidades de fraude.

Los resultados evidencian que la adopción de IA y aprendizaje automático en la detección de fraudes aun es limitada, con barreras como la falta de conocimientos técnicos, la integración con sistemas existentes y la resistencia al cambio. Aunque la mayoría reconoce su eficiencia respecto a métodos tradicionales y su impacto positivo en la gestión de riesgos, la implementación sigue en desarrollo. El fraude financiero es el más recurrente, seguido por el interno y cibernético, lo que marca la necesidad de sistemas de detección más robustos.

La propuesta desarrollada en esta investigación presenta un sistema de control interno que incorpora tecnologías emergentes, con el objetivo de ofrecer una solución efectiva para la detección temprana de riesgos y mejorar la capacidad de respuesta ante amenazas. Aunque este sistema ha sido diseñado para las PYMES de Guayaquil, su estructura y componentes permiten que pueda ser adaptado y aplicado en contextos nacionales e internacionales. El sistema integra cinco componentes: ambiente de control, evaluación de riesgos, actividades de control, comunicación interna y supervisión continua. Mediante la incorporación de tecnologías como la inteligencia artificial, blockchain y sistemas de monitoreo en tiempo real, las PYMES pueden enfrentar los riesgos de manera proactiva, fortaleciendo su adaptabilidad y sostenibilidad en un entorno empresarial en constante cambio.

REFERENCIAS BIBLIOGRÁFICAS

Barriga, M., Casal, C., & Coello, P. (2023). Estrategias de prevención y detección de fraude financiero en medianas y grandes empresas de Guayaquil. Journal business Science, 4(2), 61-84. https://doi.org/10.56124/jbs.v4i2.0005

Calle, J., Sotaminga, A., Garay, G., & Villavicencia, R. (2024). *Intelgencia artificial ysu contrbucion a la Innovacion en las empresas*. Ciencia y Desarrollo, 27(2). http://revistas.uap.edu.pe/ojs/index.php/CYD/index

Chiriguaya, S., & Mejia, M. (2022). *Propuesta metodológica para la prevención de fraudes en el sector PYMES de equipos de seguridad Industrial de Guayaquil*. Guayquil, Guayas, Ecuador. (Trabajo de titulación). Universidad Católica de Santiago de Guayaquil.

Ecuador. Instituto Nacional de Estadística y Censos. (2022). Estructura Poblacional. https://www.censoecuador.gob.ec/wp-content/uploads/2023/10/Presentacio%CC%81n_Nacional_1%C2%B0entrega-4.pdf

Erazo, J., & De la A, S. (2023). Auditoría del futuro, la prospectiva y la inteligencia artificial para anticipar riesgos en las organizaciones. *Novasinergia, 6*(1), 105-119. https://doi.org/10.37135/ns.01.11.07

García, M., Grillo, A., & Morte, T. (2021). La adaptación de las empresas a la realidad COVID una revision sistemática. 11(21), 55-70. https://doi.org/10.17163/ret.n21.2021.04

Instituto de auditores internos de españa. (2023). *Auditoria Interna de la inteligencia artificial aplicada a procesos de negocios.* Madrid-Santa Cruz. https://n9.cl/cfbg38

Jara Obregón, L. S., & Naspud Espinoza, M. G. (2025). Inteligencia Artificial: Desafíos y Oportunidades Para Las Pymes Ecuatorianas. *Arandu UTIC*, *11*(2), 3063–3077. https://doi.org/10.69639/arandu.v11i2.485

Lisicki Litvin & Asociados. (2020). *Métodos de prevención, detección e investigación de fraudes dentro de empresas.* https://www.palermo.edu/economicas/contadores/presentaciones/Binder1.pdf

Rivas, A. (2022). Control interno en empresas comerciales nacientes en Ecuador. *Polo del Conocimiento, 7*(9), 336-360. https://www.polodelconocimiento.com/ojs/index.php/es/article/view/4578

Tantalean, I. (2022). Análisis crítico al origen del fraude empresarial, efectos y tratamiento juridico. LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades, *2(3)*, 154-174. https://doi.org/10.56712//latam.v3i2.72

Tenes, E. (2023). Impacto de la inteligencia artificial en las Empresas Escuela Técnica Superior de Ingenieros Informáticos.

Unión Europea. (2024). *Informe anual de 2023 de la fiscalía europea.* https://www.eppo.europa.eu/en/documents/2023-numbers

Valladares, J., & Ordoñez, Y. (2024). *La aplicacion de inteligencia artificial en la auditoria contable*. *Revista Multidisciplinaria Perspectivas Investigativas*, *4*(especial), 73–85. https://doi.org/10.62574/rmpi.v4iespecial.172