Del Libro Mayor al Big Data: La Transformación de la Contabilidad Forense y Detección de Fraudes

From General Ledger to Big Data: The Transformation of Forensic Accounting and Fraud Detection

Orlando de Jesús Avendaño Calderón

Investigador independiente

Resumen

El objetivo del presente artículo de revisión es analizar el cambio de paradigma en la contabilidad forense desde los métodos de auditoría tradicionales, hacia el análisis forense de datos en ecosistemas digitalizados. La investigación se desarrolló bajo el enfoque cualitativo de tipo documental, empleando el método analítico para examinar literatura científica y normativa internacional sobre escándalos financieros. El estudio explora la integración de Big Data, Inteligencia Artificial y la Ley de Benford, proponiendo que el enfoque de «pruebas de población completa» se posiciona como una metodología efectiva para detectar irregularidades en entornos de Enterprise Resource Planning (ERP). Asimismo, el documento aborda ciertos desafíos provenientes de la inmutabilidad de Blockchain, el rastreo de criptoactivos y la admisibilidad legal de la evidencia digital bajo estándares forenses. Mediante el análisis crítico de la literatura, se identificaron posibles brechas en la formación técnica del auditor, así como la necesidad de evolucionar hacia un perfil profesional integral que acople la ciencia de datos, con el cumplimiento legal y la experiencia financiera. Se concluye que la transformación digital de la contabilidad forense no es solo tecnológica sino también estructural, requiriendo marcos normativos actualizados para la validación de pruebas digitales en contextos judiciales.

Palabras clave: Contabilidad Forense, Análisis de Big Data, Detección de Fraudes, Inteligencia Artificial, Ciber-forense.

Recibido: 30 de octubre de 2025 – revisión aceptada: 18 de junio de 2026 – Fecha de publicación: 20 de agosto 2026

Correspondiente al autor: orlando19081982@gmail.com

Abstract

The objective of this review article is to analyze the paradigm shift in forensic accounting from traditional auditing methods to forensic data analytics in digitized ecosystems. The research was conducted using a qualitative documentary approach, applying the analytical method to examine scientific literature and international regulations concerning financial scandals. The study explores the integration of Big Data, Artificial Intelligence, and Benford's Law, proposing that the «full population testing» approach serves as an effective methodology for detecting irregularities within Enterprise Resource Planning (ERP) environments. Furthermore, the document addresses certain challenges arising from the immutability of Blockchain, the tracing of crypto-assets, and the legal admissibility of digital evidence under forensic standards. Through a critical analysis of the literature, potential gaps in the auditor's technical training were identified, along with the need to evolve towards a comprehensive professional profile that combines data science with legal compliance and financial expertise. It is concluded that the digital transformation of forensic accounting is not only technological but also structural, requiring updated regulatory frameworks for the validation of digital evidence in judicial contexts.

Key words: Forensic Accounting, Big Data Analytics, Fraud Detection, Artificial Intelligence, Cyber-forensics.

Introducción

La economía contemporánea opera con un flujo continuo de datos. Según estimaciones de organismos internacionales como el Banco de Inglaterra (McLeay et al., 2014, p. 15), la Reserva Federal de los Estados Unidos y el Fondo Monetario Internacional[1], más del 90% de la masa monetaria global existe en formato digital. Esta desmaterialización del dinero ha optimizado la eficiencia transaccional, permitiendo el movimiento instantáneo de capitales transfronterizos. Sin embargo, esta misma infraestructura ha expandido exponencialmente la «superficie de ataque» para el crimen de cuello blanco.

En el pasado, el fraude requería de acceso a documentos tangibles y una interacción humana directa. Hoy, el defraudador opera desde la sombra, desde la *Deep Web* y con direcciones IP variables, aprovechando la complejidad de los sistemas ERP y la inmensidad de los volúmenes de datos para ocultar sus rastros. Nos enfrentamos entonces a una paradoja: mientras las corporaciones invierten millones en blindar sus perímetros de ciberseguridad externa, los controles internos contables a menudo permanecen, lamentablemente, anclados en metodologías del siglo XX.

La incapacidad de los métodos tradicionales de auditoría para detectar fraudes sistémicos ha quedado patente en escándalos financieros recientes como Wirecard en 2020, y FTX[2] en 2022, donde la manipulación no ocurrió en el papel, sino en los algoritmos

[1]Aunque el Fondo Monetario Internacional rara vez usa la frase «90% digital» en comunicados de prensa simples, sus bases de datos son las que permiten calcular este porcentaje a nivel mundial al sumar los agregados monetarios de todos los países.

y en las APIs de conexión bancaria. Por su parte, estudios recientes como el de Kaya y Özer (2023), confirman que la creciente descentralización de los activos financieros y el uso masivo de contratos inteligentes exigen que la contabilidad forense evolucione hacia la analítica forense en tiempo real, para reducir el riesgo de ofuscación de transacciones. Este escenario plantea la necesidad de una respuesta forense moderna, que abandone la revisión reactiva por una vigilancia proactiva basada en datos masivos.

Esta expansión del crimen económico es confirmada por la ACFE (2024) en su reporte global, señalando que las organizaciones pierden aproximadamente el 5% de sus ingresos anuales debido a los fraudes. Autores como Gottschalk (2010), sostienen que la detección efectiva de estos fraudes requiere una alineación estratégica entre la gestión empresarial y las capacidades de investigación de los auditores, mientras que Soltani (2014) destaca que los escándalos corporativos modernos comparten una anatomía común basada en fallas sistémicas de control.

Para abordar esta problemática, es necesario establecer una distinción taxonómica entre la Auditoría Financiera y la Contabilidad Forense, dos disciplinas que, aunque comparten la misma materia prima, es decir, la información financiera, difieren en su propósito y metodología. Por un lado, el propósito de la Auditoría Financiera es brindar la «seguridad razonable» de que los estados financieros están libres de errores materiales. Su metodología se basa básicamente en el muestreo selectivo y en el concepto de «materialidad» o importancia relativa. El auditor entonces, asume bajo la presunción de buena fe, que la administración ha preparado los informes correctamente a menos que surja alguna evidencia de lo contrario. En contraste, la Contabilidad Forense opera bajo la premisa de escepticismo presuntivo. Esto debido a que no busca la razonabilidad, sino la evidencia legal. Instituciones como el American Institute of Certified Public Accountants (AICPA, 2023), entre otras, han establecido guías claras para que el profesional de la contabilidad transite hacia la analítica de datos. Asimismo, la normativa ISA 240 (2009) define las responsabilidades que el auditor tiene frente al fraude, las cuales se han visto reforzadas por regulaciones como la Ley Sarbanes-Oxley y los estándares del PCAOB (2023) que exigen un escrutinio más riguroso de los controles internos en entornos digitales. La definición formal, propuesta por el autor y que se adopta en este estudio es:

«La Contabilidad Forense es la aplicación de diversas técnicas que van desde la investigación criminalística y conocimientos contables, como de habilidades de auditoría tecnológica para el análisis de la evidencia financiera, esto con el fin de establecer hechos que pueden ser admitidos en un procedimiento legal o administrativo.»

Esta definición, calza con la era digital al incluir la capacidad tecnológica para procesar el 100% de los datos en una suerte de *Full Population Testing*. A diferencia del auditor convencional que podría revisar, a lo sumo, hasta quinientas transacciones de una población de cinco mil, el contador forense digital, utiliza algoritmos para analizar las cinco mil transacciones, buscando patrones anómalos que el ojo humano o el muestreo aleatorio jamás detectarían. De hecho, la literatura reciente señala que la integración sistemática de técnicas de *Big Data Analytics* sobre las bases de las ERP, ha reducido drásticamente los falsos negativos en la auditoría interna de organizaciones altamente digitalizadas (Alshurafat et al., 2025).

Por su parte, la historia del fraude es la historia de la adaptación criminal a la tecnología

[2] El caso Wirecard constituye un fraude contable basado en la sobrevaloración de activos, donde se registraron 1,900 millones de euros en efectivo inexistente en el balance general. En comparación, el colapso de FTX se originó, además de las fallas del gobierno corporativo, por la falta de controles internos, lo que permitió la apropiación indebida de fondos de clientes para financiar operaciones de una parte relacionada.

disponible, y se puede categorizar en dos momentos, a saber:

- La era analogía o Fraude 1.0: Caracterizada por la manipulación física de archivos tangibles. Los esquemas típicos incluían el «jineteo» de fondos o *lapping* mediante el robo de efectivo en caja, la alteración manual de cheques, o la falsificación de facturas impresas mediante fotocopiadoras. La velocidad del fraude 1.0 estaba limitada por la velocidad humana de procesamiento y la logística física. La detección, por ende, dependía de una aguda inspección visual, el arqueo de caja y la conciliación bancaria manual.

- La era digital o Fraude 2.0: Este fraude es netamente digital y no deja rastro de papel, sino «huellas digitales». Por su parte, en la actualidad, investigaciones empíricas como la de Ozili (2024) demuestran que la adopción de algoritmos de IA generativa y de aprendizaje automático no solo es utilizado como mecanismo de defensa, sino que los propios perpetradores la emplean para sofisticar ataques de ingeniería social financiera y eludir reglas de auditoria tradicional. Se caracteriza por:

  Invisibilidad: el atacante manipula directamente las tablas en bases de datos SQL, saltándose los controles de la interfaz de usuario del software contable.

  Automatización: se emplean *scripts o bots* para desviar micro-centavos en millones de transacciones[3]. Asì se acumulan sumas millonarias sin afectar la materialidad individual de una operación.

  Deslocalización: el perpetrador puede ser un empleado trabajando remotamente o un actor externo que ha comprometido las credenciales de un usuario legítimo o *Account Takeover.*

En tal sentido, la transición del Fraude 1.0 al 2.0 exige que el contador deje de mirar el archivador y comience ahora sí, a interrogar al servidor. Por consiguiente, el presente artículo tiene como objetivo analizar el cambio de paradigma en la contabilidad forense, examinando la transición de los métodos tradicionales de auditoria hacia el análisis forense de datos, a través del uso de herramientas tecnológicas.

Objetivo y Metodología

Como se mencionó anteriormente, el presente artículo busca analizar el cambio de modelo en la contabilidad forense, estudiando la transición desde los métodos tradicionales de auditoría, hacia el análisis forense de datos en ecosistemas digitales. En tal sentido, la tesis central sostiene que la tecnología actúa como un facilitador sofisticado para el fraude 2.0 y simultáneamente, además de paradójico, como la herramienta que facilita la detección de este y su mitigación.

Para lograr el objetivo, la investigación se fundamentó bajo el enfoque cualitativo de tipo documental con diseño no experimental. Por lo tanto, el enfoque metodológico consistió en una revisión analítica de la literatura científica y normativa aplicable.

Con respecto a los criterios de selección de fuentes bibliográficas, se realizó una búsqueda sistemática en las bases de datos académicas de alto impacto, tales como *Scopus, Web of Science* y *Google Scholar*, utilizando descriptores clave como «*Forensic Accounting*», «*Big Data Analytics*», «*Fraud 2.0*» y «*Continuous Auditing*». Asimismo, se determinaron como

[3]Técnica «salami»·

criterios de inclusión, estudios empíricos, revisiones teóricas y normativas publicados, preferentemente, en los últimos 15 años, con la finalidad de asegurar la vigencia tecnológica frente a la evolución de los sistemas ERP y criptoactivos.

Finalmente, como técnicas de análisis, se emplearon el análisis de contenido cualitativo y el método hermenéutico. Esto permitió, en primer lugar, observar las adaptaciones teóricas como el Triángulo del Fraude de Cressey al entorno digital; en segundo lugar, comparar las capacidades de herramientas técnicas como la Inteligencia Artificial y la Ley de Benford frente al muestreo estadístico tradicional; y, tercero y último, resumir las implicaciones jurídicas relativas a la cadena de custodia y la admisibilidad de la evidencia digital.

Figura 1. Flujo metodológico de la revisión analítica y transición paradigmática

Nota. elaboración propia (2026)

Marco Teórico

El Triángulo del Fraude de Cressey (1953) en el entorno virtual

El modelo clásico del Triángulo del Fraude, propuesto en los años 50 por el criminólogo estadounidense Donald Cressey (1919-1987), identifica tres elementos necesarios para la comisión de un delito: Presión, Racionalización y Oportunidad. Si bien este modelo continúa vigente, el actual entorno digital ha obligado la reestructuración drástica de la naturaleza de estos vértices, como se aprecia a continuación:

1. **Presión:** En la actual era digital, la presión financiera se ha visto agravada por el creciente consumo en redes sociales y la volatilidad de los nuevos mercados. Asimismo, la presión corporativa por cumplir métricas de rendimiento, monitoreadas en tiempo real, podría conducir a ejecutivos hacia prácticas poco morales, como la

manipulación de estados financieros o la contabilidad creativa.

2. **Racionalización:** La tecnología crearía una distancia psicológica entre el perpetrador y la víctima. En otrora, robar o hurtar, requería superar barreras morales y físicas. Sin embargo, actualmente transferir fondos electrónicamente o manipular una cifra en una hoja de cálculo, se percibe como una acción abstracta, o «un simple juego de números» sin víctimas visibles para el perpetrador. El defraudador digital, por ende, se convence de que «solo está tomando prestados bits» o que «el sistema informático del banco tiene errores y esto es justicia».
3. **Oportunidad:** Este es el componente que, peligrosamente, ha crecido más gracias a la tecnología. La complejidad de los sistemas ERP genera configuraciones de seguridad bastante deficientes. En estos entornos, la falta de segregación de funciones es un problema endémico; pues es común encontrar usuarios con permisos de «superadministrador» que pueden iniciar, aprobar y registrar una transacción, y luego borrar el rastro en el log de auditoría. La oportunidad técnica, combinada con el anonimato del trabajo remoto, crea el caldo de cultivo perfecto para el fraude 2.0 desde un nivel interno.

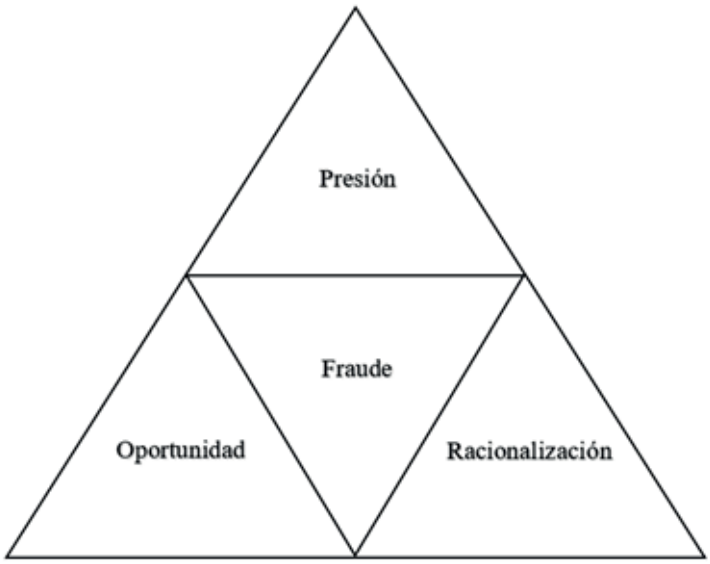

Figura 2. La teoría del triángulo de fraude

Nota. elaboración propia (2026) basado en Cressey (1953)

A pesar de la vigencia del Triángulo del Fraude de Cressey, la teoría ha evolucionado. Wolfe y Hermanson (2004), propusieron la teoría del «Diamante del Fraude», añadiendo la capacidad del individuo como un elemento crítico para ejecutar el delito. Por su parte, Dorminey et al. (2012) argumentan que el modelo propuesto por Cressey debe integrar factores psicológicos más complejos para ser efectivo en la actualidad, mientras que críticos como Huber (2017) sugieren que el triángulo tradicional podría estar llegando a su obsolescencia ante la complejidad de los actuales delitos financieros.

Modalidades de Fraude en Sistemas Enterprise Resource Planning y Nube

Es importante mencionar que la migración a la nube ha descentralizado la contabilidad, permitiendo nuevas tipologías de fraude que explotan la arquitectura de los sistemas de información, tales como:

- Manipulación de Asientos y Logs: Los perpetradores con acceso privilegiado pueden insertar asientos de diario manuales directamente en la base de datos, para ajustar los ingresos u ocultar gastos. El desafío forense aquí es que, a menudo, estos asientos se realizan generalmente en horarios atípicos, como fines de semana o madrugadas y se intenta borrar el registro de auditoría del sistema.
- Fraude en el Maestro de Proveedores: Consiste en la creación de «proveedores fantasmas» o la reactivación de proveedores inactivos, cambiando la cuenta bancaria de destino a una controlada por el empleado que generalmente aprueba los pagos. En un entorno de *Big Data* con miles de proveedores, estos registros podrían perderse o pasar desapercibidos en el ruido operacional de datos, a menos que se apliquen algoritmos de comparación aproximada o *fuzzy matching* para detectar similitudes entre direcciones de empleados y proveedores.

El análisis forense de datos como arma estratégica

En párrafos anteriores, se mencionó cómo el fraude ha pasado desde la analogía hacia formas sistémicas y digitales. En esta sección, se aborda la metodología propuesta, en esta investigación, el análisis forense de datos.

En ese sentido, cabe mencionar que la auditoría tradicional se ha enfrentado a una limitación física, la imposibilidad humana de revisar todas y cada una de las transacciones de la totalidad de una población. Esta limitación dio origen a la teoría del muestreo estadístico. Sin embargo, en el contexto del fraude 2.0, el muestreo presenta una debilidad, ya que este tipo de fraude no es un evento aleatorio, sino un evento intencional y atípico. Un fraude material podría residir en solo cinco transacciones dentro de un universo de un millón de transacciones. Por ello, la probabilidad de que una muestra aleatoria capture esas cinco transacciones es casi nula.

El análisis forense de datos propondría entonces un cambio de paradigma que se traduce en la auditoría de una población completa de transacciones. Este enfoque mitiga el riesgo de muestreo y transforma la detección de un ejercicio de azar a uno de mayor revisión fundamentada en patrones algorítmicos.

La literatura consultada sugiere que el uso de herramientas como *Audit Command Language* o ACL e IDEA constituye un estándar técnico fundamental para preservar la integridad investigativa. En tal sentido, Rezaee y Wang (2019) subrayan que el *Big Data Analytics* ha transformado la contabilidad forense en una disciplina predictiva. Esta transformación es vital considerando que, como afirman Vasarhelyi et al. (2015), la contabilidad en la era del Big Data requiere un monitoreo que supere las limitaciones del tiempo y el volumen tradicional.

Aunque las hojas de cálculo como Excel o Numbers, son herramientas de uso extendido, diversos autores como Coderre (2009), Singleton y Singleton (2010) y Dorminey, et al. (2012), señalan que las mismas podrían presentar algunas vulnerabilidades frente

a la alteración de datos. Esta debilidad comprometería la integridad en una investigación forense de gran envergadura. En tal sentido, el estándar profesional exige el uso de software de auditoría generalizada, como el *Audit Command Language* o ACL e IDEA. Estas herramientas ofrecen tres ventajas críticas sobre las hojas de cálculo, para asegurar la validez legal de la evidencia:

1. Acceso de Solo Lectura: Estas herramientas garantizan que los datos originales no serán modificados durante el análisis, preservando de esta forma la cadena de custodia.

2. Registro de Auditoría: Las herramientas graban automáticamente cada paso, filtro y comando ejecutado por el auditor. Esto permite que un tercero, ya sea otro auditor o un tribunal, pueda replicar exactamente el análisis y llegar a los mismos resultados, cumpliendo con el principio científico de reproducibilidad.

3. Capacidad de Procesamiento Masivo: de igual manera, permiten cruzar millones de registros de fuentes dispares, como cruzar la base de datos de nómina de SAP con el registro de entradas físicas del sistema de seguridad del edificio) para detectar inconsistencias, como empleados que cobran horas extras sin haber ingresado a las instalaciones.

Aplicación de pruebas estadísticas forenses en la detección de fraudes. La Ley de Benford (1938)

Para reforzar el análisis forense de datos, es necesaria la aplicación de una de las técnicas más potentes y contraintuitivas en el arsenal forense, el análisis de dígitos de la Ley de Benford, la cual sostiene que, en conjuntos de datos naturales y no manipulados que abarcan varios órdenes de magnitud, tales como facturas, pagos o saldos de inventario, los dígitos iniciales no se distribuyen uniformemente. Contrario a la intuición de que el uno al nueve tiene la misma probabilidad del 11.1%, la ley dicta entonces una distribución logarítmica donde el dígito uno aparece como primer dígito aproximadamente el 30.1% de las veces, mientras que el nueve aparece solo el 4.6%. La aplicación práctica de esta ley en entornos forenses, ha sido documentada exhaustivamente por Nigrini (2011), quien la describe como la «biblia técnica» para identificar patrones de manipulación en estados financieros y esquemas de fraude ocupacional. Sus estudios demuestran que las anomalías en los dígitos pueden ser indicadores consistentes de registros inventados o «maquillados».

La fórmula que rige esta probabilidad es:

$$P(d) = \log_{10}(1 + \frac{1}{d})$$

Donde:

P(d) es la probabilidad de que un número comience con el dígito (d).

(d) es el primer dígito (siendo (d) ∈ {1, 2, 3, …, 9}).

$\log_{10}$ es el logaritmo en base 10.

Tabla1. Distribución de la Probabilidad (Primer Dígito)

Primer Dígito (d)	Probabilidad (P(d))	Porcentaje Esperado
1	log10(1+1/1)	30.1%
2	log10(1+1/2)	17.6%
3	log10(1+1/3)	12.5%
4	log10(1+1/4)	9.7%
5	log10(1+1/5)	7.9%
6	log10(1+1/6)	6.7%
7	log10(1+1/7)	5.8%
8	log10(1+1/8)	5.1%
9	log10(1+1/9)	4.6%

Nota. elaboración propia (2026)

Cuando un defraudador intenta inventar cifras para generar estados financieros o para «maquillar los libros», inconscientemente tiende a distribuir los dígitos de manera uniforme o evita también repetir números, violando el patrón natural de Benford. Supongamos entonces que el límite de autorización de gastos que un gerente dispone es de $ 5.000,00 por cada transacción. Para apropiarse de manera desleal de $ 20.000,00 sin pedir autorización del superior, el gerente «crea» cuatro facturas falsas de servicios por $ 4.800,00; $ 4.900,00; $ 4.950,00 y $ 4.850,00. Un análisis basado en la Ley de Benford sobre los segundos dígitos o los últimos dígitos revelará un pico anormal en el número «nueve» o en cifras justo por debajo del umbral de control, denominado efecto precipicio, alertando inmediatamente al auditor sobre la manipulación sistemática para eludir controles internos (Nigrini, 2019).

Sin embargo, a pesar de su eficacia, es necesario abordar la Ley de Benford reconociendo sus limitaciones estadísticas. Como advierte el propio Nigrini (2012), esta prueba analítica no sería universalmente aplicable; pues carece de validez probabilística en poblaciones numéricas con restricciones estructurales, tales como números secuenciales, verbigracia, la numeración correlativa de cheques. Por consiguiente, una posible desviación anómala de la curva logarítmica, no constituiría por sí misma una prueba de fraude, sino una «bandera roja» estadística que justificaría una investigación forense más profunda y focalizada

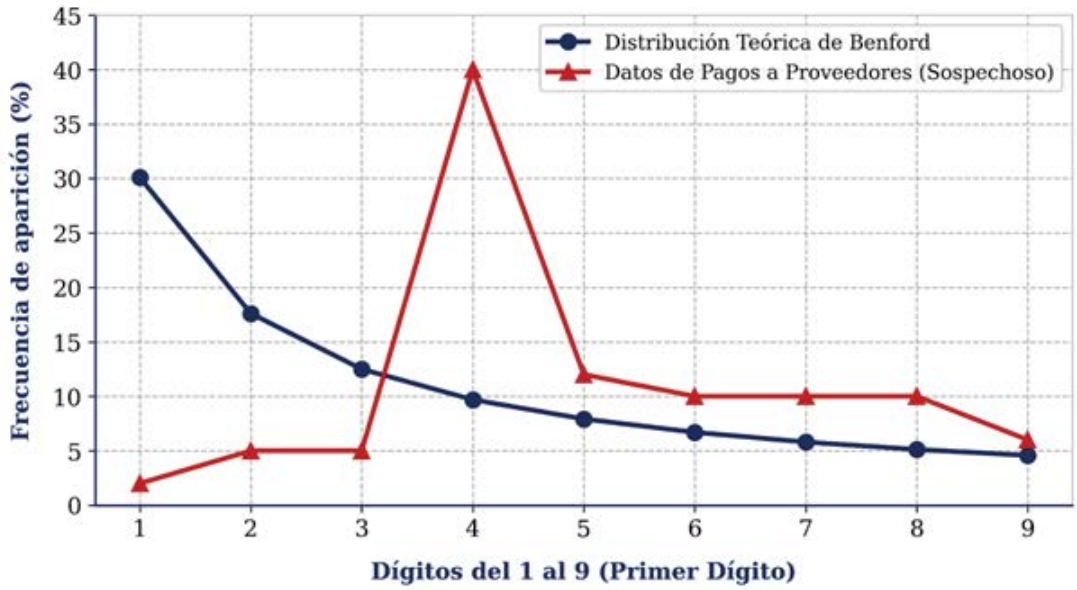

Figura 3. La Curva de Benford vs. Datos Manipulados

Nota. elaboración propia (2026)

La línea azul muestra la caída logarítmica esperada por la Ley de Benford (1938) (comenzando alto en el uno y descendiendo suavemente hasta el nueve).

La línea roja muestra la anomalía solicitada, con una frecuencia muy baja en el dígito 1 y un pico drástico en el cuatro (40%).

El pico anómalo en el dígito cuatro sugiere que el personal está manipulando facturas justo por debajo de un límite de aprobación de $5,000.

Fuente: elaboración propia (2025) basado en la Ley de Benford (1938)

En tal sentido, el fraude deja una huella financiera, o el «qué», pero la intención, el «por qué» y sobre todo el «quién», reside en los datos no estructurados. Se estima entonces que el 80% de los datos corporativos son no estructurados, tales como, correos electrónicos, chats, memos en PDF y descripciones en campos de texto libre. El Análisis forense de datos incorpora técnicas de Minería de Texto y «Análisis de Sentimientos», utilizando bibliotecas de términos asociados al fraude, verbigracia, «cuota», «regalo», «arreglar», «fuera de registro» o «borrar». Asimismo, el Análisis forense de datos permite un análisis de conceptos, que implica una identificación de correos enviados en días y horarios inusuales o con adjuntos encriptados hacia direcciones personales. Adicionalmente, permite una correlación cruzada, pues el software de análisis forense de datos, puede vincular una factura sospechosa detectada en la base de datos contable, con un correo electrónico enviado ese mismo día por el proveedor al gerente implicado con el asunto, por ejemplo, «Gracias por el favor», cerrando así el círculo probatorio.

Sin embargo, mientras el análisis forense de datos es una buena herramienta para la detección «post-mortem», la IA promete avanzar hacia la prevención en tiempo real. Los modelos de Aprendizaje Supervisado se entrenan con bases de datos históricos,

contrastando los fraudes 2.0 con transacciones legítimas, con el fin de generar un «score de riesgo» en nuevas operaciones. No obstante, la literatura académica advierte que presentar la IA como una solución infalible, podría resultar incluso arriesgado. Como señalan Baesens et al. (2015), la precisión algorítmica es altamente dependiente de la calidad e integridad de los datos de entrenamiento; si el historial corporativo contiene sesgos, falsos negativos o clasificaciones erróneas previas, la IA perpetuará y escalará dichas fallas de manera automatizada.

Por otro lado, el Aprendizaje No Supervisado, mediante algoritmos de agrupamiento o «*clustering*», permite identificar transacciones que podrían parecer estadísticamente atípicas. Aunque, investigaciones como las de Cho et al. (2020) demuestran que estos modelos pueden predecir deficiencias en controles internos, su implementación práctica podría enfrentar barreras técnicas significativas. En tal sentido, Baader y Krcmar (2018) señalan que el principal desafío del Aprendizaje No Supervisado son las elevadas tasas de «falsos positivos». Por consiguiente, en entornos transaccionales masivos, señalar cada desviación estadística, podría abrumar a los auditores con alertas irrelevantes, generando la llamada «fatiga de alertas» y diluyendo la eficiencia investigativa.

Adicionalmente, desde una perspectiva criminológica adaptativa, Abdallah et al. (2016) advierten sobre el fenómeno del «*concept drift*» o deriva de concepto. Cuando los defraudadores modernos tienen la capacidad de estudiar y comprender los límites de los controles automatizados, podrían modificar sutilmente sus tácticas como operar justo por debajo de los nuevos umbrales algorítmicos, con el fin de evadir la detección, lo que exigiría una recalibración constante de los sistemas de IA para que estos no queden obsoletos. Para mitigar estas vulnerabilidades, el enfoque de inteligencia artificial requiere integrarse con la «Auditoría Continua», un concepto pionero de Alles et al. (2002) que busca la garantía de información de forma ininterrumpida.

Auditoría continua basada en IA

Tradicionalmente, tanto la auditoría interna como la auditoría forense operan con un desfase temporal o «*lag*», ya que, por ejemplo, los errores de enero se detectan en la auditoría de marzo. En la actual era digital, este desfase es inaceptable. Ya que la auditoría y el monitoreo continuos representan la automatización de los controles.

Mediante la implementación de «sensores» de *software* en los puntos críticos del ERP, el sistema evalúa cada transacción en el momento de su origen contra un conjunto de reglas de negocio y algoritmos de IA. Si una orden de compra, verbigracia, carece de una requisición aprobada, o si un pago se dirige a una cuenta bancaria ubicada en un paraíso fiscal, predeterminada en una «lista negra», el sistema no solo registra el evento, sino que puede bloquear la transacción preventivamente. Esto transforma la contabilidad forense de una autopsia financiera a un «sistema inmunológico digital activo».

Por su parte, la tecnología *Blockchain* introduce un paradigma de contabilidad de triple entrada, a saber: debe, haber y el hash criptográfico inmutable. Para el auditor forense, esto presenta una dicotomía:

Primeramente, como ventaja se observa que una vez que una transacción se confirma en la *Blockchain*, es teóricamente inmutable. Esto eliminaría la modalidad de fraude basada en la alteración retrospectiva de libros contables, en otras palabras, podría eliminar la posibilidad de hacer contabilidad creativa después del cierre.

Sin embargo, también se podrían presentar desventajas, pues la inmutabilidad del *Blockchain* no garantiza la veracidad de la información.

Por un lado, Bonyuet (2020) advierte que la inmutabilidad no implica veracidad absoluta, lo que requeriría que el auditor valide la fuente original de los datos. Por otro lado, en el ámbito de los criptoactivos, Breisman (2019) señala que el rastreo forense, sería esencial para desarticular redes de lavado de dinero en la *Deep Web*, siendo esto un desafío también abordado en las guías técnicas de Deloitte (2023).

Por ejemplo, si un activo fijo inexistente se «tokeniza» y se registra en la *Blockchain*, el registro conocido como *Garbage In*, es inmutablemente falso. Por consiguiente, la revisión forense se desplaza de la verificación de la integridad matemática del registro, a la validación de la existencia real y la valoración de los activos subyacentes en el mundo físico.

Cripto-Forense: Rastreo de Activos en la Dark Web

Es importante mencionar que gracias a la actual era digital, el lavado de dinero ha encontrado en las criptomonedas un medio eficiente. El contador forense moderno debe poseer competencias en «*Análisis On-Chain*». Herramientas como *Chainalysis* o *Elliptic* permiten visualizar el flujo de fondos a través del libro mayor público.

En estos escenarios, la investigación se centra en identificar patrones de ofuscación, como el uso de «*Mixers*» o «*Tumblers*». Lo que implica ciertos servicios que mezclan fondos ilícitos con lícitos, con la finalidad de romper la trazabilidad. El objetivo forense es seguir la «migaja digital» hasta un punto de salida, generalmente un *Exchange* centralizado donde el perpetrador debe cumplir con algunos protocolos como el *Know Your Customer*, permitiendo así la desanonimización del sujeto mediante orden judicial.

La Cadena de Custodia de la Evidencia Digital

En el litigio moderno, la evidencia más incriminatoria suele ser efímera: un archivo temporal, un *log* de acceso o un correo borrado. Para que el *Big Data* tenga valor probatorio, se debe garantizar su integridad absoluta. En tal sentido, el procedimiento estándar exige la creación de una imagen forense del medio de almacenamiento original, conocido como *Bit-stream Image*. En este caso, no se trabaja sobre el disco original, sino sobre una copia exacta bit a bit.

Por consiguiente, se hace necesario el *Hashing Críptográfico*, ya que antes y después de la extracción de la evidencia, se calcula un valor *hash*, que no es más que una huella digital alfanumérica, por ejemplo, SHA-256. Si al presentar la evidencia en juicio, el *hash* del archivo analizado difiere, aunque sea en un carácter del *hash* original, la defensa puede argumentar exitosamente que la evidencia ha sido alterada, logrando su inadmisibilidad. En tal sentido, sería necesario el uso de hardware *Write-Blockers* o bloqueadores de escritura, para asegurar que los metadatos, como la fecha de último acceso, no se modifiquen. La integridad de la evidencia digital debe seguir estándares internacionales como la norma ISO/IEC 27001 para la seguridad de la información. Asimismo, las guías técnicas del NIST (2006) establecen los protocolos para la integración de técnicas forenses en la respuesta a incidentes, mientras que Casey (2011) y Mason (2017) enfatizan que la validez legal depende de la preservación estricta de la imagen bit a bit y del *hashing* criptográfico.

Conclusión

La transición del libro mayor físico a los ecosistemas de *Big Data* representaría un cambio de paradigma que podría redefinir estructuralmente la praxis de la contabilidad forense. Como principal aporte, este estudio de revisión sistematizó la configuración del

«Fraude 2.0» y además, demostró teóricamente la obsolescencia del muestreo estadístico tradicional.

Se concluye que, frente a la creciente automatización del fraude, el enfoque de «pruebas de población completa» a través de software de auditoría generalizada, con el apoyo de la Inteligencia Artificial, no sería meramente una ventaja competitiva, sino un imperativo metodológico que garantizaría la detección exhaustiva en entornos ERP.

Asimismo, el documento aportó una reflexión crítica sobre la tensión existente entre el avance tecnológico en la era digital y la normativa jurídica. Asimismo, el surgimiento de la Inteligencia Artificial, plantearía un riesgo legal frente a criterios de admisibilidad probatoria como el estándar Daubert. Ya que la incapacidad de explicar la metodología subyacente de un algoritmo, podría invalidar la evidencia por falta de fiabilidad científica, esto obligaría a posicionar a la transparencia algorítmica y la explicabilidad, como requisitos indispensables para la validez del dictamen pericial.

Paralelamente, la capacidad técnica de ejecutar una auditoría continua introduciría una tensión ética entre la eficacia investigativa y el derecho a la privacidad. En consecuencia, el investigador forense debe operar bajo los principios de proporcionalidad y necesidad, alineando sus procedimientos con marcos legales para no vulnerar el derecho a la privacidad en la búsqueda de la verdad económica.

Ante la constante evolución de la era digital, surgen importantes líneas de investigación futura. En primer lugar, se requeriría el desarrollo de estudios empíricos que midan la eficacia de los algoritmos de Aprendizaje No Supervisados, frente a la reducción de «falsos positivos» en auditorías continuas realizadas en sectores corporativos específicos. En segundo lugar, resultaría necesario investigar, desde el ámbito del derecho informático y contable, la implementación de normas legales para la admisión de evidencias generadas por IA predictiva en tribunales latinoamericanos. Finalmente, futuras investigaciones deberían proponer modelos pedagógicos que integren la ciencia de datos, la criptografía y el análisis *on-chain* en la formación de pregrado y posgrado en la contaduría 4.0. En última instancia, estaríamos frente a la transformación de la contabilidad forense, lo que haría necesaria la evolución del perfil del contador público hacia una figura híbrida, convirtiéndolo en un experto con competencias transversales en analítica de datos, jurisprudencia y finanzas.

Declaración sobre asistencia en la redacción y edición

Para la culminación de este manuscrito, el autor recurrió a servicios de corrección de estilo y revisión de formato por parte de terceros. En el transcurso de dichos servicios, es posible que se emplearan herramientas tecnológicas de asistencia editorial, con el propósito de refinar la gramática y asistir en la traducción al idioma inglés. El autor ha revisado y aprobado la versión definitiva del manuscrito, asumiendo la responsabilidad sobre el contenido intelectual y las conclusiones aquí presentadas.

Referencias

Abdallah, A., Maarof, M. A., & Zainal, A. (2016). *Fraud detection systems: A survey. Journal of Network and Computer Applications, 68*, 90–113. https://doi.org/10.1016/j.jnca.2016.04.007

Albrecht, W. S., Albrecht, C. O., Albrecht, C. C., & Zimbelman, M. F. (2018). *Fraud examination* (6th ed.). Cengage Learning.

Alles, M. G., Kogan, A., & Vasarhelyi, M. A. (2002). Feasibility and economics of

continuous assurance. *Auditing: A Journal of Practice & Theory, 21*(1), 125–138. https://doi.org/10.2308/aud.2002.21.1.125

Alshurafat, H., Al Shailah, A., & Beattie, C. (2025). Big data analytics and Continuous Auditing in modern forensic investigations: Frameworks, challenges, and empirical evidence. *International Journal of Accounting Information Systems*, 56, 100652. https://doi.org/10.1016/j.accinf.2024.100652

American Institute of Certified Public Accountants [AICPA]. (2023). *Guide to audit data analytics*.

Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big data and analytics in the modern audit engagement: Research needs. *Auditing: A Journal of Practice & Theory, 36*(4), 1–27. https://doi.org/10.2308/ajpt-51680

Association of Certified Fraud Examiners [ACFE]. (2024). *Report to the nations: Global study on occupational fraud and abuse.*

Baader, G., & Krcmar, H. (2018). Reducing false positives in fraud detection: Combining the red flag approach with process mining. *International Journal of Accounting Information Systems, 31*, 1–16. https://doi.org/10.1016/j.accinf.2018.09.001

Baesens, B., Van Vlasselaer, V., & Verbeke, W. (2015). *Fraud analytics using descriptive, predictive, and social network techniques: A guide to data science for fraud detection*. John Wiley & Sons.

Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical Science,* 17(3), 235–255. https://doi.org/10.1214/ss/1042727940

Bonyuet, D. (2020). Overview and impact of blockchain on auditing. *International Journal of Digital Accounting Research*, *20*, 31–43. https://doi.org/10.4192/1577-8517-v20_2

Breisman, A. (2019). *Crypto-forensics: Investigating cryptocurrency crime*. Routledge.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet* (3rd ed.). Academic Press.

Chan, D. Y., & Vasarhelyi, M. A. (2011). Innovation and practice of Continuous Auditing. *International Journal of Accounting Information Systems, 12(*2), 152–160. https://doi.org/10.1016/j.accinf.2011.01.001

Cho, S., Vasarhelyi, M. A., Sun, T., & Zhang, C. (2020). Learning from the past: A machine learning approach to identify deficiencies in internal controls. *Journal of Emerging Technologies in Accounting, 17*(1), 13–20. https://doi.org/10.2308/jeta-52726

Coderre, D. (2009). *Computer aided fraud prevention and detection: A step-by-step guide*. John Wiley & Sons.

Council of Europe. (2001). *Convention on cybercrime (Budapest Convention)*. European Treaty Series - No. 185.

Cressey, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement*. Free Press.

Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. *Journal of Information Systems,* 31(3), 5–21. https://doi.org/10.2308/isys-51804

Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).

Deloitte. (2023). *Blockchain technology and its potential impact on the audit and assurance profession*. Deloitte Development LLC.

Dorminey, J., Fleming, A. S., Kranacher, M. J., & Riley, R. A. (2012). The evolution of fraud theory. *Issues in Accounting Education,* 27(2), 555–579. https://doi.org/10.2308/iace-50131

European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation).*

Foley, S., Karlsen, J. R., & Putnins, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *The Review of Financial Studies, 32*(5), 1798–1853. https://doi.org/10.1093/rfs/hhz015

Gepp, A., Linnenluecke, M. K., O'Neill, T. J., & Smith, T. (2018). Big data techniques in auditing research and practice: Current trends and future opportunities. *Journal of Accounting Literature, 40*, 102–115. https://doi.org/10.1016/j.acclit.2017.05.003

Golden, T. W., Skalak, S. L., & Clayton, M. M. (2011). *A guide to forensic accounting investigation* (2nd ed.). John Wiley & Sons.

Gottschalk, P. (2010). *White-collar crime: Detection, prevention and strategy in business enterprises.* Universal-Publishers.

Huber, W. D. (2017). Forensic accounting, fraud theory, and the end of the fraud triangle. *Journal of Theoretical Accounting Research*, *12*(2), 28–49.

International Federation of Accountants. (2009). *International Standard on Auditing (ISA) 240: The auditor's responsibilities relating to fraud in an audit of financial statements.*

International Organization for Standardization. (2013). ISO/IEC 27001:2013 *Information technology—Security techniques—Information security management systems—Requirements.*

Karajovic, M., Kim, H. M., & Laskowski, M. (2019). Thinking outside the block: Projected phases of blockchain integration in the accounting industry. *Australian Accounting Review, 29*(2), 319–330. https://doi.org/10.1111/auar.12280

Kaya, M., & Özer, G. (2023). The impact of digital transformation and blockchain technology on forensic accounting and fraud examination: A systematic literature review. *Journal of Accounting & Organizational Change*, 19(5), 785–810. https://doi.org/10.1108/JAOC-02-2022-0034

Kranacher, M. J., & Riley, R. (2019). *Forensic accounting and fraud examination* (2nd ed.). John Wiley & Sons.

Mason, S., & Seng, D. (2017). *Electronic evidence* (4th ed.). Institute of Advanced Legal Studies.

McLeay, M., Radia, A., & Thomas, R. (2014). Money creation in the modern economy. *Bank of England Quarterly Bulletin*, 54(1), 14–27.

National Institute of Standards and Technology [NIST]. (2006). *Guide to integrating forensic techniques into incident response* (NIST Special Publication 800-86).

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Information & Management, 48*(2-3), 96–104. https://doi.org/10.1016/j.im.2010.12.001

Nigrini, M. J. (2011). *Forensic analytics: Methods and techniques for forensic accounting investigations.* John Wiley & Sons.

Nigrini, M. J. (2012). *Benford's law: Applications for forensic accounting, auditing, and fraud detection.* John Wiley & Sons.

Nigrini, M. J. (2019). The patterns of the numbers used in occupational fraud schemes. *Managerial Auditing Journal*, *34*(5), 602–622. https://doi.org/10.1108/MAJ-02-2018-1800

Ozili, P. K. (2024). Artificial intelligence and machine learning in forensic accounting and auditing: A comprehensive review of recent developments. *Journal of Financial Crime*, 31(2), 415–432. https://doi.org/10.1108/JFC-05-2023-0104

Perols, J. L. (2011). Financial statement fraud detection: An analysis of statistical and machine learning algorithms. *Auditing: A Journal of Practice & Theory, 30*(2), 19–50. https://doi.org/10.2308/ajpt-50009

Public Company Accounting Oversight Board [PCAOB]. (2023). *AS 2401: Consideration of fraud in a financial statement audit.*

Rezaee, Z., & Wang, J. (2019). Big data, big data analytics, and forensic accounting. *The Journal of Forensic & Investigative Accounting*, 11(1), 254–257.

Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745.

Singleton, T. W., & Singleton, A. J. (2010). *Fraud auditing and forensic accounting* (4th ed.). John Wiley & Sons.

Soltani, B. (2014). The anatomy of corporate fraud: A comparative study of high profile American and European corporate scandals. *Journal of Business Ethics*, 120(2), 251–274. https://doi.org/10.1007/s10551-013-1660-z

Vasarhelyi, M. A., Kogan, A., & Tuttle, B. M. (2015). Big data in accounting: An overview. *Accounting Horizons*, 29(2), 381–396. https://doi.org/10.2308/acch-51071

Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal*, 74(12), 38–42.

Yermack, D. (2017). Corporate governance and blockchains. *Review of Finance*, 21(1), 7–31. https://doi.org/10.1093/rof/rfw074