



Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado



Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

MAESTRÍA EN CONTABILIDAD INTERNACIONAL

TESIS

Análisis comparativo sobre la evidencia electrónica
de auditoría en las NIIF y US GAAP

ESTUDIANTE: MANUEL FERREIRA

DIRECTORA DE TESIS: ANA CECILIA DRISALDI

DICIEMBRE 2024



Dedicatoria

Dedico esta tesis, en primer lugar y con sincero agradecimiento, a mis padres. Su apoyo incondicional y su ejemplo siempre me impulsaron hacia mis sueños y a convertirme en el profesional que hoy soy. Gracias a ustedes, esto ha sido posible.

A mi pareja, Marlene Mereles, que estuvo conmigo a lo largo de cada paso de esta Maestría en Contabilidad Internacional. Este viaje, único y compartido, fue una experiencia invaluable de aprendizaje conjunto; espero que podamos repetirlo pronto en un nuevo desafío, quizás en el ámbito de un doctorado. Tu comprensión, paciencia y amor constantes hicieron de esta etapa algo alcanzable. Sin ti, habría sido infinitamente más difícil.

A mi hija, pequeña aún, cuya presencia me inspira diariamente a ser mejor. Ella me recuerda el propósito real detrás de mis esfuerzos. Este logro es para ti también.

A mis hermanas, que siempre estuvieron allí con su apoyo incondicional en cada etapa de mi vida, sosteniéndome en los momentos complejos y celebrando cada logro a mi lado.

Finalmente, dedico este trabajo a los profesionales de la auditoría que, en un entorno tecnológico en constante transformación, se esfuerzan cada día por mantenerse actualizados. Espero que este estudio sobre evidencia digital aporte valor al campo y contribuya a abrir nuevas vías de conocimiento que fortalezcan la práctica profesional en esta era de cambios.



Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado



Agradecimiento

Un especial agradecimiento a la Directora de Tesis Ana Drisaldi, su visión única alcanzada a partir de la experiencia en multinacionales es una fuente invaluable de conocimientos, sin su ayuda y continua guía, esta tesis no hubiese sido posible.



Resumen

El presente estudio realiza un análisis de la evidencia de auditoría comparando tres normativas: ISA 500, SAS 142 y AS 1105. Cada una de estas normativas se examina en su relación con los marcos NIIF y US GAAP, poniendo especial atención en cómo abordan la suficiencia, calidad y adecuación de la evidencia en auditoría, especialmente en un entorno digitalizado. Este análisis responde a los desafíos que presenta una auditoría en un contexto global, donde la tecnología y la interconectividad juegan un rol central. El enfoque metodológico elegido para esta investigación es cualitativo, con estudios de casos que incluyen fraudes emblemáticos como los de Madoff y Theranos. A través de una metodología no experimental, se analizan datos ya existentes, organizándolos en matrices que comparan y contrastan suficiencia y calidad de la evidencia. Con este enfoque, se destacan las limitaciones y fortalezas que cada normativa presenta para manejar la evidencia electrónica. Los resultados obtenidos revelan que, aunque las tres normativas comparten principios fundamentales, existen diferencias sustanciales en su orientación sobre la evidencia electrónica. Estas diferencias impactan la coherencia en las prácticas de auditoría a nivel global. La falta de uniformidad en los requisitos establecidos entre US GAAP y NIIF sobre la evidencia es uno de los principales problemas que se pudieron hallar. Esto aumenta la dificultad de llevar adelante auditorías que sean homogéneas en distintos contextos internacionales. La adaptación de metodologías de auditoría al siempre cambiante contexto digital es una de las implicaciones prácticas de esta tesis. Esta adaptación deberá darse a través de la modernización de técnicas de auditoría forense. Además, a nivel social, el estudio refuerza la relevancia de la transparencia y el rigor en auditoría, factores que son esenciales para mantener la confianza pública en los sistemas financieros globales.

Palabras clave: auditoría electrónica, normativas de evidencia, US GAAP vs NIIF, fraude financiero.



Abstract

The present study conducts an analysis of audit evidence by comparing three standards: ISA 500, SAS 142, and AS 1105. Each of these standards is examined in relation to the IFRS and US GAAP frameworks, with a particular focus on how they address the sufficiency, quality, and adequacy of audit evidence, especially within a digitalized environment. This analysis responds to the challenges posed by auditing in a global context, where technology and interconnectivity play a central role. The methodological approach selected for this research is qualitative, using case studies that include landmark frauds such as those of Madoff and Theranos. Through a non-experimental methodology, existing data are analyzed and organized into matrices that compare and contrast the sufficiency and quality of evidence. This approach highlights both the limitations and strengths of each standard in handling electronic evidence. The findings reveal that while the three standards share fundamental principles, there are substantial differences in their guidance regarding electronic evidence. These differences impact the consistency of audit practices at a global level. The lack of uniformity in requirements established between US GAAP and IFRS for evidence is one of the main issues identified, which increases the difficulty of conducting homogeneous audits across diverse international contexts. One of the practical implications of this thesis is the need to adapt audit methodologies to the ever-evolving digital landscape. This adaptation should involve modernizing forensic audit techniques. Additionally, at a societal level, the study reinforces the importance of transparency and rigor in auditing, factors essential to maintaining public trust in global financial systems.

Keywords: electronic auditing, evidence standards, US GAAP vs IFRS, financial fraud.



Índice

Introducción.....	9
Resumen del proyecto.....	9
Justificación	10
Planteamiento del tema/problema.....	10
Objetivos.....	12
Hipótesis	12
Metodología y técnicas a utilizar	13
Cronograma	14
Marco teórico	15
Introducción.....	15
Definición de conceptos y temas.....	19
Evidencia de auditoría	19
Suficiencia y adecuación.....	20
Relevancia y fiabilidad	20
Uso de la tecnología en la evaluación de la evidencia	21
Big data en la auditoría.....	21
Trabajo de expertos externos	22
Desafíos y oportunidades del big data en auditoría.....	22
Análisis de datos en auditoría forense	23
Muestreo estadístico en auditoría	23
La auditoría en la cripto esfera	24
Justificación de la selección de los casos.....	27
Caso Madoff	28
Fallas en la auditoría y regulación financiera en el fraude de Madoff.....	28
Automatización: el origen de la reputación de Bernard Madoff	30
La debilidad fundamental en la auditoría y el uso de la evidencia electrónica.....	31
Feeder funds y la falta de control sobre los fondos	33
La evidencia electrónica como mitigador del riesgo en auditoría	33
Pérdida de datos electrónicos.....	35
Inteligencia artificial en el fraude financiero	35
La falsificación electrónica: un desafío y una oportunidad	37
Auditoría continua y monitoreo electrónico en tiempo real.....	39



La regulación financiera y la falta de transparencia.....	40
ISA 500: evidencia de auditoría	40
SAS 142: evidencia de auditoría.....	42
AS 1105: evidencia de auditoría	42
Cumplimiento de los objetivos para el caso de estudio.....	43
Suficiencia y adecuación.....	43
Evaluación de la calidad de la evidencia.....	44
Caso Olympus	44
La Influencia de la cultura corporativa en la detección y prevención de fraudes contables...46	
Impacto del fraude en la reputación de los auditores y la reacción del mercado.....	48
El caso Olympus: un ejemplo de fraude financiero complejo	49
Evidencia electrónica y su rol en la auditoría de fraudes contables	52
Aplicación de normativas internacionales: ISA 500, SAS 142 y AS 1105.....	53
Lecciones del caso Olympus y su relevancia para la auditoría internacional	53
Cumplimiento de los objetivos para el caso de estudio.....	54
Suficiencia y adecuación.....	54
Evaluación de la calidad de la evidencia.....	55
Caso Peregrine.....	56
El fraude financiero y su impacto en las organizaciones	56
La importancia de la evidencia de auditoría en la prevención del fraude.....	57
Diferencias en la evidencia de auditoría entre US GAAP y NIIF.....	58
La importancia de la confirmación electrónica.....	59
El control interno y el rol de los auditores.....	60
La bancarrota de PFG y la gestión post-fraude	61
Profesionalismo y escepticismo en la auditoría.....	61
Evidencia electrónica y auditoría en el entorno financiero global.....	62
Impacto de la falta de homogenización en la práctica de auditoría internacional	62
Cumplimiento de los objetivos para el caso de estudio.....	63
Suficiencia y adecuación.....	63
Evaluación de la calidad de la evidencia.....	64
Caso Theranos	65
El inicio de Theranos: la promesa de una tecnología revolucionaria.....	65
Liderazgo ético y cultura corporativa	67



La evidencia exógena y su relevancia en la auditoría.....	68
La manipulación de la evidencia y el papel de la auditoría	69
El uso fraudulento de la evidencia electrónica	71
El declive y desenlace de Theranos.....	74
Cumplimiento de los objetivos para el caso de estudio.....	75
Suficiencia y adecuación.....	75
Evaluación de la calidad de la evidencia.....	76
Caso Exchange FTX.....	77
Introducción a los fraudes contables en contexto criptográficos	77
Deficiencias en la evidencia electrónica y su impacto en la auditoría de FTX.....	79
Impacto del colapso de FTX en los mercados de criptomonedas.....	81
El ascenso y caída de FTX	83
La manipulación de la evidencia electrónica y su rol en el fraude contable	85
Vulnerabilidad y riesgos en el control de claves privadas	88
Conectividad entre criptoactivos y el contagio de riesgos	89
Gobernanza corporativa y la necesidad de regulaciones más estrictas.....	90
Cumplimiento de los objetivos para el caso de estudio.....	95
Suficiencia y adecuación.....	95
Evaluación de la calidad de la evidencia.....	96
Evidencia electrónica en los casos de estudio - comparación de la ISA 500, SAS 142 y AS 1105	98
Conclusión Final.....	101
Referencias bibliográficas.....	103
Siglas y Acrónimos	108
Anexo I: El esquema ponzi y la figura de Carlo Ponzi.....	110
Anexo II: Propuesta de un marco regulatorio para criptomonedas según Jennifer J. Schulp ...	112
Anexo III: caso Madoff – mapa mental.....	114
Anexo IV: caso Olympus – mapa mental	115
Anexo V: caso Peregrine – mapa mental.....	116
Anexo VI: caso Theranos – mapa mental	117
Anexo VII: caso Exchange FTX – mapa mental.....	118



Introducción

Resumen del proyecto

El propósito del proyecto de tesis es, fundamentalmente, efectuar un análisis comparativo de la evidencia de auditoría, esto, bajo el prisma de tres normativas específicas: ISA 500¹, SAS 142² y AS 1105³.

El interés personal en la auditoría financiera es lo que motivó la selección de este tema, además de que se percibe una creciente necesidad en el sector contable. Dicha necesidad consiste en entender las diferencias y semejanzas que existen entre las normativas internacionales —NIIF⁴— y las estadounidenses —US GAAP⁵—.

La importancia del análisis radica en la calidad y suficiencia de la evidencia de auditoría. Estas son fundamentales para asegurar la confiabilidad en los estados financieros auditados. Esto cobra especial relevancia en una Maestría en Contabilidad Internacional, donde la rigurosidad es esencial.

Por su parte, los estándares ISA 500, SAS 142 y AS 1105 proporcionan guías clave. Orientan al auditor en la obtención y evaluación satisfactoria de la evidencia y, aunque hay diferencias entre estos estándares y su aplicación en distintos países, los principios de fondo presentan similitudes notables.

Comprender esas diferencias, a pesar de todo, resulta crucial, porque facilita la mejora en la práctica de la auditoría a nivel global. Durante el análisis cualitativo, se abordará la calidad, adecuación y cantidad de la evidencia de auditoría emitida por cada normativa. Además, se evaluará las normativas sobre evidencia electrónica.

El cronograma propuesto para este proyecto incluye investigación, revisión de literatura, descripción de casos y comparación, redacción y conclusión. Se terminará la tesis a fines de 2024.

¹ ISA 500: International Standard on Auditing 500, Norma sobre evidencia de auditoría.

² SAS 142: Statement on Auditing Standards, Norma sobre evidencia de auditoría.

³ AS 1105: Auditing Standard, Norma sobre evidencia de auditoría.

⁴ Normas Internacionales de Información Financiera.

⁵ Generally Accepted Accounting Principles (Principios de Contabilidad Generalmente Aceptados en EE.UU.)



Justificación

La elección del tema de esta tesis tiene una base clara: la necesidad de realizar un análisis comparativo sobre la evidencia de auditoría entre las normativas ISA 500, SAS 142 y AS 1105. Este interés surge tanto de un interés personal en la auditoría financiera, como de la creciente demanda en el sector contable. Existe, de hecho, una necesidad de entender mejor las diferencias y semejanzas entre normativas internacionales y estadounidenses.

Los antecedentes de esta investigación están en la evolución de los estándares de auditoría y también, en la complejidad que estos han alcanzado. Además, no se puede ignorar la globalización de los mercados financieros. Esta globalización exige un entendimiento actualizado y profundo de los marcos regulatorios. El análisis de la evidencia de auditoría es clave en la Maestría en Contabilidad Internacional. La razón es simple: la calidad y suficiencia de la evidencia son fundamentales. Son la base para asegurar la confiabilidad de los estados financieros auditados.

Las normativas ISA 500, SAS 142 y AS 1105 establecen directrices importantes, estas guían al auditor en la recopilación y evaluación de la evidencia. Aunque comparten principios similares, hay diferencias relevantes. Esas diferencias impactan la práctica de la auditoría en distintas jurisdicciones. El contexto globalizado hace el asunto aún más relevante. Las empresas operan bajo distintos marcos regulatorios. Por ello, es esencial entender estas variaciones para mantener prácticas coherentes y efectivas tanto a nivel local como internacional.

El objetivo de este trabajo es claro: contribuir al conocimiento en auditoría mediante un análisis comparativo exhaustivo de las normativas mencionadas. Así se busca aportar claridad sobre los principios que rigen la evidencia de auditoría. El proyecto no solo se enfoca en clarificar. También, pretende identificar áreas susceptibles de mejora. Además, busca sentar bases para futuras investigaciones. Finalmente, pretende ofrecer material académico y práctico que sea útil en la formación de auditores.

Planteamiento del tema/problema

Las Normas Internacionales de Información Financiera (NIIF) son directrices contables establecidas por el Consejo de Normas Internacionales de Contabilidad (IASB). Las



NIIF tienen por objetivo asegurar coherencia, transparencia y comparabilidad a nivel global entre varios otros objetivos.

Las NIIF se aplican en más de 140 países. Entre ellos se encuentran la Unión Europea, Canadá y gran parte de Asia. También América Latina adopta estas normas.

En contraste, en Estados Unidos se usan los Principios de Contabilidad Generalmente Aceptados (US GAAP) que son desarrolladas por el Consejo de Normas de Contabilidad Financiera (FASB). Las empresas que cotizan en las bolsas de Estados Unidos deben seguir el US GAAP. La elección entre NIIF y US GAAP depende de varios factores. La ubicación de la empresa es uno, también las regulaciones locales y finalmente, influyen los requisitos de los mercados de capitales.

El tema central de esta tesis es la comparación de tres normativas de auditoría: ISA 500, SAS 142 y AS 1105. El enfoque está en sus diferencias y semejanzas en la evidencia electrónica.

La ISA 500 se ocupa de la obtención de evidencia de auditoría suficiente y adecuada. Es responsabilidad del auditor respaldar sus conclusiones con esta evidencia. La SAS 142 se enfoca en los atributos de la información utilizada como evidencia. Se consideran factores como relevancia y fiabilidad.

Por otro lado, la AS 1105, normativa de la *Public Company Accounting Oversight Board* o Consejo de Supervisión Contable de Empresas Públicas (PCAOB), da pautas sobre la evidencia de auditoría. Su énfasis está en la calidad y cantidad de la información obtenida. Esta investigación pretende explorar cómo las diferencias entre estas normas afectan la práctica de la auditoría. Tanto en un contexto global como en el específico de Estados Unidos.

El entorno digital plantea nuevos retos para la auditoría. La evidencia electrónica es crucial. Los auditores enfrentan desafíos significativos porque deben aplicar distintos requerimientos bajo NIIF y US GAAP.

Hay varias dificultades. La primera es evaluar la relevancia de la evidencia electrónica. La segunda, su fiabilidad. También está el reto de adaptarse a las tecnologías de las empresas auditadas. Estas tecnologías incluyen sistemas ERP, bases de datos en la nube y software contable. También sistemas de gestión de documentos y plataformas de big data.



La pregunta principal es: ¿Qué desafíos enfrentan los auditores al aplicar diferentes normas sobre evidencia electrónica? Esto, bajo US GAAP y NIIF, en un escenario internacional.

Existen diferencias en cómo se maneja la calidad de la evidencia electrónica. Estas diferencias pueden afectar las auditorías globales. Los criterios de evaluación pueden variar entre US GAAP y NIIF. Esto puede generar inconsistencias en las conclusiones auditadas. A su vez, podría influir en la confianza en los informes financieros.

Por eso, la segunda pregunta clave es: ¿Cómo impactan las diferencias en la calidad de la evidencia electrónica entre US GAAP y NIIF en las auditorías globales?

La investigación se enfocará en un análisis comparativo, la cual se centrará en la evidencia electrónica. Se delimitará dentro del marco temporal y espacial de las normativas actuales. La metodología incluirá dos enfoques: contrastación empírica de casos prácticos y demostración lógica de los principios en cada normativa.

Objetivos

- **Objetivo general:** Analizar las normativas ISA 500, SAS 142 y AS 1105 para identificar similitudes y diferencias sobre la evidencia de auditoría.
- **Objetivos específicos:**
 - Evaluar los principios fundamentales de cada norma en relación con la suficiencia y adecuación de la evidencia de auditoría.
 - Comparar cómo cada norma aborda la evaluación de la calidad de la evidencia.
 - Analizar y contrastar cómo la ISA 500, la SAS 142 y la AS 1105 orientan sobre la evidencia electrónica en los casos de estudio seleccionados.

Hipótesis

- La falta de homogenización en los requerimientos sobre evidencia electrónica entre US GAAP y NIIF genera desafíos significativos en la práctica de auditoría internacional.



- US GAAP y NIIF manejan la calidad de la evidencia electrónica de manera diferente, impactando la consistencia y eficacia de las auditorías.

Metodología y técnicas a utilizar

Para esta investigación, se seleccionará un enfoque cualitativo. Esta se llevará a cabo a través del uso de estudios de caso con soporte bibliográfico. Este enfoque permitirá un análisis profundo. Se centrará en las normativas ISA 500⁶, SAS 142⁷ y AS 1105⁸. Todo esto, en relación con la evidencia de auditoría.

El diseño de la investigación será no experimental. También, será transversal ya que se analizarán datos ya existentes, sin manipular variables. Además, se centrará en un momento específico del tiempo.

El análisis de los datos tendrá un enfoque comparativo. Se utilizarán tablas y matrices. Se realizará de esta forma para identificar y contrastar similitudes y diferencias entre las normativas. Se evaluarán tres aspectos principales: suficiencia, adecuación y calidad de la evidencia de auditoría. También, se considerarán las directrices sobre evidencia electrónica.

El análisis seguirá una estructura. Estará basado en los objetivos específicos planteados. Esto proporcionará un marco claro para la discusión y, además, facilitará la interpretación de los hallazgos.

La unidad de análisis será precisa: normativas de auditoría. Específicamente, ISA 500, SAS 142 y AS 1105.

Las variables a estudiar serán varias. Primero, la suficiencia de la evidencia de auditoría, luego, su adecuación. También, se analizará la calidad de la evidencia. Por último, la orientación que ofrecen sobre la evidencia electrónica.

La población objeto de estudio estará compuesta por las normativas internacionales y

⁶ Emitida en el año 1980, pero desde entonces ha sido revisada y actualizada constantemente siendo la más importante la realizada en 2009.

⁷ Emitida en el mes de julio de 2020, dicha norma fue emitida con el fin de actualizar y ampliar las consideraciones con los avances tecnológicos, las fuentes de datos externas y que tan complejo se ha convertido el entorno de auditoría.

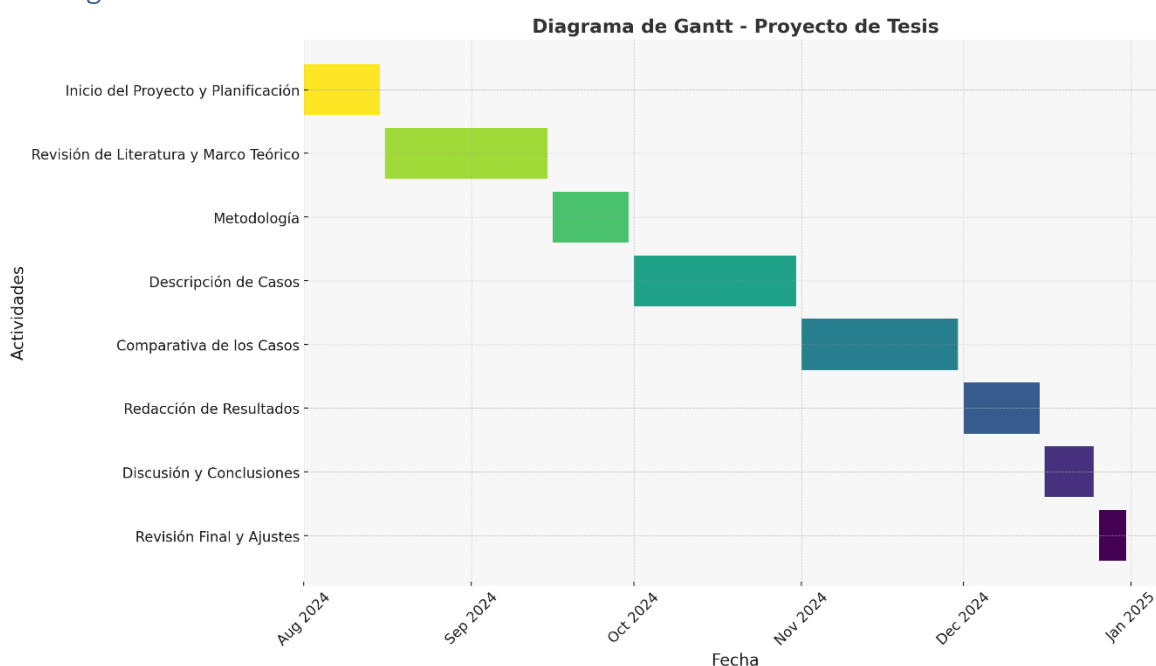
⁸ Emitida en el 2003 como parte del equipo de normas derivadas de la Ley Sarbanes-Oxley del 2002. La AS 1105 fue actualizada desde entonces incluyendo las prácticas de auditoría en entornos tecnológicos.



estadounidenses de auditoría. En cuanto a la muestra, se centrará en los estándares seleccionados: ISA 500, SAS 142 y AS 1105. Estos estándares son relevantes para el tema de la evidencia de auditoría.

La recolección de datos se hará mediante revisión bibliográfica de fuentes secundarias. Entre ellas: artículos académicos, libros, documentos técnicos de organismos de auditoría y otros estudios relevantes. Estas fuentes serán escogidas cuidadosamente. El objetivo es asegurar una cobertura exhaustiva y lograr una comprensión profunda de las normativas en estudio.

Cronograma



Actividad	Inicio	Fin
Inicio del Proyecto y Planificación	01/08/2024	15/08/2024
Revisión de Literatura y Marco Teórico	16/08/2024	15/09/2024
Metodología	16/09/2024	30/09/2024
Descripción de Casos	01/10/2024	31/10/2024
Comparación de los casos	01/11/2024	30/11/2024
Redacción de Resultados	01/12/2024	15/12/2024
Conclusiones	16/12/2024	25/12/2024
Revisión final y ajustes	26/12/2024	31/12/2024



Marco teórico

Introducción

Este trabajo se centra en un análisis comparativo sobre la evidencia de auditoría. ¿Entre qué normas? Las NIIF y US GAAP. El foco estará en tres normativas clave: ISA 500, SAS 142 y AS 1105.

El objetivo es claro: explorar las diferencias y semejanzas en la recolección de evidencia de auditoría. También, analizar la evaluación de dicha evidencia. Además, se estudiará cómo las tecnologías emergentes están influyendo en estos procesos.

Appelbaum, Kogan y Vasarhelyi destacan un desafío constante para la auditoría. La industria debe adaptarse a un entorno globalizado y cambiante. Esto implica ajustarse también a nuevas tecnologías. ¿Cuáles? La nube, el Internet de las Cosas (IoT) y fuentes de datos externas. Mantener la competitividad y relevancia en este contexto es esencial. (Appelbaum, Kogan, & Vasarhelyi, 2017)

Las normas mencionadas son fundamentales para el trabajo de los auditores. ¿Qué proporcionan? Una base para preparar, evaluar y concluir en los informes anuales. Dan criterios detallados sobre cómo recoger, evaluar y utilizar la evidencia de auditoría.

No obstante, las tecnologías de Big Data traen nuevas preguntas. ¿Están estas normas listas para manejar la complejidad y el gran volumen de datos actuales?

La ISA 500 es una normativa relevante emitida por la Federación Internacional de Contadores (IFAC). Ofrece directrices sobre la suficiencia de la evidencia de auditoría. Además, resalta la importancia de la relevancia y fiabilidad de la información obtenida. La SAS 142, por otro lado, es desarrollada por la Junta de Normas de Auditoría (ASB) del Instituto Americano de Contadores Públicos Certificados (AICPA). Esta normativa se enfoca en la fiabilidad de las fuentes de información. Analiza cuán confiable es la evidencia que se va a utilizar en la auditoría.

Finalmente, la AS 1105, creada por el Consejo de Supervisión Contable de Empresas Públicas (PCAOB) en Estados Unidos, se centra en la evaluación de la evidencia externa. Establece un marco detallado para analizar la suficiencia y adecuación de esta información.



Estas normativas son esenciales para garantizar la calidad de las auditorías. Pero, con el avance de las tecnologías, surge la duda: ¿son estas guías suficientes para los desafíos actuales?

Según Allen, Gramling y Hermanson, "los auditores reciben información de diversas fuentes y deben evaluar sus atributos para determinar si pueden ser utilizados como evidencia de auditoría" (Allen, Gramling, & Hermanson, 2023). Esto significa que la calidad de la información es clave. ¿En qué términos? En relevancia y fiabilidad. Esto es esencial para que los informes de auditoría ofrezcan conclusiones precisas y bien fundamentadas.

En un entorno globalizado, las empresas enfrentan retos adicionales. ¿Por qué? Porque operan y son auditadas en múltiples jurisdicciones. Las diferencias regulatorias entre NIIF y US GAAP son parte de estos desafíos.

Comprender estas diferencias y semejanzas es fundamental. Es la base para implementar auditorías consistentes y efectivas. Las normas de auditoría no solo orientan sobre la recolección y evaluación de evidencia. También afectan cómo se interpretan y aplican en distintos contextos.

Por ejemplo, la ISA 500 subraya que la evidencia debe ser suficiente y adecuada. Esto abarca tanto la cantidad como la calidad de la información disponible. (IAASB, 2021)

La SAS 142, en cambio, pone énfasis en la fiabilidad de las fuentes. Suele considerar la información externa más confiable que la proporcionada internamente por la empresa auditada. (AICPA, 2020)

La AS 1105 añade directrices sobre la evaluación de información electrónica. Detalla procedimientos para asegurar su fiabilidad. ¿Qué incluye? La validación de datos y controles efectivos sobre la tecnología de la información utilizada en la auditoría. (Boland, Hermanson, Higgs, Pyzoha, & Zhang, 2024)

Esta norma guía a los auditores en la evaluación de información obtenida de fuentes externas. Se destacan factores como la experiencia de la fuente, la supervisión regulatoria y su relación con la gestión de la empresa auditada. (PCAOB, 2023)

"La calidad (relevancia y fiabilidad) de esta información puede variar ampliamente, haciendo que el trabajo del auditor sea bastante desafiante". (Allen, Gramling, & Hermanson, 2023)



La integración de estos enfoques es vital. Es aún más importante al comparar normas internacionales y estadounidenses como ISA 500, SAS 142 y AS 1105. Estas normas comparten principios sobre la suficiencia y adecuación de la evidencia. Pero, hay variaciones en su aplicación y en qué aspectos se enfocan.

Entender cómo cada norma trata la evidencia electrónica es clave. También lo es comprender sus enfoques sobre la calidad de la información. Esto es esencial para auditorías efectivas y consistentes.

Choo y Tan también destacan la importancia de la capacitación en análisis de datos para los auditores. Esto resulta especialmente relevante en un mundo globalizado. Las empresas, al operar en múltiples jurisdicciones, requieren auditores capacitados en nuevas habilidades. (Choo & Tan, 2022)

En diciembre de 2022, la Public Company Accounting Oversight Board (PCAOB) lanzó una consulta. Buscaba recibir comentarios sobre una nueva norma de auditoría, "The Auditor's Use of Confirmation." Esta normativa aborda el uso de confirmaciones.

Incluye tanto el formato en papel como el electrónico. Además, propone una integración con las normas de evaluación de riesgos. (Boland, Caster, Elder, & Janvrin, 2023)

La propuesta responde a la necesidad de actualizar las prácticas de auditoría. Esto se debe a los avances tecnológicos. También refleja las crecientes demandas en la calidad de la auditoría. Así como en la protección de los inversores (Boland, Caster, Elder, & Janvrin, 2023). La PCAOB sugiere enmiendas para enfrentar estos desafíos. El objetivo es fortalecer la calidad de la auditoría. Todo esto, mediante el uso de herramientas tecnológicas.

Las modificaciones propuestas fueron discutidas por el Comité de Normas de Auditoría de la American Accounting Association. Se busca clarificar las directrices actuales. Además, se pretende reforzar las normas sobre el análisis asistido por tecnología. Las enmiendas insisten en evaluar la fiabilidad de la información electrónica.

Especialmente, la que mantiene la empresa. También subrayan la importancia de los controles tecnológicos. Esto resulta fundamental para garantizar la autenticidad de la evidencia de auditoría. (Boland, Hermanson, Higgs, Pyzoha, & Zhang, 2024)

Por otro lado, se destaca la necesidad de que los auditores adapten sus procedimientos. Es crucial aprovechar las capacidades avanzadas de las nuevas tecnologías. Esto incluye



realizar pruebas detalladas sobre todas las transacciones. También permite auditar continuamente los saldos. Con ello, se busca aumentar la precisión y la eficiencia. (Boland, Hermanson, Higgs, Pyzoha, & Zhang, 2024)

Sin embargo, la adopción de estas tecnologías requiere preparación adecuada. Es esencial validar correctamente los datos. Así, se garantiza que la información utilizada en las auditorías sea completa. Además, se asegura que la información sea exacta. (Boland, Hermanson, Higgs, Pyzoha, & Zhang, 2024)

Entender estas diferencias y similitudes resulta esencial para los auditores. Les permite aplicar un enfoque más crítico en la evaluación de la evidencia de auditoría. Este análisis es crucial no solo para la práctica global, sino también para reguladores y académicos. Estos buscan mejorar la consistencia y efectividad de las prácticas en distintos entornos regulatorios.

En la auditoría forense, la investigación de robos de efectivo ha cobrado gran importancia. La documentación de evidencia también ha ganado relevancia. Esto se debe a la creciente sofisticación de los fraudes. Además, surge la necesidad de técnicas avanzadas para su detección.

Choo y Tan (2022) destacan el valor del análisis de datos. También subrayan la importancia del muestreo estadístico. Estas herramientas son fundamentales para identificar patrones de fraude. Asimismo, permiten evaluar la efectividad de los controles internos.

En su estudio, muestran cómo las técnicas de análisis de datos pueden detectar manipulaciones en registros de ventas. Ejemplos incluyen descuentos falsos, devoluciones y anulaciones, métodos que empleados deshonestos pueden emplear para robar efectivo. (Choo & Tan, 2022)

El Ad Hoc Task Force del Auditing Standards Committee of the American Accounting Association subraya la relevancia de una norma basada en principios. Esta permitiría mayor uso del juicio profesional de los auditores. Además, busca alinearse con las normas de evaluación de riesgos del PCAOB. La propuesta enfatiza la consideración de confirmaciones electrónicas y en papel, así como la inclusión de procedimientos adicionales cuando se utilizan confirmaciones negativas. (Boland, Caster, Elder, & Janvrin, 2023)



Este análisis busca contribuir a una comprensión más profunda. La meta es entender mejor la evolución de las normas de auditoría. Se pretende asegurar que la evidencia recopilada sea de alta calidad. Además, es importante que dicha evidencia sea relevante. Esto cobra especial importancia en un entorno de datos que es cada vez más complejo. También se subraya la necesidad de que los auditores adquieran nuevas habilidades. Es fundamental que adopten enfoques sofisticados para seguir el ritmo de los avances tecnológicos y las crecientes expectativas de los stakeholders en el ámbito financiero. La evolución de estas normativas muestra el entorno dinámico en el que operan los auditores. Comprender las similitudes y diferencias entre normas internacionales y estadounidenses es clave. Este análisis comparativo es relevante para la auditoría tanto en contextos globales como locales. Además, se enfoca en implementar prácticas de auditoría más consistentes y efectivas en un entorno financiero cada vez más interconectado.

Definición de conceptos y temas

En esta sección se presentarán conceptos clave sobre la evidencia de auditoría. Estos conceptos serán definidos y explicados. El enfoque estará en las normas ISA 500, SAS 142 y AS 1105.

Evidencia de auditoría

La evidencia de auditoría es la información que usan los auditores. Con ella, llegan a conclusiones sobre los estados financieros.

Según la ISA 500 5.c), la evidencia de auditoría es "toda la información utilizada por el auditor." Esta información es la base para las conclusiones del auditor. Se incluye la información de los registros contables relacionados con los estados financieros.

Además, abarca otra información relevante. (IAASB, 2021)

La definición resalta dos aspectos cruciales: la suficiencia y la adecuación de la evidencia. La suficiencia se refiere a la cantidad de información recopilada. La adecuación se enfoca en su calidad y pertinencia. Ambos criterios permiten evaluar si la evidencia es suficiente. Y si es relevante para las conclusiones del auditor.



Choo y Tan (2022) destacan que la evidencia debe evaluarse considerando su relevancia y fiabilidad. Esto es crucial para asegurar que respalde de manera adecuada las conclusiones del auditor.

En auditorías forenses, como en la investigación de robos de efectivo, el análisis de datos es esencial. El muestreo estadístico también juega un papel importante. Estas herramientas son vitales para identificar patrones de fraude. Además, permiten documentar de forma clara y precisa la evidencia obtenida. (Choo & Tan, 2022)

De manera similar, Boland y otros afirman que la evidencia de auditoría comprende toda la información utilizada por el auditor. Esta información permite llegar a conclusiones que sustentan la opinión de auditoría. La evidencia puede incluir datos de confirmaciones y otras fuentes, tanto internas como externas. Para su uso en la evaluación de las afirmaciones de los estados financieros, debe ser relevante y fiable. (Boland, Caster, Elder, & Janvrin, 2023)

Suficiencia y adecuación

La suficiencia y la adecuación son conceptos clave en la auditoría. La suficiencia se refiere a la cantidad de evidencia obtenida. La adecuación, en cambio, se enfoca en la calidad de la evidencia.

En la SAS 142 (A9), se menciona que "la suficiencia y la adecuación de la evidencia de auditoría están interrelacionadas." Además, en el apartado 6, último párrafo, se indica que "la cantidad de evidencia de auditoría necesaria está afectada por el riesgo evaluado de incorrección material." También depende de la calidad de la evidencia obtenida. (AICPA, 2020)

Esto significa que los auditores deben obtener una cantidad suficiente de evidencia. Al mismo tiempo, esta evidencia debe ser adecuada. Solo así se puede reducir el riesgo de errores materiales en los estados financieros. El objetivo es alcanzar un nivel aceptablemente bajo de riesgo.

Relevancia y fiabilidad

La relevancia y la fiabilidad son atributos críticos en la evidencia de auditoría. La relevancia implica la conexión lógica de la información con el objetivo del auditor. Por



otro lado, la fiabilidad tiene que ver con la precisión de la información. También abarca su integridad y autenticidad.

La AS 1105.07 establece que "la relevancia de la evidencia de auditoría depende de la conexión de la información con el objetivo de auditoría específico" (PCAOB, 2023). La fiabilidad puede verse influida por la fuente de la información. La información proveniente de fuentes externas suele ser más confiable. En contraste, la información obtenida de fuentes internas puede ser menos fiable.

Uso de la tecnología en la evaluación de la evidencia

Con el avance de la tecnología, la evaluación de la evidencia de auditoría ha evolucionado. Las normas actuales reconocen el uso cada vez mayor de tecnologías contables. Estas tecnologías se utilizan para analizar la evidencia electrónica. La tecnología de la información y la comunicación ha transformado la forma en que los auditores recopilan la evidencia. También ha cambiado la manera en que la evalúan. Por ello, los auditores deben comprender los sistemas tecnológicos de las entidades auditadas. Además, deben ser capaces de evaluar estos sistemas adecuadamente (Appelbaum, Kogan, & Vasarhelyi, 2017).

Choo y Tan (2022) subrayan la relevancia del análisis de datos para evaluar la fiabilidad y seguridad de las fuentes electrónicas de información. (Choo & Tan, 2022).

Bollan y otros destacan que la norma AS 1105 ofrece una guía detallada sobre el uso de análisis asistidos por tecnología en la auditoría. Además, la norma establece las responsabilidades del auditor al evaluar la fiabilidad de la información electrónica.

Aclara, también, las diferencias entre las pruebas de detalles y los procedimientos analíticos. Se subraya, en este contexto, la importancia de desagregar la información (Boland, Hermanson, Higgs, Pyzoha, & Zhang, 2024).

Big data en la auditoría

Big Data se refiere a conjuntos de datos extremadamente grandes y complejos. Estos datos son difíciles de procesar con métodos tradicionales de gestión.



En el contexto de la auditoría, Big Data incluye datos provenientes de diversas fuentes. Esto abarca sensores, redes sociales y dispositivos conectados al Internet de las Cosas (IoT). También incluye otras fuentes no tradicionales de datos.

Appelbaum, Kogan y Vasarhelyi (2017) señalan que la integración de Big Data en los sistemas de los clientes ofrece grandes oportunidades para los auditores. Sin embargo, plantea nuevos desafíos. Entre ellos, la calidad y la veracidad de la información.

(Appelbaum, Kogan, & Vasarhelyi, 2017)

Trabajo de expertos externos

El uso del trabajo de expertos externos es un aspecto crucial en la auditoría. La evaluación de la evidencia incluye el análisis del trabajo de estos especialistas. Las normas SAS 142 y AS 1105 ofrecen guías para los auditores. Indican cómo evaluar la información proporcionada por los expertos externos. Esta evaluación sirve para respaldar las conclusiones de auditoría.

Según Allen, Gramling y Hermanson (2023), los auditores deben analizar la competencia de los expertos. También deben evaluar su objetividad. Además, es importante considerar la naturaleza y el alcance del trabajo realizado. Solo así podrá determinarse si la información puede considerarse evidencia de auditoría. (Allen, Gramling, & Hermanson, 2023)

Desafíos y oportunidades del big data en auditoría

Appelbaum et al. (2017) señalan desafíos y oportunidades en el uso de Big Data en auditoría, uno de los principales desafíos es la Verificación de Calidad. La gran cantidad de datos no siempre implica calidad, los auditores deben crear métodos para evaluar la fiabilidad de la información. Especialmente, de datos generados externamente, como en redes sociales.

Otro desafío es garantizar la Evidencia Suficiente y Apropiada, las normas actuales exigen que la evidencia cumpla con estos criterios. En un contexto de Big Data, los auditores deben manejar enormes volúmenes de información, sin embargo, deben asegurarse de que estos datos sean pertinentes y fiables.



El uso de Procedimientos Analíticos Avanzados presenta oportunidades, técnicas como el análisis predictivo y prescriptivo permiten evaluar riesgos de nuevas maneras.

También facilitan la detección de fraudes, pero requieren nuevas habilidades de parte de los auditores.

Finalmente, la Automatización y Eficiencia son ventajas clave, los procesos analíticos pueden hacer las auditorías más eficientes. Herramientas como la auditoría continua permiten la monitorización en tiempo real que reduce tanto el tiempo como los recursos necesarios en auditorías tradicionales. (Appelbaum, Kogan, & Vasarhelyi, 2017)

Análisis de datos en auditoría forense

El análisis de datos en auditoría forense utiliza técnicas avanzadas. Su objetivo es examinar grandes volúmenes de información.

El propósito es identificar anomalías que puedan señalar fraude. Choo y Tan (2022) explican cómo estas técnicas detectan manipulaciones en registros de ventas. Entre ellas, descuentos falsos, devoluciones y anulaciones.

Estos métodos permiten a los auditores forenses identificar pruebas de fraude con mayor precisión. Además, mejoran la eficiencia en la documentación de estas pruebas. La efectividad de la auditoría también aumenta, facilitando la detección de actividades fraudulentas. (Choo & Tan, 2022)

Muestreo estadístico en auditoría

El muestreo estadístico es una técnica utilizada por los auditores. Su objetivo es evaluar la efectividad de los controles internos. Además, verifica la exactitud de los registros financieros.

Para ello, se revisa una muestra representativa de transacciones. Choo y Tan (2022) subrayan la utilidad del muestreo de estimación de atributos. Esta técnica es útil para evaluar el control interno sobre las autorizaciones de ajustes en los registros de ventas. El muestreo estadístico no solo permite a los auditores inferir la efectividad de los controles internos. También facilita documentar de manera sistemática y rigurosa los hallazgos de la auditoría (Choo & Tan, 2022).



La auditoría en la criptoesfera

La criptoesfera ha surgido como un sector clave en la economía digital. Es uno de los más activos y cambiantes. Este dinamismo se debe al auge de las tecnologías blockchain, además, al crecimiento de los criptoactivos, todo esto ha transformado las transacciones financieras; sin embargo, también ha traído nuevos desafíos. La regulación y la auditoría son las áreas más afectadas.

Antes de proseguir con el desarrollo, es necesario intentar definir los términos de criptoactivos, criptomonedas y blockchain. Hasta el momento de redacción de esta tesis, no existe normativa NIIF ni US GAAP que las definan. En cambio, existen definiciones implícitas emitida por el Comité de Interpretaciones de las NIIF que, en junio de 2019, emitió una decisión bajo el título de “Tenencia de Criptomonedas”. Se entiende por criptoactivos a los activos digitales basados en criptografía y tecnología de registro distribuido (blockchain) mientras que, por criptomonedas se entiende como un tipo de criptoactivo que funciona como un medio de intercambio.

La descentralización de las criptomonedas es un factor clave; también lo es la falta de transparencia en algunas operaciones; juntas, han creado un ambiente propicio para el fraude. La auditoría se enfrenta a obstáculos particulares, requiere un conocimiento profundo de la tecnología; además, es necesario entender nuevas formas de fraude. El auge de los criptoactivos ha traído grandes oportunidades, Inversores de todo el mundo se sienten atraídos. Las criptomonedas y los derivados basados en blockchain son los principales focos de interés; pero este crecimiento también ha llamado la atención de actores malintencionados. En los últimos años, han ocurrido fraudes de gran escala, estos eventos han dejado en evidencia las fragilidades del ecosistema cripto. Un caso destacado es el colapso de FTX, este evento desestabilizó el mercado de criptoactivos, Expuso la falta de controles internos en muchas compañías. Según The Institute of Internal Auditors, “el colapso de FTX es un recordatorio contundente de los peligros de operar sin una función robusta de auditoría interna” (IIA, 2023), el impacto fue enorme, miles de inversores resultaron afectados. Este evento también resaltó la urgencia de mejorar la regulación en el ámbito cripto.

La auditoría tradicional enfrenta desafíos específicos en este nuevo entorno, Verificar la propiedad de las criptomonedas es complicado, esto se debe a la descentralización y al



carácter pseudónimo de las transacciones en blockchain. Dupuis et al. explican que “la auditoría de activos digitales requiere una comprensión profunda de las transacciones criptográficas y la microestructura del mercado” (Dupuis, Smith, Gleason, & Kannan, 2023). Esto plantea riesgos únicos para los auditores, por ejemplo, el manejo de claves privadas; también, la verificación de la seguridad en los sistemas de custodia externos. Aunque la tecnología blockchain promete seguridad, el fraude ha aumentado, la descentralización, que debería facilitar la transparencia, ha revelado vulnerabilidades. Un fraude común es el uso de identidades falsas para pasar los controles de Know Your Customer (KYC). Según un experto, “los estafadores adquieren identidades legítimas en el mercado negro y las utilizan para abrir cuentas cripto, lo que les permite mover fondos sin levantar sospechas” (IIA, 2023). Las transacciones descentralizadas complican la detección de estos fraudes. Esto añade dificultades a la auditoría en este ámbito.

Un fraude en la cripto esfera que ha ganado popularidad es el "pig butchering" o "engorde de cerdos". El enfoque es lento y calculado, los estafadores invierten semanas, e incluso meses, para establecer confianza, la manipulación se realiza a través de redes sociales. Con el tiempo, convencen a sus víctimas de transferir activos, prometen rendimientos muy altos, para hacer más creíble la estafa, falsifican documentos financieros. Los expertos lo describen como “un método sofisticado que puede involucrar semanas o meses de manipulación psicológica antes de que la víctima transfiera sus activos” (IIA, 2023). Este tipo de fraude refleja la sofisticación creciente de los delincuentes. También plantea grandes desafíos para los auditores.

Otro fraude habitual en la cripto esfera es el "pump and dump". En este esquema, un grupo de inversores manipula un criptoactivo, promueven el activo de forma exagerada. Inflan su valor rápidamente; cuando el precio está alto, venden sus participaciones de golpe. Esto causa una caída brusca del precio y las pérdidas recaen en quienes no están involucrados en el fraude. Según informes, “este tipo de esquemas son comunes en mercados cripto menos regulados, donde la falta de supervisión permite a los estafadores manipular precios sin enfrentar repercusiones inmediatas” (IIA, 2023). Estos fraudes subrayan la necesidad de supervisión más estricta, también muestran la importancia de auditorías más detalladas.



El crecimiento de los criptoactivos ha sido rápido, los reguladores se esfuerzan por ponerse al día. En Estados Unidos, la CFTC ha tomado un rol importante, regula los derivados de criptomonedas, como el bitcoin; sin embargo, las normativas aún son inciertas. Ernst & Young advierte que “el marco regulatorio para los derivados basados en criptoactivos sigue siendo inmaduro” (EY, 2022). Esta inmadurez genera inseguridad entre los participantes del mercado y también complica la labor de los auditores. La falta de normas claras añade dificultades a la evaluación de transacciones en criptoactivos.

La seguridad de los criptoactivos es otro tema crucial, es un aspecto esencial para la auditoría en este campo. Aunque la tecnología blockchain promete seguridad, no está libre de fallos. Una de las vulnerabilidades más críticas es la gestión de claves privadas, si alguien accede a la clave privada, puede vaciar una billetera por completo y no hay forma de recuperar esos fondos. Los expertos señalan que “si alguien obtiene la clave privada de una billetera cripto, puede vaciarla por completo sin que haya posibilidad de recuperar los fondos” (IIA, 2023). Esto convierte la protección de las claves privadas en una prioridad. También hace indispensable contar con controles rigurosos. Estos mecanismos son esenciales para garantizar la seguridad de los criptoactivos.

En este contexto, la auditoría interna desempeña un papel esencial. Es crucial para que las empresas en la cripto esfera implementen controles efectivos. Ernst & Young subraya la importancia de esta función. Señalan que “la auditoría interna está en la mejor posición para abordar los riesgos únicos de los criptoactivos”. (EY, 2022)

El conocimiento en la detección y prevención del fraude es una ventaja esencial de la auditoría interna. Este factor es clave en el contexto actual. A medida que los criptoactivos se integran al sistema financiero global, esta habilidad se vuelve cada vez más importante. La adaptabilidad de los auditores será fundamental, sin esta capacidad, garantizar la integridad de las operaciones será difícil, evolucionar junto al entorno cripto es una necesidad.

El mercado de derivados de criptoactivos ha crecido rápidamente, este crecimiento ha planteado nuevos retos. En 2021, el volumen de negociación de futuros de Bitcoin y Ether alcanzó niveles históricos, “El volumen global de negociación de futuros basados en Bitcoin y Ether superó los 32 billones de dólares” (EY, 2022). Esta cifra es



impresionante, subraya la necesidad urgente de que las auditorías se adapten a estos cambios y es crucial entender a fondo estos productos. Además, conocer sus riesgos asociados se vuelve imprescindible y requiere un conocimiento detallado de los productos derivados, también de los riesgos asociados a ellos.

A pesar de los avances en la tecnología blockchain, los fraudes continúan. Siguen siendo una amenaza significativa en la criptoesfera. La descentralización de los criptoactivos aporta transparencia a las transacciones, sin embargo, también facilita la anonimización de actores malintencionados. Los auditores deben estar listos para enfrentar estos desafíos. Una tarea clave es supervisar herramientas como los "mezcladores" de criptomonedas, estas herramientas permiten mezclar transacciones. Hacen que rastrear los fondos sea mucho más difícil. Esto añade complejidad al trabajo de auditoría en el entorno cripto.

Justificación de la selección de los casos

La selección de los casos de Bernie Madoff, Olympus, Peregrine Financial Group, Theranos y FTX Exchange se justifica por su importancia. Estos casos permiten estudiar fraudes contables complejos, además, son útiles para evaluar las normativas de auditoría. Las normativas específicas son ISA 500, SAS 142 y AS 1105. La diversidad en los casos seleccionados es clave, esto facilita una comparación bajo distintos marcos regulatorios. Específicamente, se analizan contextos de US GAAP y NIIF.

Caso de Bernie Madoff: Este caso destaca por su complejidad y magnitud, revela fallas significativas en la detección de fraudes financieros. Su análisis es esencial. Permite evaluar cómo las normativas manejan la evidencia, enfocándose en la electrónica. Además, se desarrolló bajo US GAAP. Esto lo hace adecuado para comparaciones con NIIF, incrementando la profundidad del análisis.

Caso de Olympus: El fraude contable de Olympus fue sofisticado, ocultaron pérdidas considerables durante años, este caso permite explorar la suficiencia de la evidencia de auditoría en fraudes corporativos. La evidencia electrónica fue fundamental en la detección de irregularidades, por eso, es un caso central para examinar la efectividad de las normativas.



Caso de Peregrine Financial Group: Russell Wasendorf falsificó documentos durante casi dos décadas, utilizó herramientas digitales para manipular datos. Este caso subraya la dificultad en la validación de evidencia electrónica, es crucial en la auditoría digital moderna, permite revisar cómo las normativas abordan la verificación de calidad y autenticidad en entornos digitales.

Caso de Theranos: Este caso implicó la alteración de información tecnológica y financiera, Theranos presentó datos falsos sobre sus innovaciones, la evidencia electrónica fue crítica para su detección. Su inclusión analiza la capacidad de las normativas en sectores tecnológicos, además, la evaluación de informes técnicos fue fundamental en este caso.

Caso de FTX Exchange: Este caso se enmarca en el ámbito de las criptomonedas, implicó la manipulación del valor financiero mediante Blockchain, las dificultades para rastrear fondos fueron evidentes. Es un caso significativo para evaluar la adaptación de las normativas a tecnologías emergentes ya que plantea la necesidad de actualizar los enfoques tradicionales de auditoría.

En su conjunto, estos casos son representativos, permiten identificar las fortalezas y debilidades en la aplicación de normativas de auditoría, la evidencia electrónica aparece como un factor clave, además, proporcionan una base práctica y teórica para comparar la eficacia de estas normativas, todo ello en un contexto global y tecnológicamente avanzado.

Caso Madoff

Fallas en la auditoría y regulación financiera en el fraude de Madoff

El fraude de Bernard L. Madoff Investment Securities (BLMIS) es el esquema Ponzi⁹ más grande registrado, puso en evidencia fallas serias en los sistemas de auditoría, como también reveló problemas en los servicios de aseguramiento. Este esquema se mantuvo activo por décadas que fue posible gracias a auditorías ineficientes y controles

⁹ Es recomendable que si el lector no conoce qué es el esquema Ponzi prosiga la lectura del Anexo I: El esquema Ponzi y la figura de Carlo Ponzi.



financieros débiles. Además de que los reguladores permanecieron pasivos. Según Hossain (2021), en su documento "An Analysis of Madoff Investment Securities", este fraude destacó problemas estructurales, señaló deficiencias en cómo se realizan las auditorías, y además, enfatizó la urgencia de reformas en los servicios de aseguramiento. (Hossain, 2021)

El caso de Madoff es uno de los fraudes más significativos de la historia moderna ya que el esquema alcanzó un valor de 65 mil millones de dólares gracias a que la reputación de Madoff generaba confianza absoluta, y a todo lo anterior hay que agregar que los reguladores no actuaron adecuadamente como tampoco lo hicieron los auditores, como consecuencia las señales de alerta pasaron desapercibidas durante años.

Un ejemplo clave ocurrió en 2006 cuando la SEC tuvo acceso a registros de la DTC, pero, no se verificaron los datos obtenidos, los informes recibidos mostraban una falta de actividad en las cuentas manejadas por Madoff. A pesar de ello, no se investigó a fondo y tampoco se cuestionaron las explicaciones dadas lo que resultó en una oportunidad perdida para detectar el esquema Ponzi (Office of Investigations, 2009).

El estudio de Ragothaman (2014) añade otra perspectiva al hablar sobre las fallas en la gobernanza corporativa fueron decisivas, también lo fue la falta de controles internos sólidos debido a que los reguladores, al no actuar a tiempo, facilitaron el éxito del esquema, así estas deficiencias permitieron que el fraude continuara sin interrupciones. (Ragothaman, 2014)

Un aspecto central en el caso Madoff fue la falta de auditorías completas. La firma auditora, Friehling & Horowitz, tenía solo tres empleados los cuales no podían realizar una auditoría adecuada para una firma tan grande como BLMIS permitiendo que las fallas en los servicios de aseguramiento pasaron desapercibidas durante años.

Este caso muestra cómo una estructura de auditoría débil puede ser aprovechada, actores malintencionados pueden explotar estas vulnerabilidades y, en consecuencia, la estabilidad del sistema financiero se ve amenazada (Hossain, 2021).

La estructura débil de auditoría en torno a la firma de Madoff fue un factor clave para la duración del fraude, esta deficiencia permitió que el esquema se mantuviera operativo durante años. Según Hossain, uno de los puntos más críticos fue la selección de la firma auditora Friehling & Horowitz, la cual fue la encargada de auditar los registros



financieros de Madoff pero, sin embargo, la magnitud de las operaciones requería una auditoría más sofisticada y profunda. Vinod (2009) también enfatiza esta situación, señalando que la complejidad de las actividades de Madoff no se ajustaba a la capacidad de esa pequeña firma. (Vinod, 2009)

Un concepto esencial en el estudio de Ragothaman (2014) es el del escepticismo profesional que hace referencia a la postura crítica y cuestionadora que deben asumir los auditores, la idea es evaluar con detenimiento la veracidad de la información financiera. El caso Madoff evidencia la falta de esta actitud, la ausencia de escepticismo permitió que las irregularidades pasaran inadvertidas.

Además, este caso subraya la importancia de que los auditores tengan las herramientas necesarias que incluyen tecnología adecuada y recursos suficientes. Solo así pueden manejar grandes volúmenes de datos por lo que la detección de irregularidades financieras depende, en gran medida, de estos elementos técnicos y profesionales.

Automatización: el origen de la reputación de Bernard Madoff

A principios de los años 1980, Bernard Madoff tomó una decisión estratégica: invertir en tecnología informática. Su objetivo era mejorar la gestión de las órdenes de sus clientes y gracias a la ayuda de su hermano, Peter Madoff, quien lideró el proyecto, la firma desarrolló un sistema automatizado que permitió procesar órdenes con mayor rapidez aumentando, por un lado, la capacidad operativa de BLMIS de forma significativa y, por el otro lado, mejoró el tiempo en la ejecución de órdenes lo que atrajo a grandes inversores institucionales quienes buscaban aprovechar la tecnología para obtener mejores precios y tiempos de ejecución (Ragothaman, 2014).

El éxito del proyecto de automatización fue clave para BLMIS con lo cual la firma se consolida como una de las principales en el NASDAQ permitiendo que en 2008, llegara a ser el sexto mayor creador de mercado. La eficiencia operativa mejoró notablemente, BLMIS logró manejar grandes volúmenes de órdenes e incrementó el flujo de transacciones hacia la firma, además, proyectó una imagen de entidad confiable y tecnológicamente avanzada.

El sistema automatizado, diseñado por Peter Madoff, tuvo un impacto considerable, permitió a BLMIS gestionar la mitad del flujo de órdenes en el New York Stock



Exchange debido a que la firma empleaba tecnología avanzada para ofrecer a los inversores información detallada sobre la actividad del mercado (Ragothaman, 2014). Este uso de tecnología fue fundamental para consolidar su reputación, BLMIS se posicionó como una firma moderna y eficiente en el mercado, además, BLMIS implementó el sistema de "payment for order flow" que consistía en pagar comisiones a brokers. La intención era obtener el derecho a ejecutar las órdenes de sus clientes y, aun cuando esta práctica era legal, generó críticas éticas, especialmente las instituciones financieras cuestionaron su transparencia. A pesar de estas controversias, la tecnología desarrollada jugó un papel crucial en el éxito de la firma.

La debilidad fundamental en la auditoría y el uso de la evidencia electrónica

En la auditoría financiera, detectar fraudes sofisticados es un reto considerable que aumenta cuando hay conspiraciones dentro de la empresa. Los auditores tienen dificultades para obtener evidencia fiable siendo que es clave para verificar los estados financieros y asegurar que no haya irregularidades.

Un aspecto que se subestima es la evidencia electrónica que según Dai y Handley-Schachler (2015), fraudes como el de Bernard Madoff expusieron fallas en la auditoría tradicional. En estos casos, los auditores no detectaron la manipulación de información financiera, esto revela la importancia de gestionar adecuadamente la evidencia digital (Dai & Handley-Schachler, 2015).

La evidencia electrónica incluye registros digitales, correos electrónicos y bases de datos para lo cual usarlas correctamente es esencial para la auditoría. Las tecnologías avanzadas permiten acceder a datos en tiempo real que ayuda a identificar patrones sospechosos en las transacciones financieras, analizar esta evidencia adecuadamente es fundamental para confirmar la autenticidad de las transacciones.

En el caso de Madoff, la SEC no utilizó la evidencia electrónica de forma efectiva, esto permitió que el fraude continuara sin ser detectado hasta la confesión de Madoff, en 2008, que desveló la verdadera dimensión del esquema (Office of Investigations, 2009). Vinod no aborda directamente la evidencia electrónica, pero su análisis destaca un punto clave: la falta de controles electrónicos sólidos facilitó el éxito del esquema Ponzi. La



evidencia digital, como los registros de transacciones, podría haber sido crucial, sin embargo, no se empleó de manera adecuada (Vinod, 2009).

El informe ‘Investigation of failure of the SEC to uncover Bernard Madoff’s Ponzi scheme’ expuso fallas graves en la regulación, en particular, la SEC no gestionó bien la evidencia electrónica, así el reporte resalta que esta falta de gestión impidió detectar las irregularidades inclusive, a pesar de las múltiples denuncias recibidas durante años (Office of Investigations, 2009).

Un ejemplo concreto fue la falta de revisión de registros en la Depository Trust Company (DTC), esta base de datos contiene información sobre transacciones de valores. Según Vinod, si los reguladores hubieran consultado estos registros, habrían visto que Madoff no realizaba las operaciones que afirmaba, esta omisión muestra la importancia de la evidencia electrónica en la detección de fraudes (Vinod, 2009).

En 1992, la SEC investigó a Avellino & Bienes, una firma conectada con Madoff, de la cual se sospechaba formar parte de un esquema Ponzi. La SEC solicitó los registros de transacciones a Madoff directamente, no recurrieron a la Depository Trust Company (DTC), que era una fuente independiente proporcionando datos más fiables. Al depender de la información entregada por Madoff, la investigación perdió imparcialidad. El informe del OIG señala que, si los datos se hubieran contrastado con la DTC, el esquema Ponzi podría haberse descubierto entonces (Office of Investigations, 2009).

Madoff manipuló registros financieros durante muchos años, creaba informes falsos que mostraban altos rendimientos para sus inversores, esos rendimientos sostenían el esquema Ponzi. La falta de una revisión minuciosa de los registros electrónicos fue crucial para la duración del fraude, de este modo, si los auditores hubieran examinado los registros de la Depository Trust & Clearing Corporation (DTCC), habrían detectado que las inversiones no existían (Hossain, 2021).

La evidencia electrónica es esencial en la verificación de transacciones financieras, en el caso de Madoff, una auditoría forense digital habría sido clave, con herramientas de análisis masivo de datos podrían haber identificado irregularidades, los algoritmos especializados habrían detectado patrones anómalos, y los rendimientos constantes de Madoff habrían resultado imposibles de justificar.



El informe del OIG resalta la importancia de la auditoría forense electrónica en fraudes complejos, estas herramientas avanzadas son fundamentales, el análisis de correos electrónicos y registros digitales habría mostrado inconsistencias. La SEC, sin embargo, confió en la información que Madoff ofrecía, nunca cuestionaron sus afirmaciones, aunque fueran dudosas o contradictorias (Office of Investigations, 2009).

Además, el informe menciona que la auditoría forense fue reactiva, no preventiva debido a que la SEC actuó demasiado tarde, si las auditorías electrónicas se hubieran implementado desde el comienzo, muchas señales de alerta habrían sido visibles y el esquema Ponzi de Madoff podría haberse descubierto años antes de su confesión en 2008 (Office of Investigations, 2009).

Feeder funds y la falta de control sobre los fondos

Un aspecto importante del caso Madoff fue el papel de los feeder funds que canalizaban dinero hacia BLMIS de distintas instituciones e individuos, que, al final representaron más del 50% de las pérdidas que reclamaron los inversores. A pesar de que grandes firmas, como KPMG, auditaban estos fondos, no detectaron las irregularidades en la gestión de Madoff, así este error resalta la necesidad de auditorías más detalladas, es crucial incluir el análisis de evidencia electrónica para confirmar la autenticidad de las transacciones (Hossain, 2021).

La falta de transparencia en los feeder funds permitió que el esquema Ponzi se expandiera, por lo que no se detectó a tiempo; con un sistema de monitoreo electrónico continuo podría haber vigilado las transacciones de manera regular, y las irregularidades habrían sido más fáciles de ver.

La evidencia electrónica como mitigador del riesgo en auditoría

La evidencia electrónica es esencial para reducir el riesgo en los procesos de auditoría, debiendo permitir manejar grandes volúmenes de datos de forma eficiente por cuanto en un entorno donde la tecnología es parte fundamental de las operaciones, los registros electrónicos son útiles para auditar transacciones masivas rápidamente puesto que disminuye el margen de error y permite un análisis detallado que abarque múltiples periodos contables (Miller, Cipriano, & Ramsay, 2012).



Otro aspecto importante es la evaluación del riesgo de fraude y los controles internos deficientes en BMIS. Como Madoff tenía un control casi total sobre las operaciones de la firma, le permitió falsificar transacciones, ocultar pérdidas y crear informes financieros fraudulentos que mostraban altos rendimientos consistentes, además de eso la falta de controles internos sólidos en la organización facilitó que Madoff manipulara la información financiera sin ser cuestionado (Ragothaman, 2014).

Los sistemas de auditoría asistidos por computadora (CAATs) son una herramienta clave, considerando que permiten a los auditores comparar grandes cantidades de información, buscan discrepancias entre las bases de datos internas de las empresas y los estados financieros porque estos sistemas procesan registros, generan informes y detectan patrones inusuales; así, añaden una capa extra de control que facilita la detección de fraudes y de irregularidades no evidentes (Dai & Handley-Schachler, 2015).

Vinod también subraya una debilidad crítica, una firma del tamaño de BLMIS dependía de una auditoría realizada por una empresa pequeña y con recursos limitados, y esto cuestiona la capacidad de los sistemas tradicionales para detectar fraudes complejos, por otra parte, una auditoría basada en evidencia electrónica podría haber mitigado estas limitaciones (Vinod, 2009).

Además, la SEC recibió varias denuncias contra Madoff desde los años 1990, sin embargo, falló en su supervisión porque no investigó de manera adecuada las irregularidades señaladas, así la SEC y otras entidades regulatorias no revisaron los informes financieros de Madoff, ni tampoco verificaron los registros electrónicos, que habrían mostrado las discrepancias entre las transacciones reportadas y las reales (Ragothaman, 2014).

Estas herramientas podrían haber identificado patrones inusuales en las transacciones de Madoff, por ejemplo, la falta de inversiones reales a pesar de los altos retornos que reportaba. Por otra parte, una auditoría electrónica continua habría permitido una supervisión en tiempo real de sus actividades financieras, siendo que esto habría reducido el margen para que un fraude de esa magnitud se mantuviera por tanto tiempo.



Pérdida de datos electrónicos

A razón de que una falla importante en la investigación de Madoff fue la pérdida de correos electrónicos críticos, el informe del OIG indica que hubo varios problemas técnicos que afectaron la conservación de correos esenciales, además se perdieron datos por fallos en los sistemas de respaldo, junto a que también hubo cintas dañadas y errores en hardware y software que retrasó la investigación y limitó la capacidad de la SEC para acceder a información clave sobre Madoff (Office of Investigations, 2009).

Debido a estas deficiencias, la SEC contrató a un equipo externo conocido como First Advantage Litigation Consulting Services, su especialidad era la recuperación de datos electrónicos, se encargaron de restaurar los correos perdidos y otros datos electrónicos, pero el proceso de recuperación fue largo y complicado, y aunque algunos datos cruciales se restauraron, las fallas iniciales en la gestión de la evidencia electrónica por parte de la SEC ya habían perjudicado la investigación (Office of Investigations, 2009).

Inteligencia artificial en el fraude financiero

Bernard Madoff y su hermano Peter desarrollaron tecnologías avanzadas, utilizaron lo que Madoff llamaba "inteligencia artificial" para optimizar las operaciones bursátiles, siendo que el objetivo era atraer grandes volúmenes de órdenes (Hossain, 2021). Visto que Madoff fue un pionero en el uso de plataformas electrónicas para procesar compras y ventas en mercados bursátiles, esto proyecta una imagen de sofisticación tecnológica y facilitaba la expansión de su esquema fraudulento.

El sistema de IA mejoró el procesamiento de órdenes dado que permitía a la firma gestionar enormes flujos de operaciones, destacando que, en su punto máximo, Madoff procesaba alrededor del 50% de las órdenes del New York Stock Exchange (Hossain, 2021). Sin embargo, las mismas tecnologías, diseñadas para aumentar la eficiencia, ayudaron a sostener su esquema Ponzi, puesto que los registros electrónicos creados por sus sistemas incluían datos falsificados porque estos mostraban retornos consistentemente positivos, lo cual despertó sospechas en algunos analistas externos, generando una pregunta crucial: ¿qué era realmente esa "inteligencia artificial"? Durante las investigaciones de la SEC, Madoff explicó que usaba un modelo algorítmico para sus operaciones de trading y este modelo era utilizado por hedge funds,



como Fairfield Sentry y Tremont, puesto que el algoritmo sugería cuándo comprar y vender en el mercado, ya que se presentaba como una herramienta eficiente para maximizar ganancias y minimizar riesgos; sin embargo, Madoff admitió que también se basaba en su "instinto" para tomar decisiones finales (Office of Investigations, 2009). Esta mezcla de un modelo algorítmico con decisiones subjetivas generó preocupaciones entre los reguladores por cuanto en el mundo financiero, los algoritmos son comunes en el trading, pero la falta de transparencia sobre el funcionamiento del modelo específico se constituyó en una fuente de dudas, la legitimidad de los retornos consistentes y sin riesgo que generaba Madoff fue cuestionada.

La manipulación de registros electrónicos fue clave para mantener oculto el esquema durante años para lo cual Madoff y su equipo emplearon programas avanzados que falsificaban informes electrónicos de operaciones para así respaldar una estrategia ficticia de inversión, por otra parte, los informes se generaban de forma retroactiva para que las operaciones coincidieran con resultados específicos, haciendo difícil aún más la detección del esquema (Hossain, 2021).

Madoff usaba un programa para ingresar manualmente operaciones de cierre falsas, por lo tanto, podía generar ganancias aparentes y cumplir con los retornos prometidos a los clientes, así, las declaraciones de inversión mostraban siempre un crecimiento positivo manteniendo la ilusión de una estrategia de inversión exitosa (Hossain, 2021). La manipulación tecnológica complicaba el rastreo de transacciones reales, además de, nuevamente, limitar las posibilidades de detección por parte de auditores externos.

Los sistemas electrónicos planteaban dudas sobre las auditorías tradicionales, de ahí que los auditores confiaran en los informes electrónicos que entregaba Madoff, pero estos informes, sin embargo, estaban manipulados digitalmente, por consiguiente, los métodos convencionales de auditoría no fueron suficientes ya que, en tal contexto, revisar solo las transacciones proporcionadas por la firma no bastaba para detectar este tipo de fraude tecnológico (Hossain, 2021).

El modelo algorítmico que Madoff usaba carecía de transparencia, durante varias investigaciones de la SEC, los documentos entregados por Madoff no permitieron una verificación independiente resultando en un aumento de las sospechas sobre la falta de claridad en sus operaciones (Office of Investigations, 2009).



En 2006, la SEC recibió una lista de entidades que, supuestamente, ejecutaban operaciones para Madoff, pero la revisión de estos documentos no esclareció cómo funcionaba el modelo algorítmico, ni tampoco explicaba cómo se lograban los retornos consistentes que Madoff reportaba, además, fueron fallos en la supervisión la falta de verificación externa y la aceptación de las respuestas de Madoff (Office of Investigations, 2009).

Debido a que, la confianza excesiva en los sistemas automatizados sin comprobaciones independientes, el fraude siguió, aun cuando las revisiones limitadas de las plataformas electrónicas, junto con la falta de un análisis tecnológico detallado, revelaron vulnerabilidades en las auditorías contemporáneas.

La falsificación electrónica: un desafío y una oportunidad

Uno de los riesgos del uso de evidencia electrónica es la manipulación de registros digitales, en ese sentido Dai y Handley-Schachler (2015) se refieren a esto como "irregularidades inusuales", siendo que este tipo de fraude incluye la creación de documentos electrónicos falsos, junto a que también puede implicar la alteración de bases de datos a la vez que se usa el hackeo para cambiar datos críticos sin autorización, haciendo todo esto mucho más complicado cuando los auditores no están bien capacitados junto a que pueden basar sus conclusiones en información errónea puesto que esta información puede haber sido diseñada específicamente para engañar.

A pesar de este riesgo, la naturaleza electrónica de los registros financieros ofrece ventajas como, por ejemplo, los auditores pueden utilizar la tecnología para rastrear los cambios no autorizados en los sistemas.

El fraude de Madoff es un ejemplo de manipulación de sistemas electrónicos en una conspiración, así destaca Vinod (2009) que la confianza en la reputación de Madoff fue clave, dado que la falta de supervisión permitió que ocultara sus actividades fraudulentas (Vinod, 2009) en las que Madoff manipulaba datos electrónicos, entre ellos, registros contables y transacciones simuladas, constituyendo este tipo de fraude en un riesgo constante en auditorías de este tipo, sin embargo, las tecnologías avanzadas pueden ayudar a mitigar este riesgo, por lo cual las herramientas de auditoría forense digital son fundamentales. No solo, el análisis de metadatos permite detectar cambios en



los sistemas, sino también monitorear logs de acceso ayuda a rastrear alteraciones en los registros, todas estas técnicas habrían sido esenciales para descubrir las falsificaciones en las operaciones de Madoff.

Los auditores pueden usar herramientas de análisis forense digital para recuperar información eliminada o manipulada, como así también permiten extraer metadatos de archivos electrónicos que indican cuándo y por quién fueron creados, modificados o eliminados los documentos lo que facilita la detección de cambios fraudulentos en los registros financieros, incluso si los conspiradores intentan borrar sus rastros, se pueden identificar las alteraciones gracias a procedimientos más rigurosos y tecnología avanzada, el fraude de Madoff podría haberse descubierto antes.

Uno de los errores graves en las investigaciones de la SEC fue no verificar a través de terceros independientes, sino que, en lugar de buscar registros en bases externas, como la DTC o la National Securities Clearing Corporation (NSCC), la SEC confió en la información dada por Madoff, por lo que esta dependencia comprometió la capacidad de los investigadores para detectar anomalías. En un esquema Ponzi, es fundamental verificar transacciones con fuentes externas, evidentemente la SEC no lo hizo en varias ocasiones, lo que permitió que el fraude de Madoff continuara (Office of Investigations, 2009).

El informe menciona varias ocasiones en que la SEC tuvo acceso a información sobre irregularidades, por ejemplo, en 2006, se descubrió que no había actividad de opciones en las cuentas de Madoff y a pesar de que afirmaba usar una estrategia de "split-strike conversion", basada en opciones, no se detectaron operaciones reales, haciendo esta discrepancia una señal de alerta clara, pero de alguna forma los investigadores no actuaron con la diligencia necesaria.

Además, los investigadores no siguieron las pistas de otros informes externos, como el caso de 2005, donde se presentó una queja formal a la SEC, la denuncia incluía más de 30 señales de alerta sobre las operaciones de Madoff y a pesar de la gravedad de estas advertencias, la SEC no investigó adecuadamente las irregularidades ni tampoco verificó si Madoff operaba con los volúmenes de opciones que afirmaba manejar (Office of Investigations, 2009).



Auditoría continua y monitoreo electrónico en tiempo real

La auditoría continua ha ganado importancia gracias a la evidencia electrónica logrando que este tipo de auditoría permita la revisión constante de transacciones financieras y a diferencia de la auditoría tradicional, que se enfoca en períodos específicos, la auditoría continua es posible gracias a la integración de sistemas electrónicos que facilitan un monitoreo en tiempo real, además de permitir la ejecución automática de ciertos procedimientos de auditoría.

La falta de monitoreo en tiempo real tiene consecuencias, un caso ilustrativo es el de la SEC que, al no analizar registros electrónicos en tiempo real, pierde la capacidad de anticiparse por lo que no pudo actuar a tiempo en el caso Madoff y si hubiera habido sistemas de monitoreo activo, las inconsistencias en sus informes se habrían detectado mucho antes (Office of Investigations, 2009).

La auditoría forense digital va más allá de simple revisar el pasado empleando herramientas avanzadas para analizar los datos a medida que se generan permitiendo identificar problemas en el momento logrando que la revisión de transacciones ya no se limite a lo que sucedió, sino que ahora se puede observar lo que está sucediendo en tiempo real. Dai y Handley-Schachler (2015) critican a la auditoría convencional señalando que basarse en la revisión de transacciones individuales es insuficiente y que esto se debe a que hay fraudes donde los registros electrónicos son manipulados; sin embargo, la auditoría continua facilita la identificación de estas alteraciones.

El uso de tecnologías como el big data y la inteligencia artificial resulta crucial, gracias a las cuales, los auditores pueden analizar grandes volúmenes de datos, y lo hacen en tiempo real, permitiendo detectar patrones anómalos en los sistemas financieros consiguiendo la detección de irregularidades que antes pasaban desapercibidas, por ejemplo, los algoritmos de inteligencia artificial detectan transacciones irregulares basándose en comparar con patrones normales de comportamiento financiero, una desviación en estos patrones puede ser indicativa de un fraude permitiendo que las alertas automáticas permita actuar antes de que el problema se agrave.

El monitoreo continuo tiene otra ventaja permitiendo a los auditores ser proactivos, así no esperan a que el fraude ocurra, sino que lo previenen reduciendo la escala de los problemas antes de que lleguen a niveles críticos.



La auditoría continua es una respuesta a los límites de la auditoría tradicional ya que antes, se dependía de muestreos parciales y análisis tardíos, con la tecnología actual, la auditoría es más eficaz, las organizaciones pueden proteger mejor sus activos, detectar fraudes o errores es más rápido y preciso.

La regulación financiera y la falta de transparencia

Vinod subraya la necesidad de mayor transparencia en la regulación financiera, insiste en mecanismos más sólidos para garantizar la independencia de los auditores, además señala que el esquema Ponzi de Madoff fue posible, en parte, por la falta de supervisión adecuada, además de haber conflictos de interés entre los reguladores y la industria financiera (Vinod, 2009).

Una de las recomendaciones de Vinod es separar la custodia y el asesoramiento financiero, así, se evitaría que las instituciones financieras manipulen los fondos que tienen bajo su custodia, además de proponer una vigilancia más estricta sobre las operaciones electrónicas de los fondos. Estas medidas, según Vinod, habrían sido efectivas para evitar que Madoff enviara reportes falsos y de esa forma el fraude no habría durado tanto tiempo si se hubiera ejercido un control más riguroso (Vinod, 2009).

ISA 500: evidencia de auditoría

La Norma Internacional de Auditoría 500 (ISA 500) establece que el auditor debe obtener evidencia suficiente y adecuada para sustentar sus conclusiones, lo que claro incluye la evidencia electrónica que se considera una parte integral del proceso de auditoría, además, la norma subraya la importancia del escepticismo profesional, gracias a que este enfoque es esencial al evaluar registros electrónicos, hay que tener en cuenta que dicha evidencia, por su naturaleza, es susceptible de manipulación.

El informe del OIG revela fallos en la actuación de la SEC en el caso Madoff, a pesar de detectar contradicciones en la información, no se tomaron acciones, por ejemplo, en 2006, Madoff declaró que había abandonado el uso de opciones cuando sin embargo, la evidencia de los fondos que invertían en él mostraba lo contrario, en la que seguía informando a sus inversores que utilizaba opciones en su estrategia y esta discrepancia



no fue investigada por lo que no se siguieron las pistas que habrían desvelado el esquema Ponzi.

El escepticismo profesional, junto a la evaluación rigurosa de la evidencia, es fundamental como lo fue en el caso de Madoff, la falta de esta práctica permitió que su esquema pasara desapercibido durante años aun cuando hubo múltiples señales de alerta, además, la evidencia electrónica disponible podría haber desenmascarado el fraude.

El informe OIG-5090 resalta la falta de búsqueda de evidencia independiente, señala que la SEC recibió varias quejas sobre Madoff pero, no se verificaron la información con fuentes externas, como tampoco se acudió a la Depository Trust Company (DTC), una entidad clave que podría haber validado las transacciones. La ISA 500 requiere una verificación independiente en una auditoría efectiva lo que garantiza la objetividad y la precisión de la información. (Office of Investigations, 2009).

La ausencia de un enfoque crítico en la evaluación de la evidencia tuvo consecuencias; en la auditoría, la evidencia electrónica debe manejarse con cautela, sin una validación independiente, hay un riesgo alto de manipulación como lo es en el caso Madoff, el cual muestra que la falta de escepticismo y de fuentes externas adecuadas puede ocultar fraudes complejos durante mucho tiempo.

La evidencia electrónica es clave para cumplir con la ISA 500 ya que permite revisar grandes volúmenes de transacciones como así también facilitar la detección de irregularidades de forma más eficaz.

En el caso de Madoff, la SEC no usó herramientas de auditoría forense lo que significó varias oportunidades perdidas debido a que los registros electrónicos no fueron examinados en profundidad y por lo tanto, se dejaron pasar indicios del esquema Ponzi. El uso correcto de la evidencia digital, según la ISA 500, habría sido crucial permitiendo analizar transacciones en tiempo real, además, se podría haber validado la autenticidad de las inversiones que Madoff afirmaba realizar (Office of Investigations, 2009).



SAS 142: evidencia de auditoría

La SAS 142 subraya la necesidad de obtener evidencia suficiente y adecuada en una auditoría, resalta la calidad y confiabilidad de la información como factores cruciales. En el caso de Madoff, el informe del OIG evidenció fallos debido a que la SEC confió demasiado en la información de Madoff y no buscó evidencia electrónica independiente, esto a las claras afectó la objetividad del proceso.

El incumplimiento de la SAS 142 quedó claro cuando la SEC no revisó los registros de la DTC, como tampoco realizó auditorías electrónicas sobre las transacciones financieras que Madoff reportaba, y todas estas omisiones debilitaron la capacidad de la SEC, de haber auditado correctamente, las irregularidades podrían haberse descubierto mucho antes.

La SAS 142 también destaca la importancia de la relevancia de la evidencia, que es crucial en contextos donde la información puede manipularse. En este caso, una revisión independiente de registros electrónicos habría sido clave, habría revelado que las operaciones reportadas por Madoff no existían.

Como se expresó anteriormente, el uso de auditoría forense digital habría sido determinante y habría permitido un análisis más exhaustivo de los datos electrónicos para poder identificar las discrepancias en las transacciones y gracias a los patrones inconsistentes, se habrían expuesto las falsificaciones.

AS 1105: evidencia de auditoría

La AS 1105 establece que el auditor debe evaluar la suficiencia y adecuación de la evidencia obtenida ya que son cruciales para respaldar las conclusiones de la auditoría. En el caso de Madoff, el informe del OIG muestra que la SEC no evaluó correctamente la calidad de la evidencia proporcionada por él, especialmente, esto se reflejó en los registros electrónicos. Si la SEC hubiera aplicado los principios de la AS 1105, habría buscado confirmar la información directamente con fuentes independientes en la cual la DTC habría sido una fuente clave para validar las transacciones reportadas, sin embargo, este paso crucial nunca se llevó a cabo.

La AS 1105 también enfatiza la importancia de la evidencia suficiente y confiable en fraudes financieros que es especialmente relevante en fuentes electrónicas afirmando



que la falta de herramientas de auditoría digital para analizar grandes volúmenes de datos fue un error significativo en la investigación de la SEC.

La auditoría forense digital, conforme a la AS 1105, habría sido esencial, que permitiría revisar los registros electrónicos de Madoff con mayor profundidad y de esta forma, se habrían identificado patrones inusuales y expuesto manipulaciones en los datos de transacciones financieras, al realizar esto, se podría haber detectado mucho antes el fraude.¹⁰

Cumplimiento de los objetivos para el caso de estudio

Suficiencia y adecuación

En el fraude perpetrado por Madoff, se evidenció que la recolección y evaluación de la evidencia fue deficiente. Esta falencia permitió que el esquema Ponzi se mantuviera por un tiempo prolongado. La ISA 500, por ejemplo, pone énfasis en la obtención de evidencia pertinente y confiable. Evalúa si la evidencia recogida por el auditor es adecuada para fundamentar su opinión. Es crucial considerar tanto la calidad como la cantidad de la evidencia. Sin embargo, en el caso Madoff, no se aplicaron con rigor estos principios, especialmente al verificar la autenticidad de la documentación y las operaciones.

Por otro lado, la SAS 142 aborda la calidad de la evidencia desde un ángulo específico. Esta norma incluye aspectos de relevancia y fiabilidad y refuerza cómo se debe interpretar la evidencia obtenida. Además, resalta la importancia de considerar fuentes electrónicas de evidencia. En el caso Madoff, estas fuentes no fueron validadas con la meticulosidad necesaria.

En cuanto a la AS 1105, normativa del PCAOB, se subraya la importancia de que la evidencia permita sustentar de manera coherente los hallazgos de la auditoría. Este estándar exige pruebas sustantivas y de control que certifiquen que las conclusiones del auditor son sólidas. En el fraude de Madoff, la falta de escepticismo y de un análisis

¹⁰ El caso Madoff se puede ver de forma resumida en el Anexo III: Caso Madoff – Mapa Mental.



crítico por parte de los auditores fue evidente. Esto contribuyó a no detectar las señales de alerta que debieron haberse investigado.

La falta de una aplicación rigurosa de estas normativas, junto con una evaluación insuficiente de la evidencia, llevó a que los auditores no pudieran prevenir el fraude. En entornos complejos, como el digital, la aplicación de estos principios debe ser estricta. La revisión no fue exhaustiva al igual que el insuficiente escepticismo, lo que evidenció las debilidades del proceso de auditoría y permitió que el fraude avanzara.

Este análisis demuestra que, para prevenir irregularidades, la adherencia a los principios de suficiencia y adecuación debe ser rigurosa y meticulosa. La aplicación uniforme y la actitud crítica son esenciales. En el caso Madoff, la falta de estas prácticas resultó en una auditoría que falló en detectar un fraude que tuvo repercusiones significativas.

Evaluación de la calidad de la evidencia

En este caso, la revisión de la evidencia no fue lo suficientemente profunda ni adecuada. Esto permitió que el fraude pasara desapercibido. Este hecho resalta la importancia de ajustar los enfoques de evaluación. Adaptar las metodologías se vuelve esencial. La auditoría necesita mantener un nivel de rigurosidad elevado. Este requisito es particularmente crítico en entornos con evidencia electrónica. Los sistemas tecnológicos complejos agravan el panorama. Detectar irregularidades en estos contextos es más difícil.

Los tres estándares enfrentan un desafío compartido. La adaptación de procedimientos tradicionales a entornos digitales se muestra crucial. En el fraude de Madoff, la sofisticación de los sistemas complicó la detección y expuso la necesidad de evaluar consistentemente la calidad de la evidencia en auditorías de este tipo.

Caso Olympus

El fraude contable es un problema recurrente en el ámbito corporativo. Un ejemplo destacado es el escándalo de la Olympus Corporation, descubierto en 2011; notable no solo por la magnitud del fraude, sino también el tiempo que logró ocultarse.



Olympus es una de las principales empresas japonesas especializada en dispositivos médicos, cámaras y equipos de información. La crisis surgió al descubrir maniobras fraudulentas que estaban compuestas por transacciones financieras complejas para encubrir pérdidas significativas. Esto demuestra las dificultades que enfrentan los auditores ante los esquemas diseñados para evitar la detección que complican su labor. En este contexto, evaluar la suficiencia y adecuación de la evidencia de auditoría se vuelve esencial. El impacto del fraude en Olympus fue significativo, las acciones cayeron un 18% el primer día tras el escándalo, y en los días posteriores, la caída total alcanzó el 24%. La pérdida de valor fue de \$1.3 mil millones (Verschoor, 2012). Este caso es clave para entender la evidencia de auditoría, refleja cómo la manipulación de datos financieros facilita fraudes a gran escala, además, una cultura empresarial poco transparente agrava la situación.

La empresa fue sorprendida encubriendo pérdidas millonarias desde los años 90, estas pérdidas derivaban de inversiones fallidas. El caso evidenció serias debilidades en la gobernanza y la ética corporativa de la compañía.

Además, dejó al descubierto fallos graves en los procesos de auditoría, tanto internos como externos. Los auditores involucrados, KPMG en años anteriores y Ernst & Young (E&Y) durante el fraude, no lograron identificar ni reportar las irregularidades financieras, esto permitió que la situación se prolongara por más de una década (Verschoor, 2012).

Frendy y Hu (2011) califican estos errores como una "falla de auditoría" que es la incapacidad del auditor para emitir una opinión modificada en situaciones necesarias (Frendy & Dan, 2012). Este esquema pone en evidencia la necesidad de auditorías exhaustivas, es esencial que evalúen adecuadamente la evidencia, especialmente cuando hay transacciones complejas involucradas.

La falta de controles efectivos fue un factor determinante, los auditores no lograron detectar las maniobras fraudulentas durante varios años, la carencia de controles adecuados facilitó la prolongación del fraude (Elam, Madrigal, & Jackson, 2014).

El fraude en Olympus fue posible gracias a la manipulación de activos conocida como tobashi, que consiste en desviar activos mediante vehículos de propósito especial (SPV) para ocultar pérdidas financieras. El informe del comité especial de Olympus revela que



la empresa había "postergado la contabilización de pérdidas en valores de inversión desde alrededor de los años 90" (Verschoor, 2012).

Este esquema permitió a Olympus encubrir sus pérdidas a través de adquisiciones infladas, también realizaron pagos excesivos a consultores financieros, ni los controles internos ni los auditores externos cuestionaron estos pagos.

El caso de Olympus es significativo para el estudio de la auditoría en fraudes contables, resalta la importancia de recolectar y evaluar adecuadamente la evidencia de auditoría, esto es esencial según las normas internacionales y estadounidenses. En el caso de Olympus, los auditores no lograron obtener evidencia suficiente y adecuada para sus conclusiones, esta fue una de las fallas clave observadas.

El escándalo subraya la necesidad de revisar y mejorar los estándares de auditoría, en especial, es necesario poner atención en la evidencia electrónica, que resulta crucial para detectar fraudes complejos.

La Influencia de la cultura corporativa en la detección y prevención de fraudes contables

En el contexto del fraude contable, la cultura organizacional tiene un papel clave en la prevención, detección y encubrimiento de actos ilícitos. En muchos casos, una cultura corporativa poco ética facilita la ocurrencia de fraudes, en la Corporación Olympus se evidenció cómo una cultura que favorecía la lealtad y el secretismo dificultó la detección temprana del fraude.

El análisis revela que "la cultura de insider en Olympus es reminiscente de Tokyo Electric Power... el instinto predominante en estas firmas es ocultar los errores a toda costa" (Morgan & Burnside, 2014). Esto muestra la complejidad de detectar fraudes cuando la cultura corporativa da prioridad a la lealtad interna y no a la transparencia. Otro estudio señala que los ejecutivos implicados no buscaban beneficios financieros personales, sus acciones se motivaban por "orgullo y un malentendido sobre la reputación de la empresa" (Elam, Madrigal, & Jackson, 2014). Este aspecto resalta la importancia de considerar las implicaciones culturales en la auditoría.



Para los auditores, entender la cultura organizacional es crucial, deben evaluarla al analizar la calidad de la evidencia y la confiabilidad de los controles internos, especialmente en contextos culturales diversos.

El caso de Olympus demuestra el impacto de la estructura organizativa en la calidad de la evidencia en auditorías de fraudes. La investigación reveló que la junta directiva estaba formada, en su mayoría, por personas internas. Este tipo de estructura genera obstáculos significativos para la detección de irregularidades, estas personas eran reticentes a contradecir a los altos ejecutivos de la empresa (Morgan & Burnside, 2014). Esta estructura dificultaba la obtención de evidencia suficiente y adecuada.

Los auditores se enfrentaron a obstáculos significativos para acceder a la información, esto subraya la necesidad de una cultura organizacional abierta más transparente que facilite la labor de los auditores, especialmente en casos de fraudes financieros.

El papel del denunciante, o whistleblower, es también crucial en la detección de fraudes, en muchos casos, este actor proporciona la evidencia clave. En el caso de Olympus, fue el presidente Michael Woodford quien asumió ese rol, descubrió irregularidades financieras y trató de alertar a la junta directiva, sin embargo, la cultura empresarial existente hizo difícil este proceso.

Woodford señaló que "la cultura de la empresa valora la armonía y el consenso"; aun así, enfatizó que "el escrutinio y los desafíos... conducen a mejores decisiones" (Morgan & Burnside, 2014). Esto destaca cómo la resistencia al cambio y la falta de transparencia pueden perjudicar la recolección de evidencia en auditorías de fraudes.

La relación entre la cultura organizacional y los sistemas legales influye en la capacidad de detectar y mitigar fraudes contables, en el caso de Olympus, la cultura japonesa fue un factor determinante; el énfasis en la armonía (wa) y la lealtad a los superiores (giri) contribuyó a la prolongación del fraude, según el estudio, esta cultura "pone más énfasis en la serenidad que en la veracidad, por lo que los japoneses no consideran incorrecto mentir si ser veraz perturba o causa daño a otros" (Morgan & Burnside, 2014).

En contraste, la evidencia de auditoría debe ser precisa y objetiva, esto genera un desafío significativo cuando la cultura corporativa no fomenta la transparencia. En el caso de Olympus, esta discrepancia complicó la detección temprana del fraude.



Un aspecto clave fue el papel de Michael Woodford, presidente y CEO de la empresa, se convirtió en denunciante al identificar grandes discrepancias en las tarifas de fusiones y adquisiciones, fue despedido dos semanas después de hacer públicas sus preocupaciones, pero persistió en su denuncia. Su intervención fue crucial para exponer el fraude.

Este caso resalta el valor de los denunciantes en la detección de fraudes, la recolección de evidencia clave a menudo depende de estos actores, especialmente en contextos donde la estructura interna y la cultura corporativa son obstáculos. Los estándares de auditoría deberían considerar con más profundidad la importancia del papel de los denunciantes (Elam, Madrigal, & Jackson, 2014).

Impacto del fraude en la reputación de los auditores y la reacción del mercado

El fraude de Olympus impactó la percepción sobre la calidad de la auditoría, sin embargo, en Japón, el efecto fue particular, a diferencia de mercados como el estadounidense, no se observó una caída significativa en los precios de las acciones, las empresas auditadas por las firmas implicadas en el fraude mantuvieron sus valores sin grandes alteraciones.

Los estudios muestran que "los inversionistas japoneses no responden de manera significativa a las noticias que afectan la reputación de los auditores asociados con el fraude de Olympus" (Frendy & Dan, 2012). Esto evidencia diferencias en la reacción de los mercados ante fallos en la auditoría, factores culturales y regulatorios influyen en estas respuestas.

El hallazgo refuerza la importancia de considerar factores culturales y legales. Al evaluar la calidad de la auditoría y la evidencia recolectada, es crucial tener en cuenta el contexto específico de cada entorno regulatorio.

El fraude en Olympus revela las debilidades de la auditoría externa cuando los procedimientos no logran identificar irregularidades significativas en los estados financieros. Durante años, la firma auditora KPMG no detectó las pérdidas ocultas, esto se hizo a través de la sobrevaloración de activos y adquisiciones a precios inflados, aunque KPMG eventualmente forzó a Olympus a registrar una pérdida de 55.7 mil millones de yenes en 2009, el hecho de que el fraude permaneciera oculto durante tanto



tiempo destaca la importancia de la suficiencia y adecuación de la evidencia de auditoría. Las normativas ISA 500, SAS 142 y AS 1105 subrayan estos principios esenciales.

El caso de Olympus demuestra cómo la auditoría puede fallar si no se implementan controles rigurosos. La falta de mecanismos de verificación adecuados facilita que las irregularidades no sean detectadas, comprometiendo la integridad de la auditoría (Elam, Madrigal, & Jackson, 2014). En el caso de Olympus, tanto KPMG como Ernst & Young fueron las firmas auditoras en distintos momentos, ambas plantearon preocupaciones sobre adquisiciones específicas y pagos excesivos en tarifas de asesoría, sin embargo, estas inquietudes no se tradujeron en acciones correctivas. Las firmas auditoras no actuaron ante señales claras de irregularidades, esto permitió que el fraude continuara sin ser descubierto.

El caso resalta la importancia de normas como la SAS 142 y la AS 1105, estas normas proporcionan pautas claras para identificar fraudes y evaluar riesgos, también destacan la necesidad de examinar transacciones inusuales o de partes relacionadas, crucial para prevenir manipulaciones financieras (Dutta, Caplan, & Marcinko, 2014).

[El caso Olympus: un ejemplo de fraude financiero complejo](#)

El fraude de Olympus consistió en dos mecanismos fundamentales, uno fue el conocido esquema Tobashi, donde se ocultaban pérdidas transfiriéndolas a entidades ficticias externas, lo que las excluía de los estados financieros; el otro mecanismo giró en torno a la compra de compañías por precios exagerados, encubriendo así pérdidas mediante la contabilización de goodwill (crédito mercantil). Estos métodos, implementados con el apoyo de terceros y a través de entidades fuera de balance, resultaron en una detección más compleja del fraude por parte de los auditores (Fukukawa, Mock, & Srivastava, 2014).

Olympus usó estas entidades para desplazar activos problemáticos fuera del balance, activos obtenidos mediante inversiones de alto riesgo, fueron posteriormente "transferidos" a entidades ficticias, inflando deliberadamente sus valores. Se pretendía, con esta táctica, ocultar las pérdidas hasta que el mercado experimentara una recuperación favorable. Esta maniobra buscaba evitar las obligaciones de transparencia



impuestas por las normativas contables japonesas, y ello complicó enormemente la labor de los auditores. Para ellos, se volvió imprescindible un análisis detallado sobre la calidad de la evidencia obtenida, así como el rastreo meticuloso de las transacciones que involucraban a partes relacionadas. Normativas como la ISA 500 subrayan la importancia de que la evidencia sea suficiente y adecuada, destacando también la relevancia del uso de registros electrónicos y otros documentos al rastrear transacciones financieras complejas (Dutta, Caplan, & Marcinko, 2014).

Los auditores de Olympus, aunque siguieron los procedimientos estándar, no detectaron el fraude. La sofisticación de los esquemas y la manipulación de la evidencia electrónica lo impidieron, en este contexto, la Teoría de las Funciones de Creencia se muestra como una herramienta más robusta. Esta teoría permite evaluar mejor el riesgo de fraude, integra múltiples fuentes de evidencia y ajusta las creencias sobre la probabilidad de fraude, esto se hace con base en la evidencia disponible.

La evidencia de auditoría es esencial, es la base para emitir una opinión objetiva sobre los estados financieros de una empresa. La ISA 500 establece dos criterios: suficiencia y adecuación, esto significa que la cantidad y calidad de la evidencia deben respaldar con confianza las conclusiones del auditor, sin embargo, en el caso de Olympus, la evidencia confiable fue insuficiente; no se obtuvieron pruebas sobre los pagos a consultores financieros, a pesar de su importancia en las transacciones fraudulentas, estos pagos representaban una parte considerable del fraude (Verschoor, 2012).

El fraude en Olympus involucró pagos masivos, superando los 687 millones de dólares, destinados a una entidad ubicada en las Islas Caimán, este fue calificado como "la tarifa más alta en la historia de las fusiones y adquisiciones" (Verschoor, 2012). Tal cifra debió haber generado alertas entre los auditores.

Según la ISA 500, era imperativo que estos profesionales profundizaran en la recolección de evidencia adicional, evaluando la legitimidad y justificación de ese monto tan elevado, sin embargo, no cumplieron con dicha obligación; el fraude, así, continuó sin ser descubierto durante años.

En Estados Unidos, la SAS 142 establece que los auditores deben obtener evidencia que permita responder a los riesgos de fraude identificados en la auditoría. En el caso de Olympus, la obligación incluía considerar los riesgos asociados a pagos inusualmente



elevados a consultores financieros, también debían evaluar las adquisiciones a precios inflados, que no guardaban relación con la actividad principal de la compañía. Sin embargo, estos riesgos fueron desatendidos, poniendo de manifiesto una deficiencia en la aplicación rigurosa de las normativas de auditoría (Verschoor, 2012).

La AS 1105, que rige en las auditorías estadounidenses, destaca la importancia de la fiabilidad de la evidencia de auditoría, este es aún mayor cuando la evidencia proviene de fuentes electrónicas o sistemas complejos. La AS 1105 especifica que los auditores deben considerar los riesgos asociados con la evidencia proveniente de entornos electrónicos y verificar la efectividad de los controles que rigen estos sistemas, además, es esencial que verifiquen que los controles sobre estos sistemas sean adecuados y efectivos.

La auditoría en Olympus falló en este aspecto, las firmas Ernst & Young y KPMG no emitieron las alertas necesarias sobre las prácticas fraudulentas contables que la empresa implementaba. Este escenario no solo permitió que el fraude persistiera, sino que también impactó negativamente la percepción pública sobre la reputación de las firmas auditoras.

Frendy y Hu (2011) destacan una "relación inversa entre la magnitud del fallo de auditoría y la calidad de la auditoría". Este vínculo afecta el valor económico que los mercados financieros asignan a los auditores (Frendy & Dan, 2012).

El caso de Olympus enfatiza la importancia de evaluar de manera adecuada tanto la suficiencia como la adecuación de la evidencia auditora, cuestiones tratadas por las normativas analizadas en esta investigación.

Dutta, Caplan y Marcinko (2014) señalan que "la falta de independencia de los auditores internos y la apatía de los directores contribuyeron a que el fraude pasara desapercibido durante tanto tiempo", este hecho subraya la relevancia de normativas de auditoría como la ISA 500.

La ISA 500 enfatiza la implementación y evaluación de controles efectivos. El objetivo es asegurar que la evidencia de auditoría incluida en los informes financieros sea precisa y confiable (Dutta, Caplan, & Marcinko, 2014).



Evidencia electrónica y su rol en la auditoría de fraudes contables

En el caso de Olympus, la evidencia electrónica fue clave, la empresa manipuló documentos y registros digitales para ocultar sus pérdidas, este tipo de evidencia se ha vuelto cada vez más común en auditorías. Esto se debe al uso extendido de tecnologías digitales en contabilidad y finanzas, sin embargo, la evidencia electrónica presenta riesgos adicionales. Entre ellos, la posibilidad de falsificación o alteración de documentos.

Fukukawa et al. (2014) proponen un enfoque cauteloso para los auditores, que consiste en que la autenticidad de la evidencia electrónica debe ser contrastada mediante fuentes externas e independientes. A su vez, sugieren la realización de pruebas adicionales que trasciendan las verificaciones internas tradicionales. En el caso de Olympus, no se realizaron estas verificaciones externas, esta falta de controles permitió que el fraude se mantuviera encubierto durante más de una década (Fukukawa, Mock, & Srivastava, 2014).

El uso de vehículos financieros complejos y transacciones electrónicas en el fraude de Olympus destaca la importancia creciente de la evidencia electrónica en auditorías contemporáneas. La globalización y la digitalización de los mercados han hecho que esta evidencia sea una fuente clave de información en auditorías. Sin embargo, esto plantea nuevos desafíos para los auditores.

En el caso de Olympus, la falta de control sobre los sistemas electrónicos fue un factor decisivo. La dependencia excesiva en consultores externos permitió que las transacciones fraudulentas pasaran desapercibidas. Esto ocurrió durante varios años (Verschoor, 2012).

La ISA 500 establece que la fiabilidad de la evidencia electrónica depende de los controles internos. En Olympus, estos controles eran claramente deficientes. Esto facilitó la realización de transacciones fraudulentas, además, no se contaba con la documentación necesaria.

El comité especial indicó que "el método utilizado para ocultar las pérdidas fue táctico", no se conservaron documentos que demostraran la existencia de esas transacciones (Verschoor, 2012).



Este caso resalta la importancia de realizar una revisión más exhaustiva de los sistemas electrónicos, también destaca la importancia de analizar rigurosamente los controles internos; esto es aún más crucial en empresas globales con operaciones en diversas jurisdicciones.

De igual manera, tanto la SAS 142 como la AS 1105 destacan la relevancia de la evidencia electrónica, ambas normativas destacan que los auditores deben actuar con extrema cautela al evaluar la fiabilidad de la evidencia electrónica.

En el caso de Olympus, la dependencia en estructuras electrónicas complejas complicó la tarea de los auditores, además, la falta de transparencia en las transacciones digitales añadió más dificultades.

Este caso pone en evidencia los desafíos que enfrentan los auditores en un mundo cada vez más digitalizado la evidencia puede ser manipulada o alterada sin dejar rastros físicos visibles.

[Aplicación de normativas internacionales: ISA 500, SAS 142 y AS 1105](#)

El análisis del caso Olympus destaca la importancia de aplicar normativas rigurosas en casos de fraude. La ISA 500, la SAS 142 y la AS 1105 son fundamentales en la recolección de evidencia, exigen que los auditores obtengan evidencia suficiente y adecuada, además debe ser relevante y confiable.

La ISA 500 subraya la necesidad de recoger evidencia de diversas fuentes, esencial para asegurar su validez. Por otro lado, la SAS 142 y la AS 1105 ofrecen guías específicas para escenarios con un alto riesgo de fraude.

En el caso de Olympus, aplicar estas normativas de manera más estricta habría sido crucial, un enfoque más detallado en la evaluación del riesgo de fraude podría haber permitido una detección más oportuna.

Esto demuestra que los auditores deben mantener un escepticismo profesional elevado especialmente en entornos complejos y con alto riesgo de fraude.

[Lecciones del caso Olympus y su relevancia para la auditoría internacional](#)

El caso de Olympus subraya la necesidad urgente de fortalecer los estándares de auditoría, en particular, esto es crucial para la recolección y evaluación de la evidencia



electrónica. Las normas ISA 500, SAS 142 y AS 1105 proporcionan guías claras sobre cómo gestionar la evidencia en auditorías complejas. Sin embargo, lo ocurrido en Olympus demuestra que aplicar estos estándares en la práctica continúa siendo un reto significativo, la falta de uniformidad entre las normas internacionales y estadounidenses genera inconsistencias que dificultan la detección de fraudes en empresas multinacionales. En el caso de Olympus, la compañía se regía tanto por regulaciones japonesas como por expectativas internacionales, esto provocó vacíos en la supervisión y control.

Lo observado en Olympus refuerza las hipótesis de esta tesis sobre las dificultades que enfrentan los auditores al aplicar normativas distintas en un entorno globalizado, estas diferencias impactan en la calidad de la evidencia, especialmente en fraudes contables; además, el caso de Olympus subraya las graves consecuencias de una supervisión deficiente y el riesgo que implica una gobernanza corporativa concentrada en la figura del presidente. El control excesivo de los ejecutivos, junto con la apatía de los directores y la falta de diversidad en la Junta Directiva, permitió que el fraude se perpetuara durante años sin ser detectado. Esto resalta la necesidad de una estructura de gobernanza sólida y de auditores independientes que deben ser una línea de defensa crucial contra fraudes financieros.

En la auditoría de fraudes, la implementación de controles efectivos es fundamental, además, la independencia de los auditores, tanto internos como externos, es clave. Estos elementos requieren especial atención bajo las normativas internacionales de auditoría, como la ISA 500 y la AS 1105.¹¹

Cumplimiento de los objetivos para el caso de estudio

Suficiencia y adecuación

Este fraude contable, caracterizado por la ocultación de pérdidas mediante complejas transacciones ficticias, evidenció deficiencias en la aplicación de los estándares.

¹¹ El caso Olympus se puede ver de forma resumida en el Anexo IV: Caso Olympus – Mapa Mental.



Además, la evidencia electrónica y la tecnología jugaron un papel crucial. La manipulación de documentos y las operaciones financieras internacionales dificultaron la evaluación de la fiabilidad de la evidencia. Las normas como la ISA 500, que sugieren la evaluación de la integridad de la evidencia digital, enfrentan limitaciones si los auditores carecen de experiencia tecnológica.

Por otra parte, la relevancia de la evidencia también es cuestionable. La capacidad del auditor de evaluar su pertinencia y adaptarse a la complejidad tecnológica fue clave. Olympus empleó sistemas avanzados para modificar y ocultar información. Los auditores debían mantener un escepticismo profesional robusto y considerar la posible manipulación de la evidencia.

Esto revela una debilidad crítica: la confianza ciega en la documentación interna. La falta de verificación independiente permitió que el fraude pasara desapercibido. Las normas como la AS 1105 enfatizan la necesidad de corroboración externa, una práctica que los auditores podrían haber reforzado con consultas a expertos.

En suma, la evidencia de auditoría, para ser suficiente y adecuada, requiere más que recopilación. Exige un análisis crítico y multidimensional.

[Evaluación de la calidad de la evidencia](#)

La ISA 500 se centra en la suficiencia y adecuación de la evidencia. Este enfoque destaca la capacidad del auditor para determinar si la evidencia es de calidad suficiente. La relevancia de esto en Olympus es evidente. La complejidad de sus registros y el uso de esquemas para ocultar pérdidas exigían un análisis detallado. Así, se requería confirmar si la evidencia obtenida era realmente adecuada.

Por otro lado, la SAS 142 enfatiza los atributos de la evidencia, como la relevancia y la fiabilidad. Este énfasis podría haber sido determinante en la identificación de señales de alerta en los estados financieros de Olympus. La norma obliga a una revisión cuidadosa de la fiabilidad. En el contexto de Olympus, los informes internos y transacciones simuladas dificultaron la tarea de los auditores. Esta norma, por tanto, hubiera demandado una atención más minuciosa en esos aspectos.

La AS 1105 introduce un enfoque centrado en la calidad y cantidad de la evidencia. Resalta tanto la procedencia como los métodos de recolección. En el caso Olympus,



esto implicaría un análisis detallado del origen de los documentos y registros electrónicos presentados. Las transacciones estructuradas y los movimientos financieros opacos habrían requerido la aplicación estricta de la AS 1105. Esto habría ayudado a desenmascarar su falta de veracidad.

Las implicaciones sobre el caso Olympus reflejan cómo estas normativas influyen en la detección de irregularidades. La ISA 500, al enfatizar la suficiencia y adecuación, habría promovido un enfoque crítico. La SAS 142 subraya la revisión de la fiabilidad de la evidencia, un punto débil en las auditorías de Olympus. Finalmente, la AS 1105, al enfocarse en la calidad y la procedencia, requeriría una revisión exhaustiva de las fuentes.

Cada norma aborda la calidad de la evidencia desde ángulos distintos. Esta diversidad de enfoques podría haber influido en el desarrollo del caso. En última instancia, resaltan la importancia de una evaluación rigurosa.

Caso Peregrine

[El fraude financiero y su impacto en las organizaciones](#)

El fraude financiero ha sido un problema frecuente en muchas organizaciones, afecta especialmente a aquellas que manejan grandes volúmenes de fondos de terceros; estas prácticas fraudulentas no solo dañan a la empresa implicada, también tienen consecuencias para el sistema financiero en general.

Inversionistas y clientes son gravemente perjudicados, además, la confianza en los mercados se ve afectada, un ejemplo emblemático es la quiebra de Peregrine Financial Group (PFG). Un informe del síndico destacó que este fraude tuvo un doble impacto, por un lado, afectó a los clientes que confiaron sus recursos a la entidad; por otro, dejó al descubierto graves deficiencias en los controles internos de la empresa (United States Bankruptcy Court for the Northern District of Illinois, 2014).

El fraude en PFG evidencia cómo la manipulación constante de la información contable puede quedar oculta y esto puede suceder a lo largo de varios años, incluso, las irregularidades financieras pueden pasar inadvertidas bajo la supervisión de mecanismos regulatorios.



Este caso revela las vulnerabilidades en los sistemas de control interno, también muestra cómo las tácticas fraudulentas pueden escapar al escrutinio durante años.

El esquema de PFG subraya la facilidad con la que se pueden falsear documentos contables, esto permite desviar fondos sin detección inmediata y esto sucede incluso con la supervisión de los organismos reguladores.

Russell Wasendorf, Sr., fundador y CEO de PFG, fue quien perpetró este fraude, utilizó técnicas de falsificación de estados financieros y también manipuló cuentas bancarias para desviar fondos.

La malversación superó los 200 millones de dólares, pero sin embargo, su esquema no fue detectado hasta la introducción de un sistema de confirmaciones electrónicas, fue este sistema el que permitió evidenciar las irregularidades.

El informe detalla que "la manipulación de fondos por parte de Wasendorf se extendió por un período de años, durante el cual los controles financieros internos fueron insuficientes para detectar las irregularidades" (United States Bankruptcy Court for the Northern District of Illinois, 2014).

Wasendorf llevó a cabo sus manipulaciones durante más de dos décadas. Falsificó documentos financieros y manipuló cuentas bancarias, empleó herramientas digitales como Photoshop para crear documentos fraudulentos. Según Elder y sus colaboradores, "Wasendorf utilizó Photoshop, Excel, escáneres y varios tipos de impresoras para crear falsificaciones convincentes de prácticamente todos los documentos que provenían del banco" (Elder, Janvrin, & Caster, 2014).

[La importancia de la evidencia de auditoría en la prevención del fraude](#)

La evidencia de auditoría es clave para la detección y prevención del fraude financiero, las normativas internacionales, como la ISA 500, establecen estándares claros; en el contexto estadounidense, normas como la SAS 142 y la AS 1105 también son fundamentales, estas exigen que los auditores recopilen evidencia adecuada y suficiente, esto permite evaluar la fiabilidad de los estados financieros.

En el caso de PFG, se evidenció una falta de controles sobre la evidencia documental, además, las auditorías previas fueron deficientes, esto permitió que Wasendorf manipulara los balances contables durante años sin ser detectado.



En este contexto, la evidencia electrónica tiene una importancia central, la transición hacia confirmaciones electrónicas fue decisiva. En el caso de PFG, la National Futures Association (NFA) impulsó este cambio, esta implementación fue esencial para detectar el fraude. El informe indicó que "fue la implementación de las confirmaciones electrónicas lo que finalmente expuso la falsedad de los documentos enviados por Wasendorf" (United States Bankruptcy Court for the Northern District of Illinois, 2014). Este caso subraya la importancia de la tecnología en las auditorías, las herramientas tecnológicas pueden disminuir de manera considerable el riesgo de fraude.

Peterson explica que, durante años, Wasendorf logró manipular los balances financieros con falsificaciones complejas, utilizó software de edición digital como Photoshop y esto permitió que el fraude pasara desapercibido, sin embargo, la implementación de un sistema de confirmaciones electrónicas fue clave. La NFA introdujo este sistema, lo que permitió detectar discrepancias, se reveló, de este modo, la discrepancia entre los estados financieros reportados y los saldos reales en las cuentas bancarias.

Peterson (2014) señala que "la implementación de confirmaciones electrónicas fue el catalizador que finalmente desmanteló el fraude, exponiendo la falsificación de documentos bancarios" (Peterson, 2014). Elder añade que "el fraude finalmente fue descubierto cuando los reguladores implementaron un sistema de confirmación electrónica", este sistema eliminó la capacidad de Wasendorf de manipular manualmente los documentos (Elder, Janvrin, & Caster, 2014).

Este caso destaca la importancia de que las normas de auditoría consideren la evidencia electrónica, tanto US GAAP como NIIF deben asegurar la fiabilidad de la información financiera.

A pesar de que ambos marcos reconocen la importancia de la evidencia electrónica, la falta de uniformidad es un desafío; este problema se intensifica en auditorías internacionales, sobre todo ante fraudes complejos que involucran manipulación tecnológica.

Diferencias en la evidencia de auditoría entre US GAAP y NIIF

Las normativas US GAAP y NIIF ofrecen directrices sobre la evidencia de auditoría, sin embargo, tienen enfoques distintos respecto a la evidencia electrónica. En US GAAP, la



SAS 142 introduce criterios específicos para evaluar la calidad de la evidencia, la fiabilidad y suficiencia de la evidencia electrónica son aspectos clave; pero, la interpretación de estos principios puede variar según el auditor y las condiciones de la auditoría. En contraste, las NIIF y la ISA 500 también proporcionan pautas para la evidencia electrónica, sus principios son más generales, esta flexibilidad puede generar inconsistencias en auditorías realizadas en diferentes países.

Peterson (2014) indica que "la flexibilidad en la aplicación de los principios bajo NIIF permite que las empresas en distintas jurisdicciones adopten diferentes enfoques, esto afecta la recopilación y verificación de evidencia electrónica, como resultado, puede afectar la consistencia de las auditorías" (Peterson, 2014).

Elder y sus colegas coinciden en este punto, ellos afirman que "la falta de un enfoque coherente en la recopilación y verificación de evidencia electrónica entre US GAAP y NIIF puede llevar a disparidades significativas en la calidad de las auditorías" (Elder, Janvrin, & Caster, 2014).

La falta de uniformidad en los estándares globales crea un entorno complejo, los auditores se enfrentan a desafíos importantes, especialmente en auditorías internacionales. Este es uno de los factores que permitió la prolongación del fraude en PFG, la inconsistencia en la aplicación de los mecanismos de verificación hizo que el fraude pasara desapercibido por años.

La importancia de la confirmación electrónica

Una de las lecciones más evidentes del caso de PFG es la importancia de adoptar tecnologías avanzadas para verificar la evidencia de auditoría, durante años, Wasendorf logró falsificar manualmente los estados financieros sin ser detectado; no obstante, cuando la National Futures Association (NFA) introdujo confirmaciones electrónicas, el fraude fue descubierto casi de inmediato.

Elder y sus colegas señalan que "la adopción de confirmaciones electrónicas por parte de los reguladores fue lo que finalmente reveló la discrepancia entre los saldos bancarios reportados y los reales" (Elder, Janvrin, & Caster, 2014).



Este caso pone en evidencia que las herramientas tecnológicas, como la confirmación electrónica, son fundamentales en la auditoría moderna, permiten verificar rápidamente la autenticidad de la información, además, minimizan el riesgo de manipulación.

El control interno y el rol de los auditores

La solidez de una organización financiera se basa en la efectividad de sus controles internos, estos controles son cruciales. En el ámbito de las auditorías, su importancia es fundamental, garantizan la veracidad de los informes financieros y además, aseguran la correcta gestión de los fondos de los clientes.

En PFG, la falta de supervisión fue clave, se permitieron prácticas irregulares dentro de la organización, esto aumentó considerablemente la magnitud del fraude. El informe del síndico indica lo siguiente: "los controles internos de PFG no fueron adecuados para evitar la manipulación de fondos por parte de su fundador, lo que permitió que el fraude continuara sin interrupciones durante más de dos décadas" (United States Bankruptcy Court for the Northern District of Illinois, 2014).

La labor de los auditores externos es igualmente crucial, son fundamentales en la prevención de fraudes contables. Normativas internacionales, como la ISA 500, exigen mantener un escepticismo profesional, esto implica cuestionar la veracidad de la información proporcionada por la empresa auditada.

En el caso de PFG, los auditores no identificaron señales de alerta tempranas, esto podría haber revelado el fraude antes. Según Peterson (2014), "la falta de escepticismo profesional y la confianza excesiva en la documentación proporcionada por la empresa auditada fueron factores clave que permitieron que el fraude se prolongara" (Peterson, 2014).

La SAS 142 subraya este punto, destaca que la calidad y suficiencia de la evidencia de auditoría deben ser evaluadas rigurosamente, esto es especialmente importante si hay posibles señales de fraude. Sin embargo, en PFG, los auditores fallaron en detectar estas señales, este error resalta la necesidad de ir más allá de la simple revisión de documentos. Los auditores deben emplear herramientas, como la confirmación electrónica, para validar la exactitud de la información recibida.



La bancarrota de PFG y la gestión post-fraude

El caso de PFG ilustra la importancia de los procedimientos legales, también muestra el rol esencial del síndico en la gestión de un fraude financiero a gran escala. Tras la quiebra de la empresa en 2012, se designó un síndico, su tarea fue recuperar los activos, luego, debía distribuirlos entre los acreedores y los clientes afectados.

El informe menciona una de las primeras medidas: "cerrar todas las oficinas de PFG y reducir la nómina, al tiempo que se investigaba la ubicación de los fondos desviados" (United States Bankruptcy Court for the Northern District of Illinois, 2014).

La quiebra de PFG generó múltiples demandas contra terceros, estos beneficiarios habían recibido transferencias fraudulentas, además, hubo negociaciones para la recuperación de activos. El síndico logró acuerdos extrajudiciales significativos, por ejemplo, recuperó más de 2,8 millones de dólares de la exesposa de Wasendorf (United States Bankruptcy Court for the Northern District of Illinois, 2014).

Estas acciones fueron esenciales, ayudaron a mitigar las pérdidas de los acreedores y clientes afectados; sin embargo, las recuperaciones quedaron muy por debajo de la cantidad total malversada.

Profesionalismo y escepticismo en la auditoría

Un aspecto central en el caso de PFG fue la falta de escepticismo profesional por parte de los auditores, las normas de auditoría, como la SAS 142 y la ISA 500, subrayan su importancia y los auditores deben cuestionar la información proporcionada por la empresa auditada y esto debe hacerse a lo largo de todo el proceso de auditoría.

En PFG, los auditores no investigaron adecuadamente las inconsistencias, estas señales podrían haber detectado el fraude antes.

Elder y sus colegas afirman: "la falta de escepticismo profesional y la confianza excesiva en la documentación presentada fueron factores clave que permitieron que el fraude de PFG se prolongara durante tanto tiempo" (Elder, Janvrin, & Caster, 2014).

Este error destaca la necesidad de mayor rigor en los auditores, la evaluación de la evidencia de auditoría debe ser más detallada, crucial cuando hay riesgo de fraude.



Las normas de auditoría necesitan ser más estrictas, es esencial utilizar tecnologías avanzadas para verificar la evidencia. Así se reduce el riesgo de manipulación, además, se aumenta la confianza en los resultados de las auditorías.

Evidencia electrónica y auditoría en el entorno financiero global

En el entorno financiero global actual, la evidencia electrónica es esencial, juega un papel clave en la detección y prevención de fraudes. Los auditores enfrentan desafíos cada vez mayores, deben verificar activos y también, comprobar la autenticidad de documentos electrónicos.

El caso de PFG lo demostró claramente, las confirmaciones electrónicas lograron desenmascarar el fraude; este había evadido los controles tradicionales durante años. Este caso destaca una necesidad clara, las normativas de auditoría deben adaptarse a los avances tecnológicos, además, es crucial ajustarse a las nuevas formas de malversación y estas formas suelen utilizar herramientas digitales.

El uso de tecnologías avanzadas aporta múltiples beneficios, mejora la precisión en las auditorías; también agiliza el proceso; además, disminuye la posibilidad de fraudes similares.

Normativas como la ISA 500 reconocen la importancia de la evidencia electrónica, sin embargo, es necesario que las firmas de auditoría adopten plenamente estas tecnologías, solo así se evitarán futuros casos similares al de PFG.

Impacto de la falta de homogenización en la práctica de auditoría internacional

La falta de homogenización en los requerimientos de evidencia electrónica entre US GAAP y NIIF genera importantes desafíos, esto impacta directamente en la práctica de auditoría internacional.

En el caso de PFG, la ausencia de estándares uniformes permitió que el fraude permaneciera oculto durante años. Las diferencias entre US GAAP y NIIF son evidentes en la verificación de la evidencia electrónica, esto destaca una necesidad crítica, las auditorías en diferentes jurisdicciones deben ser más coherentes, además, necesitan un enfoque estandarizado.



Peterson (2014) señala que "la falta de un enfoque unificado en la verificación de la evidencia electrónica en auditorías internacionales puede generar inconsistencias que afectan la calidad de las auditorías. Como consecuencia, se dificulta la detección de fraudes contables complejos" (Peterson, 2014).

En el contexto globalizado actual, las empresas operan en múltiples jurisdicciones, es esencial que los marcos normativos internacionales se alineen mejor. La convergencia en los enfoques sobre la evidencia electrónica es crucial, especialmente ante casos de fraude.¹²

Cumplimiento de los objetivos para el caso de estudio

Suficiencia y adecuación

En el análisis del caso Peregrine, evaluar los principios fundamentales de las normas de auditoría vinculadas a la suficiencia y adecuación de la evidencia resultó crucial.

Esto permite entender los retos y fallos que llevaron al colapso de la empresa. La suficiencia de la evidencia implica que la cantidad debe ser la adecuada para sustentar las conclusiones. En el caso de Peregrine, la deficiencia en la cantidad y calidad de la evidencia fue evidente.

Este fallo expuso una carencia crítica en la aplicación rigurosa de las normas de auditoría. Además, la adecuación de la evidencia se centra en la calidad y relevancia de la misma. Esta debe ser capaz de respaldar de manera efectiva los hallazgos de la auditoría.

Las normas, como ISA 500, SAS 142 y AS 1105, detallan aspectos esenciales. Los criterios que establecen buscan guiar al auditor en la evaluación de la validez de la información que sustenta los estados financieros.

El caso Peregrine muestra cómo la aplicación deficiente de los principios de los estándares permitió la omisión de aspectos clave. La auditoría tradicional, sin un análisis exhaustivo de evidencias electrónicas contemporáneas, facilitó que el fraude no se detectara. Este punto ilustra un problema profundo.

¹² El caso Peregrine se puede ver de forma resumida en el Anexo V: Caso Peregrine – Mapa Mental.



La falta de adaptación de algunos auditores al entorno de evidencias digitales emergentes es alarmante. Por otro lado, las normas subrayan la relevancia del escepticismo profesional. Este es un componente esencial para evaluar la suficiencia y adecuación de la evidencia.

En Peregrine, al carecer de escepticismo, se aceptaron evidencias que no eran completas o simplemente eran falsas. El caso, por tanto, subraya la necesidad urgente de un enfoque más riguroso. También resalta la importancia de la formación continua de los auditores.

La evolución tecnológica impone desafíos complejos. La adaptación de las prácticas de auditoría a la evidencia electrónica moderna es ineludible. De lo contrario, la integridad de los procesos financieros queda en riesgo.

Evaluación de la calidad de la evidencia

Al desplegar una comparación de cada norma, se notarán diferencias importantes que impactan directamente sobre la auditoría.

Primero, la ISA 500 impone un enfoque que varía en cuanto a la interpretación de la "calidad" de la evidencia, dependiendo del juicio profesional del auditor. Esto se traduce en una flexibilidad que, aunque útil, puede presentar riesgos de inconsistencias cuando se enfrenta un fraude estructurado como el de Peregrine.

Por otro lado, la SAS 142 complementa estas pautas centrándose en los atributos de la evidencia en términos de relevancia y fiabilidad, pero introduce un matiz más estructurado sobre la documentación de la procedencia y contexto de la evidencia. Este énfasis puede fortalecer la trazabilidad y credibilidad del proceso de auditoría. Así, mientras ISA 500 permite cierta variabilidad en la evaluación, SAS 142 refuerza la documentación meticulosa como un pilar de la calidad.

En contraste, la AS 1105, norma aplicada en el entorno estadounidense (PCAOB), subraya la importancia de la suficiencia y competencia de la evidencia auditada con un marco más rígido, apuntando a la reducción de incertidumbres y margen de error. Para un caso como Peregrine, donde la manipulación de la evidencia jugó un papel central, el enfoque más riguroso de AS 1105 podría ayudar a identificar discrepancias a través de controles más estrictos y procedimientos estandarizados.



En resumen, ISA 500 otorga flexibilidad y confía en la competencia profesional, SAS 142 introduce robustez documental, y AS 1105 prioriza una evaluación cuantitativa y cualitativa que busca minimizar riesgos. Esto implica que la elección y aplicación de estas normas pueden influir en la profundidad de la detección de irregularidades, siendo AS 1105 potencialmente más efectiva para identificar el fraude de Peregrine debido a su enfoque exhaustivo.

Caso Theranos

El inicio de Theranos: la promesa de una tecnología revolucionaria

El caso de Theranos, uno de los startups más notables de Silicon Valley, resalta por cómo los fraudes contables y la manipulación de evidencias fueron claves en su desplome.

Elizabeth Holmes fundó Theranos en 2003, la empresa prometía una revolución en el sector salud, su visión giraba en torno a una tecnología que, supuestamente, realizaba pruebas diagnósticas complejas con apenas unas gotas de sangre. Holmes afirmaba que su sistema permitía ejecutar más de doscientas pruebas con esa mínima muestra, de ser cierto, esto habría transformado el acceso a la salud a nivel mundial (Bundy & Ndu, 2023).

La propuesta era seductora, prometía pruebas más veloces, menos invasivas y a un costo mucho menor que los métodos convencionales e inmediatamente, Theranos captó la atención de inversores y del ámbito médico.

Holmes, tras abandonar Stanford, se dedicó por completo a su idea, pronto se rodeó de figuras relevantes de la industria tecnológica y médica, esto incrementó la credibilidad de la compañía. En su apogeo, Theranos alcanzó una valoración de 9 mil millones de dólares y ya se consideraba uno de los startups más prometedores en Silicon Valley (Carreyrou, 2018).

Sin embargo, todo se vino abajo, empleados como Erika Cheung y Tyler Shultz empezaron a denunciar prácticas fraudulentas dentro de la empresa (Rogal, 2021). Estas denuncias revelaban la manipulación sistemática de resultados de pruebas, los informes



que se presentaban a los inversores estaban falsificados, además, la tecnología no funcionaba como se decía.

El engaño no solo se dirigía a inversores y reguladores, también afectaba a los propios empleados, se les obligaba a firmar acuerdos de confidencialidad estrictos, además, trabajaban bajo un ambiente de presión y represión (Rogal, 2021).

Cuando las denuncias finalmente llegaron a las agencias reguladoras y a la prensa, la caída fue inevitable, la SEC y otros organismos llevaron a cabo investigaciones exhaustivas. Descubrieron que la tecnología nunca había sido viable y también encontraron que la información financiera había sido manipulada para atraer enormes inversiones (Rogal, 2021).

Detrás de la imagen de innovación y éxito, Theranos ocultaba un secreto oscuro, su tecnología no funcionaba. Aunque se promocionaba como capaz de realizar más de 200 pruebas diagnósticas, los resultados no eran precisos, eran inexactos, inconsistentes y en muchos casos, manipulados para parecer exactos. Holmes y su equipo ocultaron estos fallos, ni empleados ni inversores conocían la verdad, se instauró una cultura de secretismo debido a que la manipulación de la información era constante.

Los resultados de pruebas médicas eran manipulados, los fallos tecnológicos, ocultados. Esto revela las debilidades en la auditoría de evidencia electrónica es un tema central en esta investigación (Rogal, 2021). Desde el inicio, el dispositivo Edison no funcionaba, prometía realizar pruebas, pero estaba lejos de ser efectivo.

La máquina tenía problemas mecánicos, fallaba en la precisión, los inversores no sabían tampoco las autoridades reguladoras conocían la verdad ni los pacientes. “El Edison no solo no podía regular la temperatura ni transferir fluidos correctamente, sino que también los resultados eran falseados por la dilución excesiva de las muestras” (Bundy & Ndu, 2023).

La falta de transparencia en Theranos fue evidente, los controles adecuados brillaban por su ausencia lo que creó un ambiente perfecto para la manipulación y el fraude. Theranos implementó una estrategia de ocultamiento, manipulaba información financiera y operativa, inversores y pacientes fueron engañados. Esto expuso graves fallas en los controles de auditoría, también mostró la fragilidad en la interpretación de la evidencia en situaciones de fraude (Rogal, 2021).



Liderazgo ético y cultura corporativa

El liderazgo corporativo es esencial para promover prácticas éticas dentro de una organización, en Theranos, Elizabeth Holmes y Ramesh "Sunny" Balwani dirigieron la empresa con una falta notable de transparencia. El ambiente laboral era de intimidación, los empleados que dudaban de la tecnología eran presionados lo que derivó en una cultura de secretismo.

Las voces internas fueron silenciadas, esto permitió la expansión del fraude, según (Cambaza, 2024), “Theranos fue caracterizado por una cultura de secretismo y miedo que silenciaba a los empleados y perpetuaba prácticas poco éticas dentro de la empresa”.

Uno de los elementos centrales del fraude en Theranos fue la falta de controles internos sólidos, el entorno de secretismo impidió detectar errores e inconsistencias en las pruebas sanguíneas que no se descubrieron hasta mucho tiempo después, para entonces, la empresa ya había recaudado miles de millones en capital. Esto destaca la importancia de una supervisión adecuada.

Las normativas de auditoría actuales, como SAS 142 y AS 1105, insisten en la confiabilidad de la información financiera, como se menciona en Integrity Line, “Theranos fue capaz de engañar a tanta gente porque la información crítica nunca fue compartida, y los controles internos eran insuficientes para detectar las fallas” (Integrity Line, 2023), también subraya la relevancia de una cultura empresarial que facilite las denuncias internas, esto debe hacerse de manera segura y efectiva.

Las normativas de auditoría, como ISA 500, reconocen la importancia de obtener evidencia suficiente y adecuada, es fundamental para emitir una opinión sobre los estados financieros. En Theranos, la ausencia de denuncias internas permitió que el fraude continuara, según Integrity Line, “una cultura de denuncia efectiva puede haber evitado el colapso de Theranos y haber protegido a sus inversores y clientes” (Integrity Line, 2023).

La auditoría depende de la honestidad y la transparencia de la administración y sin un liderazgo ético, los datos críticos pueden manipularse. Esto recalca la necesidad de que los auditores mantengan independencia y el escepticismo profesional es clave para evaluar la evidencia que las empresas proporcionan.



La evidencia exógena y su relevancia en la auditoría

Las normas SAS 142, ISA 500 y AS 1105 destacan la importancia de la evidencia en la evaluación de estados financieros. Es fundamental que la información provenga de fuentes confiables y relevantes. Tradicionalmente, los auditores han puesto su atención en la evidencia interna generada por las empresas, pero ahora, la disponibilidad de datos externos ha crecido. Según Cheong et al. (2022), “los auditores tienen acceso a nuevas fuentes de información crítica. Estas incluyen redes sociales, búsquedas en línea y datos de transacciones” (Cheong, Duan, Huang, Vasarhelyi, & Zhang, 2022).

En Theranos, la información interna no era fiable y esto fue clave, ni los auditores ni los reguladores detectaron el fraude a tiempo. "La evidencia obtenida de una fuente externa es más confiable que la obtenida únicamente de fuentes internas" (Cheong, Duan, Huang, Vasarhelyi, & Zhang, 2022), esto indica la necesidad de buscar evidencia externa.

En el caso de Theranos, los exámenes externos y análisis de plataformas como Glassdoor y Yelp fueron esenciales, proporcionaron datos sobre el mal ambiente laboral como también dieron pistas sobre la falta de transparencia (Cheong et al., 2022). Las reseñas en Glassdoor eran claras, apuntaban a una alta rotación de personal y a prácticas inseguras en los laboratorios, estas señales debieron haber alertado a los auditores.

También, las revisiones en Yelp fueron fundamentales porque proporcionaron testimonios clave a periodistas e investigadores, ayudaron a destapar el fraude.

Theranos mostró el daño que provoca la desconfianza en la evidencia y en los controles, los efectos no solo se limitan a los inversores, también afectan a la sociedad en general.

La credibilidad en la tecnología y en la innovación biomédica se vio seriamente afectada, este impacto es similar al de los fraudes contables.

Cuando se pierde la confianza en la auditoría financiera, las consecuencias pueden ser devastadoras para la economía, Das y Drolet (2022) afirman que "es necesario alinear los incentivos entre la industria y la innovación académica para restaurar la confianza del público" (Das & Drolet, 2022). Este principio aplica también a la auditoría, la transparencia y la rigurosidad en la recolección de evidencia son esenciales para mantener la confianza en los mercados financieros.



La manipulación de la evidencia y el papel de la auditoría

A medida que Theranos crecía, las auditorías se volvieron un desafío importante, no solo por el tamaño creciente de la empresa, sino también por la evidencia electrónica que utilizaba para respaldar su tecnología.

Las normas de auditoría son fundamentales en estos contextos, especialmente en casos de fraude, como ocurrió con Theranos. La ISA 500, por ejemplo, exige que los auditores recopilen evidencia suficiente y apropiada para emitir conclusiones válidas; sin embargo, en Theranos, los resultados de las pruebas eran manipulados.

Los auditores no tenían acceso a información completa ni fiable para realizar una evaluación adecuada, Holmes ejercía un control estricto sobre los datos compartidos lo que impidió detectar a tiempo las inconsistencias en los dispositivos (Carreyrou, 2018). La manipulación deliberada de resultados médicos electrónicos podría haberse identificado con controles más rigurosos, la normativa insiste en el uso de tecnologías adecuadas y la validación de sistemas informáticos al generar evidencia (Rogal, 2021). Holmes y su equipo no solo ocultaron problemas técnicos, sino que también tergiversaron informes financieros. Según Bundy y Ndu, "Theranos recaudó más de 700 millones de dólares de inversores de renombre sin proporcionar estados financieros auditados que pudieran reflejar la verdadera situación de su tecnología" (Bundy & Ndu, 2023).

El engaño sistemático que llevó a esta situación se vio facilitado por la ausencia de normativas estrictas para las empresas privadas en Estados Unidos que, a diferencia de las empresas públicas, no se les exige presentar ciertos tipos de evidencia financiera. Las entidades reguladoras, como la FDA o Administración de Alimentos y Medicamentos de Estados Unidos y la CMS o Centro de Servicios de Medicare y Medicaid, no actuaron con la proactividad necesaria, esto permitió que Theranos operara con tecnología deficiente durante años. "Las respuestas regulatorias fueron tardías y fragmentadas, lo que permitió que la tecnología defectuosa de Theranos perjudicara a muchos pacientes antes de que se tomaran medidas significativas" (Cambaza, 2024).

La importancia de evaluar la calidad de la evidencia, especialmente la generada de forma electrónica, es resaltada en la SAS 142. En Theranos, los dispositivos de pruebas



sanguíneas fallaban constantemente y los resultados, además, no siempre se generaban en tiempo real; esta situación forzaba al equipo de Theranos a reutilizar grabaciones de pruebas exitosas anteriores para engañar a los inversores (Carreyrou, 2018). La ausencia de una auditoría efectiva sobre la calidad de estos dispositivos permitió la presentación de información falsificada como evidencia confiable (Rogal, 2021).

Este tipo de manipulación se presentaba como evidencia válida, pero violaba los principios de auditoría sobre la fiabilidad de la evidencia electrónica; además, Das y Drolet (2022) señalan que "Theranos explotó lagunas en las políticas regulatorias, llevando sus pruebas al mercado sin revisión previa ni validación científica". Esto enfatiza la necesidad de auditorías rigurosas que impidan a las empresas presentar información manipulada o incompleta (Das & Drolet, 2022).

Por su parte, la AS 1105 exige que los auditores recopilen evidencia confiable y suficiente para respaldar su opinión en los estados financieros. En el caso de Theranos, la falta de controles internos y la manipulación de datos se combinaron con una ausencia de transparencia lo que generó un entorno en el que la evidencia electrónica, esencial para la empresa, no se auditó de manera adecuada. "Holmes controlaba todo, desde los informes hasta las pruebas", lo cual dificultaba el acceso de los auditores a la verdad sobre la situación real de los dispositivos (Carreyrou, 2018).

La dependencia de Theranos en dispositivos defectuosos para obtener resultados clínicos subraya la importancia de la norma que exige la validación de sistemas electrónicos. Solo así se pueden aceptar sus resultados como evidencia válida en una auditoría (Rogal, 2021). Theranos operó sin supervisión adecuada, esto dejó en evidencia las fallas en los controles internos.

Las normativas de auditoría, como AS 1105, resaltan la necesidad de información clara y verificable por parte de la gerencia. Los auditores deben evaluar la situación financiera con precisión.

En Theranos, "la falta de controles internos permitió que la empresa manipulara la información sin ser detectada por los inversores ni los reguladores" (Das & Drolet, 2022). La falta de controles adecuados resalta la importancia de que los auditores sean escépticos al revisar la evidencia proporcionada.



La ética es fundamental en la auditoría, los auditores deben verificar que la información financiera refleje la realidad económica de la empresa. En Theranos, se manipulaban los datos y se distorsionaban las capacidades tecnológicas y esto tuvo consecuencias graves. Según Cambaza (2024), “el escándalo de Theranos gira en torno a la falsificación deliberada de los resultados tecnológicos, lo que resultó en daños para los pacientes y pérdidas significativas para los inversores”, la falta de una recolección adecuada de evidencia puede tener efectos negativos importantes.

En la auditoría financiera, la evidencia debe ser suficiente y adecuada, los auditores tienen una obligación ética de mantener estos estándares. El caso Theranos muestra que manipular información técnica equivale a falsificar datos financieros lo que subraya la necesidad de una recolección rigurosa de la evidencia para evitar fraudes.

El escándalo de Theranos también expone la falta de escepticismo profesional ya que confiar ciegamente en la reputación de la gerencia puede llevar a errores serios.

SAS 142 y AS 1105 insisten en la necesidad de una recolección meticulosa de evidencia ya que es crucial cuando hay señales de riesgo, como la falta de transparencia o el secretismo en la empresa.

En Theranos, los auditores no detectaron las irregularidades a tiempo, esto ocurrió porque no hubo una evaluación exhaustiva de la información disponible. “La evaluación de la evidencia debe ser exhaustiva y escéptica, especialmente cuando hay indicios de manipulación o falta de transparencia por parte de la gerencia” (Integrity Line, 2023).

[El uso fraudulento de la evidencia electrónica](#)

El caso de Theranos destaca la relevancia de la evidencia electrónica en las auditorías actuales, la manipulación no solo abarcaba resultados de pruebas médicas como así también se falsificaban contratos con grandes farmacéuticas. Elizabeth Holmes aseguraba a los inversores que compañías como Pfizer y Novartis utilizaban la tecnología de Theranos en ensayos clínicos y esto era completamente falso (Carreyrou, 2018).

Las afirmaciones fraudulentas se apoyaban en documentación electrónica alterada, lo que generaba serios problemas de fiabilidad para los auditores debido a que disponían de los medios necesarios para verificar la autenticidad de esos datos. Bajo el liderazgo



de Holmes y Sunny Balwani, la empresa manipuló resultados clínicos, pero también presentó informes electrónicos falsos.

Estos informes pretendían demostrar que los dispositivos funcionaban correctamente, sin embargo, empleados reportaron la eliminación de resultados negativos en las pruebas de control de calidad. "Los resultados negativos de las pruebas de control de calidad eran eliminados como anómalos" (Rogal, 2021) y esto comprometió la veracidad de la información presentada a reguladores e inversores.

Al eliminar datos no conformes, Theranos ocultaba los fallos tecnológicos del dispositivo Edison y así, mantenían una imagen de éxito frente a inversores y autoridades (Jeske, 2020).

El dispositivo Edison no podía realizar pruebas diagnósticas precisas, era un claro ejemplo de cómo la tecnología mal gestionada genera evidencia engañosa. Según Cambaza (2024), "la promesa de Theranos de transformar el diagnóstico médico fue socavada por la falta de capacidad técnica de su dispositivo Edison, que produjo resultados erróneos y poco confiables" (Cambaza, 2024).

Theranos también realizó pruebas en pacientes sin que los dispositivos estuvieran listos para su uso clínico, "los resultados eran inconsistentes y poco confiables", poniendo en riesgo la salud de los pacientes, mientras la empresa seguía ocultando estas fallas bajo una atmósfera de secretismo (Carreyrou, 2018). La SAS 142, que enfatiza la evaluación del riesgo en evidencia electrónica, fue ignorada en este caso, ya que la manipulación digital era crucial en el fraude.

El caso de Theranos revela fallos en la regulación contable respecto a los activos intangibles generados internamente, especialmente en relación con la investigación y desarrollo de tecnologías no verificadas. Según el estudio, "la falta de una norma contable adecuada en EE. UU. para los activos intangibles generados internamente permitió a empresas como Theranos inflar sus estados financieros sin representar realmente su capacidad tecnológica" (Bundy & Ndu, 2023). Este vacío regulatorio dejó a Theranos capitalizar costos de desarrollo que, en verdad, no debían registrarse como activos, ya que la tecnología no estaba comprobada.

La manipulación de la evidencia electrónica también se extendió a la comunicación interna de la empresa, donde los empleados fueron segregados física e intelectualmente



para impedir que entendieran el panorama total de las operaciones y esto permitió que se ocultaran los fallos tecnológicos durante mucho tiempo. Theranos instauró un ambiente de represión y vigilancia para evitar denuncias internas ya que los denunciadores, como Erika Cheung y Tyler Shultz, fueron amenazados y sufrieron represalias de la alta dirección cuando intentaron exponer las irregularidades (Rogal, 2021). La manipulación de pruebas y la represión de voces disidentes fueron clave en la estrategia de ocultamiento.

En auditoría, la evaluación de la calidad de la evidencia electrónica es cada vez más crucial, los auditores necesitan contar con herramientas adecuadas; también requieren habilidades específicas para validar la evidencia digital. Es esencial asegurar que la evidencia no esté manipulada ni tenga defectos lo que se vuelve especialmente relevante en casos de fraude contable.

En el contexto globalizado actual, esta tarea es vital, las transacciones electrónicas son comunes y exigen una vigilancia constante para garantizar su integridad. El juicio de Elizabeth Holmes y Ramesh Balwani es un ejemplo claro, las consecuencias legales de un fraude contable no solo afectan a la empresa y también recaen sobre las personas responsables. Holmes y Balwani fueron acusados de engañar a los inversores, presentaron datos falsos sobre la tecnología de Theranos, esto tuvo un gran impacto. La responsabilidad legal resalta la importancia del escepticismo profesional en los auditores debido a que deben cumplir con las normativas que exigen verificaciones exhaustivas de la información de la gerencia.

Según el Departamento de Justicia de EE. UU., "Holmes y Balwani promovieron información falsa, lo que llevó a grandes pérdidas para los inversores" (United States Attorney's Office, 2022) y, aunque los datos exógenos presentan una gran oportunidad para mejorar la detección de fraudes, su implementación enfrenta varios desafíos. Cheong et al. (2022) señalan que analizar y procesar grandes volúmenes de datos externos puede ser costoso y requiere habilidades técnicas avanzadas.

Las normativas actuales reconocen la importancia de la evidencia externa, pero no siempre ofrecen directrices claras para integrarla de manera eficaz en la auditoría de fraudes, este es un campo que necesita más investigación y desarrollo.



El declive y desenlace de Theranos

A pesar de sus prácticas fraudulentas, Theranos siguió operando durante años y ni las autoridades ni los inversores se percataron de la magnitud del engaño solo hasta que en 2015, una investigación del Wall Street Journal, liderada por John Carreyrou, reveló las irregularidades. El artículo expuso que Theranos manipulaba resultados y falsificaba pruebas, la compañía había engañado tanto a pacientes como a inversores. Esto desató una serie de investigaciones federales, que llevaron finalmente al colapso de la empresa (Carreyrou, 2018).

Entre los inversores afectados estaban figuras importantes, Rupert Murdoch y la familia Walton, quienes habían inyectado grandes sumas de capital, sufrieron pérdidas significativas y, para cuando se descubrió que la base tecnológica de Theranos era un fraude, las consecuencias fueron enormes (Bundy & Ndu, 2023).

Theranos enfrentó una avalancha de demandas y una investigación exhaustiva. La SEC y los Centros de Servicios de Medicare y Medicaid (CMS) lideraron estas pesquisas, las investigaciones revelaron que Theranos utilizaba dispositivos que no cumplían con los estándares médicos, además, la evidencia que presentaban para validar resultados estaba manipulada.

Se estima que cerca de un millón de pruebas médicas realizadas por la empresa fueron anuladas o corregidas, los errores graves en las pruebas causaron un daño incalculable a los pacientes (Rogal, 2021).

En 2018, Theranos fue disuelta. Elizabeth Holmes y Sunny Balwani, el director de operaciones, fueron acusados de fraude. En 2022, Holmes fue declarada culpable de varios cargos, la sentencia fue significativa: 11 años de prisión. El escándalo marcó el final de uno de los startups más prometedores de Silicon Valley y también resaltó la importancia de auditar adecuadamente la evidencia electrónica en un entorno financiero digital.

La falta de transparencia financiera fue evidente, la manipulación de la evidencia electrónica contribuyó al fraude masivo. Además, la ausencia de normativas claras para evaluar activos intangibles en empresas privadas facilitó este engaño (Bundy & Ndu, 2023).



Walgreens fue uno de los socios comerciales más importantes de Theranos que terminó su relación con la empresa, además, presentó una demanda por incumplimiento de contrato y daños a su reputación (Rogal, 2021).

El caso Theranos no solo significó el fin de un startup que prometía cambiar la salud sino que también dejó lecciones cruciales para la auditoría y la regulación tecnológica. Jeske (2020) sostiene que la narrativa de Theranos ha sido tratada como un "caso excepcional", esto ha permitido centrar la atención en los errores individuales de Holmes. Mientras tanto, se han evitado debates más profundos sobre los fallos sistémicos que permitieron el fraude (Jeske, 2020).

Este enfoque desvía la atención de las estructuras organizativas que facilitan estos comportamientos y también oculta los incentivos que permiten la manipulación de evidencia electrónica. Es crucial fortalecer la regulación contable ya que las empresas tecnológicas deben presentar evidencia verificable antes de capitalizar costos de desarrollo y atraer inversores. El colapso de Theranos dejó una advertencia sobre los peligros de manipular la evidencia electrónica en un entorno digital (Rogal, 2021).¹³

Cumplimiento de los objetivos para el caso de estudio

Suficiencia y adecuación

Analizar los principios esenciales de las normas sobre suficiencia y adecuación de la evidencia de auditoría es fundamental al examinar el caso Theranos. La complejidad de este fraude y la manipulación sistemática de la evidencia resaltan la importancia de estos principios para detectar y contrarrestar fraudes complejos.

La evidencia de auditoría, primero, debe ser suficiente. Esto se refiere a la cantidad de pruebas necesarias que los auditores deben reunir. En Theranos, la insuficiencia de pruebas externas permitió a la empresa mantener una imagen falsa de legitimidad. Esta falta expuso fallos en la aplicación de los principios de suficiencia. Por tanto, no se alcanzó la cantidad requerida para sustentar conclusiones confiables sobre la viabilidad de las operaciones.

¹³ El caso Theranos se puede ver de forma resumida en el Anexo VI: Caso Theranos – Mapa Mental.



En segundo lugar, la adecuación apunta a la calidad de la evidencia. Theranos manipuló datos, presentando información que aparentaba ser confiable, pero carecía de una base sólida. La revisión crítica de la adecuación de la evidencia —que incluye relevancia y fiabilidad— no fue aplicada con el rigor necesario. Este enfoque inadecuado permitió la aceptación de evidencias defectuosas sin el análisis profundo de fuentes externas. Cada normativa aborda estos principios desde perspectivas diferentes. La ISA 500 exige evidencia suficiente y adecuada para justificar conclusiones razonables. En Theranos, la falta de verificación exhaustiva de la evidencia tecnológica y médica mostró un uso deficiente de estos principios. La SAS 142 pone el foco en la relevancia y fiabilidad de la evidencia utilizada. Esta evaluación es esencial cuando, como en este caso, las operaciones dependen de resultados internos poco claros. Por su parte, la AS 1105 del PCAOB establece lineamientos para evaluar la cantidad y calidad de la evidencia, siendo fundamental en entornos donde la tecnología y la subjetividad dificultan la identificación de irregularidades.

La deficiente aplicación de los principios de suficiencia y adecuación permitió que el fraude en Theranos se desarrollara sin oposición. La innovación tecnológica y una estrategia de marketing bien construida ocultaron la realidad durante años. Esto evidencia la necesidad de un enfoque crítico en la auditoría. Un enfoque que contemple tanto los procedimientos clásicos como los nuevos retos tecnológicos. La constante revisión y adaptación de los marcos regulatorios es esencial. Igualmente, las prácticas de auditoría deben ajustarse de manera continua. Solo así se responde a un entorno dinámico y cambiante.

[Evaluación de la calidad de la evidencia](#)

En el caso Theranos, las normas ISA 500, SAS 142 y AS 1105 presentan enfoques distintos sobre la calidad de la evidencia. Estas diferencias influyen directamente en la práctica y resultados de auditoría.

ISA 500 enfatiza la suficiencia y adecuación. Es decir, exige que el auditor obtenga evidencia que respalde su opinión. Frente a Theranos, un caso caracterizado por datos manipulados y tecnología inexistente, la aplicación de ISA 500 habría significado un



escrutinio profundo. Analizar la fuente y verificar la fiabilidad de las pruebas, tanto internas como externas, se habría vuelto crucial.

Por otro lado, SAS 142 aborda la relevancia y fiabilidad de la evidencia, más allá de su cantidad. Theranos empleó informes y presentaciones aparentemente creíbles para ocultar fallos. Así, aplicar SAS 142 hubiera implicado una inspección minuciosa.

Evaluar la autenticidad y congruencia de las pruebas electrónicas presentadas se habría convertido en un requisito. Las evidencias que parecían sólidas, pero eran fraudulentas, habrían puesto a prueba la habilidad del auditor para discernir su validez.

AS 1105, normativa del PCAOB, refuerza la necesidad de que la evidencia sea suficiente y adecuada, con un enfoque en la objetividad. En Theranos, la dependencia de fuentes imparciales y la revisión de controles internos habrían sido esenciales bajo AS 1105. Este estándar exige una evaluación independiente. La evidencia difícilmente verificable debía alertar a los auditores sobre posibles irregularidades.

Estos enfoques diversos muestran efectos específicos. ISA 500 podría haber llevado a un examen más detallado de los sistemas de recopilación de datos. SAS 142 habría subrayado la importancia de la fiabilidad frente a la narrativa persuasiva de los ejecutivos. AS 1105, a su vez, habría insistido en evidencias externas confiables y escepticismo.

La combinación de estos métodos es reveladora. Resalta la necesidad de integrar enfoques que consideren tanto cantidad como calidad. Además, pone de manifiesto que el escepticismo profesional es clave. Especialmente, en auditorías de alta complejidad.

Theranos es un ejemplo de cómo la sofisticación puede enmascarar la realidad.

Un enfoque más integrado habría sido crucial. Las normas, aplicadas en conjunto, podrían haber mejorado la detección de irregularidades.

Caso Exchange FTX

[Introducción a los fraudes contables en contexto criptográficos](#)

En un entorno donde la digitalización avanza rápidamente, los fraudes contables se han transformado. Ahora, se valen de tecnologías emergentes: criptomonedas, activos digitales y la tecnología blockchain. Un ejemplo reciente y destacado de esto es el caso



de FTX, una plataforma de intercambio de criptomonedas que se desplomó y este evento tuvo un impacto considerable en el mercado global de criptoactivos.

Además, expuso importantes debilidades en los sistemas de control interno y regulación, en palabras de Conlon, el colapso de FTX desnudó “fallos fundamentales en la gestión de riesgos y la gobernanza corporativa” (Conlon, Corbet, & Hu, 2023). No solo generó efectos devastadores para los inversores en criptomonedas sino que también evidenció la necesidad de que los auditores adapten sus enfoques, esto afecta tanto la recopilación como la evaluación de evidencia en un entorno financiero digital.

La caída de FTX fue significativa, ¿cómo una empresa valorada en más de 32 mil millones de dólares antes de noviembre de 2022 pudo desmoronarse tan rápidamente? Su desplome reveló la falta de controles internos y también puso de manifiesto el uso indebido de los activos de los clientes. La ausencia de prácticas de auditoría adecuadas quedó al descubierto, la fiabilidad de las transacciones con criptomonedas estaba en entredicho.

El impacto del colapso no se limitó a grandes corporaciones e inversores institucionales, afectó también a millones de usuarios individuales, muchos vieron desaparecer sus ahorros en solo unos días. En total, cerca de 1.2 millones de personas en Estados Unidos se vieron afectadas mientras que, en todo el mundo, la cifra alcanzó los 5 millones y todo esto tras la declaración de quiebra de FTX.

John Ray III, nombrado como nuevo director ejecutivo de la compañía describió la situación, afirmó que FTX había operado con una "falta completa de controles internos y una ausencia total de información financiera confiable" (Crypto crash: why the FTX bubble burst and the harm to consumers, 2022).

El caso de FTX pone de manifiesto algo importante y la ausencia de controles internos efectivos y la mala gestión pueden devastar ya que falta de transparencia financiera fue un factor clave. Este evento es un estudio de caso crucial para analizar la evidencia de auditoría, normativas como ISA 500, SAS 142 y AS 1105 son pertinentes en este contexto.

Finalmente, la quiebra de FTX resalta algo esencial ya que hay que revisar profundamente las normativas de auditoría, el objetivo es adaptarlas a contextos digitales, y, sobre todo, evitar fraudes contables en entornos cada vez más digitalizados.



Deficiencias en la evidencia electrónica y su impacto en la auditoría de FTX

El caso de FTX reveló fallas críticas en la gestión y control de la evidencia electrónica. Esto afectó la capacidad de los auditores para detectar y reducir el riesgo de fraude. Los auditores principales, Armanino LLP y Prager Metis CPAs, presentaron informes de auditoría cuestionados que según la demanda, esos informes no reflejaban con precisión la situación financiera de la empresa. Además, pasaron por alto deficiencias en los controles internos que comprometieron la validez de la evidencia electrónica.

En la *Disclosure Statement*, se añade que "las prácticas comerciales parecían estar motivadas por un deseo de secretismo". Esto, a su vez, dificultó la auditoría y generó un entorno favorable para el fraude (Disclosure Statement, 2024).

Un aspecto clave es que "los Auditores emitieron informes de auditoría limpios a pesar de la falta total de controles financieros internos confiables y la ausencia de un sistema de contabilidad adecuado" (FTX Cryptocurrency Exchange Collapse Litigation, 2023).

Esto evidenció una debilidad en el proceso, los auditores no prestaron atención a diversas "banderas rojas" presentes en los sistemas electrónicos de FTX y si estas señales se hubieran investigado a fondo, habrían revelado prácticas fraudulentas.

El control de los activos digitales fue inadecuado, la auditoría tradicional no resultó suficiente para identificar la gravedad de la gestión en FTX. Con la digitalización en aumento y el uso de blockchain para registrar transacciones, los métodos de auditoría deben adaptarse. Las normas SAS 142 y AS 1105 lo reconocen pero, sin embargo, el caso de FTX deja claro que aún existen importantes brechas en la supervisión de activos digitales.

El colapso de FTX se considera uno de los mayores fraudes desde Bernie Madoff (Trautman & Foster II, 2023), uno de los puntos más críticos fue la gestión de sus activos digitales y la falta de transparencia en los informes financieros. Los tokens¹⁴ FTT y Serum tenían valores documentados que superaban su precio real en el mercado lo que indica que "el valor documentado en el balance de FTX no podría haberse realizado en el mercado abierto" (Conlon, Corbet, & Hu, 2023). Este hecho destaca la

¹⁴ Activo digital que representa algún valor o derecho dentro de una plataforma o ecosistema específico.



fragilidad de los activos digitales como así también muestra cómo pueden distorsionar la percepción de la solvencia de una empresa.

Los auditores que revisaron los informes de FTX encontraron un entorno digital confuso donde verificar de forma independiente los activos resultaba complejo. En situaciones como esta, la normativa de auditoría necesita ser sólida, debe garantizar que los procedimientos de recolección y validación de la evidencia electrónica sean adecuados e identificar riesgos potenciales de fraude es fundamental. Esto adquiere mayor relevancia en contextos donde los activos electrónicos, como los tokens de FTX, pueden manipularse, ya sea interna o externa, puede inflar los balances financieros.

El uso incorrecto de los activos electrónicos fue un problema, además, la incapacidad de asegurar la integridad de las transacciones creó un vacío que afectó la evidencia disponible para los auditores. La falta de segregación entre los activos de los clientes y los corporativos complicó aún más la situación debido a que FTX operaba, en esencia, como una "caja negra" en la que los fondos se mezclaban sin trazabilidad clara ni control adecuado, esto hacía casi imposible rastrear el flujo de dinero en la plataforma. Violaba principios básicos de la ISA 500 que exige que la evidencia sea suficiente y adecuada, pero debido a las irregularidades y a la mala gestión de los datos electrónicos, no se cumplió con esta exigencia.

Sin embargo, Dupuis y sus colegas destacan algo importante, señalan que "los auditores aún enfrentan un paisaje cambiante de responsabilidades cuando se trata de clientes con participaciones significativas en criptoactivos" (Dupuis, Smith, Gleason, & Kannan, 2023). Los mercados de criptoactivos están en constante evolución y por ello, los auditores deben ajustar sus enfoques continuamente, especialmente en lo que respecta a la suficiencia y adecuación de la evidencia auditada.

El sistema financiero tradicional está diseñado para activos tangibles y financieros, estos activos son más estables y verificables en su valoración. En contraste, las criptomonedas, como los tokens de FTX, presentan un gran reto, son altamente volátiles ya que su valor depende de la percepción del mercado, no de un valor intrínseco fijo. Ray subrayó la falta de un sistema fiable en FTX, esto fue un factor crucial en su colapso: "Cuando asumí el control, no había una sola lista clara de clientes ni registros



fiables de las cuentas" (Crypto crash: why the FTX bubble burst and the harm to consumers, 2022).

La falta de regulación en el ámbito de las criptomonedas y los activos digitales incrementó los riesgos relacionados con FTX, Conlon et al. (2023) subrayan un aspecto importante: "Los activos no regulados como los tokens emitidos de manera privada por FTX jugaron un papel central en su caída" (Conlon, Corbet, & Hu, 2023).

La ausencia de un marco regulatorio sólido permitió que FTX operara con un elevado nivel de opacidad, lo que dificultó que los auditores pudieran obtener evidencia fiable para sustentar sus informes financieros.

El colapso de FTX demuestra la necesidad de normativas más precisas para los auditores, además, requieren directrices claras sobre cómo manejar la evidencia electrónica en entornos desregulados y las normas internacionales de auditoría ofrecen una base adecuada. Sin embargo, estas normativas deben adaptarse continuamente a los cambios tecnológicos y financieros que surgen en el entorno digital.

Por otro lado, la naturaleza de los activos digitales genera incertidumbre sobre la fiabilidad de la evidencia disponible. Allen destaca que "los activos cripto pueden ser creados de la nada, lo que genera apalancamiento y aumenta la vulnerabilidad del sistema a auges y caídas repentinas" (Crypto crash: why the FTX bubble burst and the harm to consumers, 2022). Esta volatilidad complica evaluar la suficiencia y adecuación de la evidencia.

La necesidad de marcos regulatorios específicos es clara, se requieren directrices para auditar la evidencia electrónica en contextos digitales, donde la complejidad y la incertidumbre son elevadas.

[Impacto del colapso de FTX en los mercados de criptomonedas](#)

Este fenómeno plantea un desafío importante para los auditores, deben validar la fiabilidad de las transacciones en un mercado que es, por su naturaleza, volátil y de rápida evolución. En este contexto, normas como ISA 500, SAS 142 y AS 1105 ofrecen directrices claras, su objetivo es guiar la recolección de evidencia que sea adecuada y suficiente. Sin embargo, las dinámicas cambiantes del mercado criptográfico exigen



ajustes constantes en estas normativas, así se garantiza que la evidencia recopilada siga siendo relevante en un entorno tan inestable.

El análisis de Fu et al. refuerza esta idea, "el colapso de FTX no fue un accidente, sino el resultado de violaciones graves contra un modelo racional de mercado" (Fu, Wang, Yu, & Chen, 2022). Esto pone en evidencia que el caso de FTX no fue un incidente aislado, sino un fraude sistémico e involucró no solo la manipulación de activos internos, como el token FTT, sino también el uso indebido de los fondos de los clientes. La caída de FTX revela las deficiencias en la gestión financiera cuando no existen controles adecuados sobre la calidad y suficiencia de la evidencia de auditoría. La evaluación de la calidad de los activos electrónicos adquiere especial relevancia, Fu et al. señalan que "FTT es un token de tipo Ponzi inherente, lo que significa que no está respaldado por ningún activo" (Fu, Wang, Yu, & Chen, 2022). Este hecho presenta un desafío directo para las normativas de auditoría en la valoración de activos electrónicos. La falta de respaldo financiero real para este tipo de activos digitales dificulta la obtención de evidencia suficiente para asegurar la exactitud de las declaraciones financieras.

Una de las conclusiones clave del análisis sobre FTX es significativa, las Criptomonedas "verdes" como Ethereum y Polygon tuvieron solo un aumento moderado en la volatilidad tras el colapso, sin embargo, las stablecoins¹⁵ mostraron un comportamiento distinto.

Las Stablecoins como Tether y USD Coin registraron una inestabilidad mucho mayor, el estudio afirma que "las stablecoins, que se supone son las más estables, mostraron la mayor inestabilidad". Tether multiplicó su volatilidad intradía hasta 9 veces, en el caso de USD Coin, esta se incrementó hasta 14 veces (Esparcia, Escribano, & Jareño, 2024). Este resultado es crucial para la auditoría debido a que demuestra que incluso los activos considerados seguros no son inmunes a fraudes y malas prácticas. Esto indica la necesidad de un escrutinio más riguroso y la evidencia electrónica vinculada a estos activos requiere mayor atención.

¹⁵ Tokens emitidos que mantienen la paridad de una moneda, usualmente dólar estadounidense.



El colapso de FTX no solo impactó el mercado de criptomonedas, su efecto se extendió también a los mercados financieros tradicionales; esto provocó un "efecto contagio", un fenómeno donde la crisis de una empresa o sector afecta a otras partes del sistema financiero.

Conlon et al. (2023) destacan este punto, "el colapso de FTX desencadenó efectos de contagio" y estos efectos impactaron no solo a las criptomonedas sino también afectaron activos financieros tradicionales, como las divisas y los productos básicos (Conlon, Corbet, & Hu, 2023). Este hecho subraya algo importante, existe una creciente interconexión entre los mercados de criptomonedas y los mercados financieros tradicionales.

Para los auditores, este tipo de contagio presenta un reto adicional, es complejo evaluar los riesgos sistémicos asociados al colapso de una empresa en un entorno digital. La evidencia debe ser suficiente para prever y mitigar estos riesgos, por ello, es fundamental adaptar las normativas de auditoría, estas deben incluir aspectos sobre el posible impacto global de empresas que manejan activos digitales.

El ascenso y caída de FTX

Fundada en 2019, FTX alcanzó una posición influyente en el mercado de activos digitales. A poco de su creación, ya había logrado una valorización superior a \$30 mil millones, pero en noviembre de 2022, ocurrió el abrupto colapso de FTX. Como lo relatan Roy, Anand y Chandra (2022), "el 11 de noviembre de 2022, FTX presentó la solicitud de quiebra debido a la falta de fondos para pagar a sus acreedores y honrar las retiradas de los clientes" (Roy, Anand, & Chandra, 2022). La filtración de un balance financiero de Alameda Research precedió a esta quiebra, anticipando así el desenlace, esta empresa estaba profundamente vinculada a FTX.

El balance reveló una composición de activos altamente inestable ya que la mayoría de estos se sustentaban en el token FTT, emitido por FTX, que perdió valor de manera abrupta. Mackenzie (2024) añade, además, otro aspecto clave: la "actividad ilegal tras bambalinas".

Esta actividad incluía el uso indebido de depósitos de clientes para financiar operaciones de riesgo en Alameda Research, asimismo, financiaba gastos personales de



Sam Bankman-Fried (Mackenzie, 2024). La falta de segregación de los fondos de los clientes y una gestión interna ineficaz contribuyeron críticamente a la debacle de FTX. Este caso acentúa la relevancia de controles internos robustos en auditoría, de lo contrario, los sistemas internos se tornan vulnerables y en este contexto, la integridad de las transacciones electrónicas debe ser evaluada rigurosamente por los auditores. La crisis de confianza en FTX, acelerada por las decisiones de Binance, un actor competidor en criptomonedas, y la incapacidad de FTX para cubrir retiros masivos, generaron una crisis de liquidez y todo esto culminó en la inevitable declaración de quiebra.

La situación expone los efectos de una ausencia de auditoría externa confiable y controles internos sólidos, además, se advierte sobre los riesgos de dependencia en activos propios, que suelen ser más vulnerables. La falta de controles adecuados y la mezcla de activos entre entidades relacionadas violaron principios de auditoría fundamentales. Normas como la ISA 500, que regula la suficiencia y adecuación de evidencia, se incumplieron flagrantemente.

En efecto, FTX permitió que Alameda mantuviera un saldo negativo, accediendo sin límites a reservas de intercambio. En la práctica, FTX empleaba el dinero de sus clientes en apuestas del mercado de criptomonedas, cuestionando profundamente la confiabilidad de sus registros financieros.

La dependencia de FTX en tokens autogenerados, como FTT y Serum, muestra cómo la falta de un respaldo intrínseco o una valoración confiable en los mercados tradicionales afectó su estabilidad. El colapso se debió en gran medida a la falta de liquidez y transparencia en estos activos digitales. Conlon et al. (2023) explican que "la mayor parte del valor de los activos de FTX se atribuía a una pequeña cantidad de tokens emitidos de manera privada" (Conlon, Corbet, & Hu, 2023), y esta estructura permitió que, por medio de FTT, FTX inflara sus balances, poniendo en riesgo a sus inversores y acreedores.

Los auditores, en un contexto así, enfrentan serios desafíos para evaluar la validez de la evidencia financiera que una empresa digital como FTX presenta, especialmente si esta se basa en activos sin un valor determinado en mercados tradicionales. La ISA 500, norma internacional que regula la suficiencia de evidencia en auditoría, se pone a



prueba cuando, como en FTX, el balance refleja asimetría entre activos y pasivos, creando dudas sobre la solvencia que esos activos digitales podrían garantizar.

La manipulación de la evidencia electrónica y su rol en el fraude contable

La volatilidad en el caso de FTX resalta cómo la correcta gestión y análisis de la evidencia electrónica es fundamental para detectar y mitigar posibles fraudes. Un punto crucial fue la transferencia no autorizada de unos 4 mil millones de dólares hacia Alameda Research, entidad ligada directamente a Sam Bankman-Fried. Este movimiento financiero se convirtió en un factor decisivo que precipitó la bancarrota de FTX.

El problema se amplificó por la carencia de una separación clara entre los fondos de los clientes y los corporativos, lo que facilitó que estos fueran manejados sin restricciones. Al no contar con barreras efectivas entre las cuentas, los activos de los clientes podían ser utilizados para otros fines, exponiendo a FTX a riesgos financieros significativos sin mecanismos de control que aseguraran la transparencia de las operaciones.

La utilización de software para eliminar conversaciones y ocultar decisiones cruciales complicó el rastreo de las transacciones como así también impidió a los auditores y reguladores determinar con precisión las actividades financieras de la empresa.

La "Disclosure Statement For Debtors' Joint Chapter 11" reporta que la falta de registros confiables y el uso de aplicaciones de mensajería con funciones de autodestrucción, como Signal, imposibilitaron la recolección de evidencia adecuada. Esto no solo dificultó la reconstrucción de los hechos financieros, sino que obstruyó la posibilidad de una auditoría precisa (Disclosure Statement, 2024).

Roy y otros autores destacan que Sam Bankman-Fried incentivaba el uso de aplicaciones que eliminaban automáticamente las conversaciones. Estas prácticas no solo erosionaban la posibilidad de obtener evidencia suficiente en casos de fraude, sino que también permitían ocultar el estado financiero real de FTX (Roy, Anand, & Chandra, 2022). Esta falta de rastros claros de las decisiones empeoró la situación. Las investigaciones revelaron que Alameda Research utilizó fondos de clientes para inversiones de alto riesgo, incrementando la vulnerabilidad de ambas entidades. Según el testimonio del senador Patrick Toomey ante el Senado de Estados Unidos, esta



operación involucraba "préstamos no autorizados de activos de clientes a una entidad afiliada, además de promesas fraudulentas a los inversores" (Crypto crash: why the FTX bubble burst and the harm to consumers, 2022).

Estas prácticas revelan fallos profundos en los controles internos de FTX, especialmente en una empresa que maneja criptomonedas. Aunque las normativas de auditoría como la ISA 500, SAS 142 y AS 1105 ofrecen un marco para la recolección y evaluación de la evidencia, el caso FTX evidencia que la auditoría de criptomonedas aún está en evolución, dejando vacíos significativos en cuanto a la identificación y mitigación de riesgos relacionados con la integridad de los controles financieros (Dupuis, Smith, Gleason, & Kannan, 2023). El uso inadecuado de la evidencia electrónica por parte de FTX, especialmente la falta de reconciliación de activos digitales con las posiciones de los clientes, intensificó el problema. No existía segregación clara de activos ni control adecuado sobre las transacciones. Los gestores utilizaron los fondos de los clientes para inversiones fallidas y gastos personales (Disclosure Statement, 2024). Esto no solo dañó la confianza de los inversionistas, sino que además complicó la labor de los auditores. La carencia de registros precisos conlleva a enfatizar la necesidad de sistemas que garanticen la trazabilidad de las transacciones electrónicas.

Normativas como ISA 500 y AS 1105 resaltan esta trazabilidad y la tenencia de registros detallados, más aún en entornos de transacciones electrónicas. En FTX, la incapacidad para mantener estos registros críticos socava la posibilidad de una auditoría precisa. Este problema, especialmente en entornos digitales donde las transacciones rápidas pueden "desaparecer", complica aún más la labor de auditoría. La evidencia digital resulta clave en la detección de irregularidades financieras.

La caída del 77.34% del valor del token FTT en una sola sesión de negociación provocó una crisis de liquidez (Esparcia, Escribano, & Jareño, 2024), lo cual generó una masiva cantidad de datos electrónicos que los auditores deben analizar para identificar posibles fraudes.

Así, las normativas de auditoría cumplen un papel esencial en el manejo de evidencia electrónica en situaciones de fraude. La volatilidad de los criptoactivos, unida a la opacidad en algunas transacciones electrónicas, complica la tarea de los auditores, quienes necesitan herramientas avanzadas para analizar grandes volúmenes de datos.



Un aspecto crítico del colapso de FTX fue la ausencia de controles internos efectivos. John J. Ray III calificó la situación como una "falla completa de los controles corporativos" y una falta de información financiera confiable (Roy, Anand, & Chandra, 2022). Además, FTX no segregaba los fondos de los clientes, mezclándolos en cuentas 'ómnibus' (FTX Cryptocurrency Exchange Collapse Litigation, 2023), lo que violaba tanto los acuerdos con los clientes como los principios contables básicos, generando una estructura financiera opaca.

La ausencia de libros de contabilidad adecuados y la mezcla indiscriminada de activos entre diversas entidades dentro del grupo FTX representan una serie de malas prácticas que complicaron enormemente la labor de los auditores para obtener evidencia confiable. La profesora Hilary J. Allen lo describe con precisión en su testimonio, señalando que "la falta de auditorías independientes y la manipulación de los activos mediante tokens generados por la propia empresa hacían imposible realizar una auditoría efectiva bajo estándares tradicionales" (Crypto crash: why the FTX bubble burst and the harm to consumers, 2022). Este tipo de manipulación no solo revela la carencia de controles internos sólidos, sino que también subraya la importancia de que las auditorías se realicen bajo estrictos marcos normativos.

Las normas de auditoría como ISA 500 y SAS 142 se vuelven esenciales en escenarios como el de FTX, ya que proveen directrices sobre la suficiencia y adecuación de la evidencia de auditoría. Sin embargo, la ausencia de registros contables adecuados dentro de FTX violó principios fundamentales de estas normativas, lo que hizo imposible realizar una auditoría completa y transparente. En este tipo de casos, los auditores deben tener acceso completo a todas las transacciones electrónicas relevantes para evaluar si se cumplen las regulaciones contables y los principios financieros aceptados. La deliberada opacidad y la falta de control sobre los registros electrónicos en FTX fueron determinantes para impedir una evaluación precisa de su situación financiera.

Uno de los elementos más críticos fue el uso indebido de las cuentas bancarias de Alameda para recibir depósitos de clientes de FTX sin su conocimiento. Mackenzie (2024) afirma que "Bankman-Fried mintió a los funcionarios bancarios de EE. UU. al abrir una nueva cuenta en nombre de Alameda, afirmando que estaba destinada a la



actividad especulativa de esa empresa, cuando en realidad se utilizó para recibir depósitos de FTX” (Mackenzie, 2024).

Este fraude, en su impacto, expone una urgencia crítica por establecer controles más rigurosos sobre transacciones electrónicas y evidencia digital en auditoría. La estructura de cuentas "ómnibus" utilizada complicó la trazabilidad, permitiendo que Sam Bankman-Fried y otros ejecutivos desviarán fondos sin el conocimiento de clientes o de reguladores. Además, la facilidad con la que pudieron ocultarse los movimientos exacerbó la crisis de manera alarmante.

La imposibilidad de los auditores para identificar las inconsistencias entre los fondos reportados y las transacciones reales dejó ver que la falta de controles internos y externos fue un factor clave. Prácticas fraudulentas lograron sostenerse en gran medida debido a esta carencia y en este contexto, SAS 142 y AS 1105 aparecen como normativas relevantes. Ambos estándares proporcionan guías sobre la recolección y evaluación de la evidencia electrónica en ambientes de alta volatilidad y riesgo, como el mercado de criptomonedas.

Sin embargo, la aplicación insuficiente de estos estándares permitió que el fraude continuara. Así, las pérdidas escalaron hasta un punto crítico, dejando en evidencia la urgente necesidad de marcos normativos más sólidos y de una supervisión activa en el manejo de la evidencia digital.

Vulnerabilidad y riesgos en el control de claves privadas

En la auditoría de activos digitales, un punto esencial radica en la vulnerabilidad asociada al manejo de las claves privadas. Dichas claves, dentro del contexto de las criptomonedas, confieren un acceso determinante para controlar y transferir estos activos digitales. El riesgo crítico aquí es la potencial pérdida o robo de una clave privada, evento que conlleva la irrecuperabilidad absoluta de los fondos vinculados. El caso de FTX ejemplifica cómo una deficiencia en la administración de claves puede exponer los activos a fraude y resultar en pérdidas significativas.

Dupuis et al. (2023) advierten: "los auditores deben mantener un escepticismo profesional en cuanto a las afirmaciones de los clientes sobre la tenencia de criptomonedas y la solidez de sus marcos de control interno". Esta premisa está alineada



con la ISA 500, que recalca la necesidad de evidencia suficiente y adecuada. En criptomonedas, esto implica la inspección rigurosa de elementos críticos, como el almacenamiento en frío y la integridad de la gestión de las claves privadas.

Conectividad entre cryptoactivos y el contagio de riesgos

Otro aspecto relevante del caso FTX es la conectividad y el contagio entre diferentes cryptoactivos, el estudio muestra cómo la caída de FTX provocó un efecto dominó en otros mercados, especialmente en aquellos directamente conectados con el token FTT. “El token FTT mostró un alto efecto de spillover [contagio] hacia otras criptomonedas, especialmente hacia stablecoins como USD Coin” (Esparcia, Escribano, & Jareño, 2024). Manda y Yadav fueron más efusivos al afirmar que “la caída de FTX añadió combustible al fuego y desencadenó un efecto dominó que llevó a la caída de varias otras instituciones financieras vinculadas al negocio de las criptomonedas” (Manda & Yadav, 2023).

Esta conectividad entre activos plantea desafíos adicionales para los auditores que necesitan evaluar cómo las fluctuaciones en un activo pueden afectar la estabilidad y la veracidad de otros. En un entorno financiero tan interconectado, la capacidad de identificar y analizar las relaciones entre diferentes activos es fundamental para proporcionar una evaluación adecuada de la evidencia de auditoría.

La fragilidad del sistema financiero emergente basado en criptomonedas queda de manifiesto en sus similitudes con el sistema financiero tradicional. Entre las vulnerabilidades compartidas se destacan los riesgos de contraparte, el potencial de lavado de dinero y, además, la opacidad presente en ciertas operaciones.

Surge, entonces, una necesidad imperiosa de regulación más estricta también es crucial el desarrollo de mecanismos de evaluación de riesgos que fortalezcan la estructura de estas plataformas.

La propagación de riesgos entre distintas criptomonedas subraya la necesidad de que las metodologías de auditoría evolucionen. Es imprescindible que estas metodologías incorporen la interconexión entre diferentes tipos de evidencia debido a que no basta con evaluar cada cryptoactivo de forma aislada; el enfoque debe considerar cómo la caída de una plataforma puede impactar en la estabilidad de otros activos asociados.



Esta perspectiva interrelacionada resulta fundamental para auditorías que reflejen de manera precisa la complejidad tecnológica y financiera actual de los entornos criptográficos.

El contagio financiero, documentado en crisis anteriores, se evidenció de manera contundente con el colapso de FTX. Sus efectos se extendieron más allá de las empresas con vínculos directos, alcanzando incluso a entidades sin conexiones explícitas. Este “riesgo de contagio”, es decir, la propagación del estrés financiero entre entidades se observó en las caídas de plataformas como BlockFi y Silvergate Bank tras la quiebra de FTX. BlockFi, por ejemplo, informó de una “exposición significativa” a FTX, esto precipitó su bancarrota al día siguiente del colapso (Manda & Yadav, 2023).

Silvergate Bank, que mantenía estrechos vínculos con el sector crypto al actuar como intermediario entre clientes y el sistema financiero tradicional, sufrió una pérdida superior a mil millones de dólares en 2022. Asimismo, enfrentó una fuga de depósitos cercana al 52 % debido a la desconfianza generada.

El derrumbe de FTX también desencadenó investigaciones regulatorias y creó un efecto en cadena en firmas auditoras como Mazars, responsable de verificar las reservas de Binance y Crypto.com. La creciente desconfianza llevó a Mazars a suspender sus auditorías, exponiendo una falencia crítica: la falta de transparencia y la ineficacia de las auditorías para validar de manera confiable las reservas digitales.

El caso FTX demuestra la relevancia de contar con evidencia de auditoría robusta y detallada, especialmente electrónica y evaluar la calidad y suficiencia de la información financiera en activos digitales requiere controles efectivos. La manipulación y ocultación de datos financieros en FTX se facilitó por la falta de controles adecuados, evidenciando una debilidad estructural del sector. Esto subraya la necesidad de establecer controles más estrictos y auditorías adaptadas a los riesgos específicos de los entornos digitales.

Gobernanza corporativa y la necesidad de regulaciones más estrictas

Un factor que profundizó el colapso de FTX fue la notable ausencia de controles internos robustos junto con una deficiente gobernanza corporativa, el informe sostiene que “la crisis de FTX se originó más por fallos en la gobernanza corporativa y la falta



de supervisión regulatoria que por problemas inherentes a las criptomonedas” (Esparcia, Escribano, & Jareño, 2024). Este hecho implica un análisis profundo para evaluar la evidencia en auditoría; no es suficiente limitarse a las transacciones. Es crucial examinar tanto los sistemas de control interno como las estructuras de gobernanza, encargadas de evitar desde el inicio transacciones fraudulentas.

La operativa de plataformas como FTX, en un entorno con regulaciones escasas y volatilidad, obstaculiza el uso de enfoques tradicionales de auditoría. Entre los principales problemas, la falta de un marco regulatorio efectivo se destaca, según la demanda colectiva: "FTX estaba utilizando los activos de los clientes para financiar otras operaciones y no mantenía un registro adecuado de estas transacciones electrónicas" (FTX Cryptocurrency Exchange Collapse Litigation, 2023). Las plataformas, en ausencia de una supervisión firme, actúan sin restricciones.

La profesora Hilary J. Allen, en sus intervenciones ante el Congreso estadounidense, afirmó que "las pruebas de reserva y otros métodos de contabilidad que se utilizan en la industria de las criptomonedas son pobres sustitutos de las auditorías rigurosas e independientes" (Crypto crash: why the FTX bubble burst and the harm to consumers, 2022). Esta afirmación evidencia la urgente necesidad de implementar marcos regulatorios sólidos para proteger a los consumidores y garantizar verificaciones más completas.

El contexto regulatorio incierto en las transacciones electrónicas subraya una deficiencia preocupante, exponiendo la auditoría a desafíos significativos en la verificación de registros. La adaptación de normativas, tales como la ISA 500 y la AS 1105, se convierte en un requerimiento indispensable en este panorama. Esta adaptación debe enfocarse en cubrir los riesgos inherentes y los elementos específicos de los activos digitales y plataformas de criptomonedas.

Lograr esta actualización normativa no solo ayudaría a mitigar riesgos de fraude y manipulación de registros, sino que constituiría un avance fundamental hacia la creación de un entorno financiero en el que la transparencia y la seguridad en el ámbito de las criptomonedas sean reales y efectivas.

En esta misma línea de pensamiento, durante el testimonio presentado por Kevin O’Leary, inversor, ante el Senado de los Estados Unidos, afirmó que la empresa



operaba de manera "no regulada" y fuera del alcance de las normativas tradicionales. Este vacío regulatorio permitió que se realizaran transacciones riesgosas y no se implementaran controles internos adecuados. O'Leary afirma que "la razón por la que esto está sucediendo una y otra vez [...] es la falta de regulación" (Crypto crash: why the FTX bubble burst and the harm to consumers, 2022). En la misma sesión del Senado, Ben McKenzie Schenkkan, actor y autor, sostiene que esta carencia de regulación permitió que FTX realizara prácticas de alto riesgo con el dinero de sus usuarios sin tener que rendir cuentas a ninguna autoridad reguladora. Las plataformas centralizadas de criptomonedas, como FTX, deberían haber estado sujetas a auditorías externas e independientes, tal como lo exigen las normativas aplicadas a las instituciones financieras tradicionales (Crypto crash: why the FTX bubble burst and the harm to consumers, 2022). Las normas de auditoría, como la SAS 142, insisten en que las auditorías deben evaluar las transacciones con partes relacionadas y cualquier actividad que pueda poner en peligro los fondos de los clientes. Sin embargo, FTX operaba sin estar sujeta a estas normas, lo que permitió que los riesgos financieros no fueran detectados hasta que ya era demasiado tarde.

McKenzie Schenkkan sostiene que un marco regulatorio diseñado exclusivamente para las criptomonedas es no solo necesario, sino imprescindible, y debe adaptarse a las particularidades y la naturaleza cambiante de este sector (Crypto crash: why the FTX bubble burst and the harm to consumers, 2022). La complejidad y rápida evolución del mercado cripto indican que las regulaciones tradicionales resultan insuficientes para abordar los riesgos únicos que conllevan los activos digitales.

Desarrollar normativas nuevas es, por tanto, crucial; las regulaciones deben integrar tanto los avances tecnológicos propios de las criptomonedas como las vulnerabilidades particulares de este mercado.

Esto permitirá establecer medidas de protección que sean efectivas y realistas para los activos digitales. En un entorno digital caracterizado por una velocidad y complejidad en constante aumento, la generación de datos es ahora más extensa que nunca.

Dado este contexto, resulta esencial que los auditores cuenten con herramientas avanzadas que les permitan abordar la verificación de estos datos de manera efectiva. Así, pueden abordar eficazmente la magnitud y diversidad de la información y podrán



procesar las enormes cantidades de información electrónica que el sistema demanda. Por tanto, se requiere aplicar técnicas especializadas en análisis de datos e igualmente, se vuelve necesario incorporar el blockchain, lo cual permite una trazabilidad más robusta, además su uso facilita la verificación de transacciones electrónicas en tiempo real.

El caso de FTX ha demostrado que la incapacidad de los auditores para adaptarse a los avances tecnológicos puede permitir la omisión de fraudes importantes, los cuales podrían haberse detectado mediante controles más rigurosos sobre la evidencia digital. Aunque FTX ha sido objeto de duras críticas, O'Leary resalta el potencial de la tecnología blockchain, la cual podría ofrecer soluciones sólidas en el contexto adecuado. Según su argumento, "la tecnología blockchain es muy poderosa, y deberíamos ser líderes mundiales en ella" (Crypto crash: why the FTX bubble burst and the harm to consumers, 2022). Este comentario subraya que, pese a la vulnerabilidad de los sistemas cripto frente al fraude cuando operan sin regulación, los mecanismos tecnológicos como el blockchain pueden facilitar una auditoría efectiva y rastreo de transacciones, siempre que existan marcos regulatorios apropiados.

La insuficiencia de regulaciones adecuadas en el sector de los criptoactivos sigue siendo una problemática creciente. A pesar de los esfuerzos regulatorios, como la ley de mercados en criptoactivos (MiCA) en la Unión Europea y las recientes normas de la Junta de Normas de Contabilidad Financiera (FASB) en Estados Unidos, aún "queda mucho por hacer" para garantizar la protección de los inversores y mejorar la transparencia del mercado (Esparcia, Escribano, & Jareño, 2024).

Las normativas de auditoría, tales como la ISA 500, SAS 142 y AS 1105, requieren una continua adaptación, esto es crucial para implementar criterios más estrictos en la evaluación de controles internos. En el sector cripto, los riesgos de fraude y malversación se elevan significativamente debido a la descentralización y a la opacidad frecuente de sus transacciones.

El colapso de FTX ha desencadenado una respuesta regulatoria a nivel global, ya que diversos organismos, entre ellos la Comisión de Valores de EE. UU. (SEC) y la Comisión de Comercio de Futuros de Productos Básicos (CFTC), ya han iniciado investigaciones sobre las prácticas internas de la empresa. Según el informe, "el colapso



de FTX provocará casi con certeza una respuesta regulatoria de varios gobiernos en todo el mundo” (Roy, Anand, & Chandra, 2022).

Esto evidencia la necesidad de normativas más estrictas sobre el uso de fondos de clientes en plataformas de criptomonedas y de procedimientos de gobernanza fortalecidos.

La teoría de la "normalización de la devianza", propuesta por Mackenzie (2024), expone cómo FTX fue adoptando prácticas riesgosas hasta convertirlas en costumbre aceptada dentro de la empresa, sin que se evaluaran sus consecuencias. Esta aceptación progresiva de altos riesgos, sin controles adecuados, fue un factor clave en su colapso. En paralelo, Jennifer J. Schulp presentó ante el Senado estadounidense la necesidad de un marco regulatorio¹⁶ que contemple las particularidades de las criptomonedas, en lugar de aplicar normas creadas para valores tradicionales. Según Schulp, "las políticas diseñadas para abordar los riesgos de los intermediarios financieros centralizados no deben aplicarse ciegamente a proyectos descentralizados" (Crypto crash: why the FTX bubble burst and the harm to consumers, 2022). Esto indica que la regulación debe adaptarse a las características específicas de los criptoactivos y la tecnología blockchain. La situación de FTX subraya, en última instancia, la urgencia de una regulación especializada para el sector cripto, con controles específicos que respondan a su complejidad y particularidades.

La cultura corporativa de FTX estaba profundamente influenciada por la figura de Bankman-Fried, quien, según el autor, promovía un enfoque despreocupado ante los riesgos. Esto generó un ambiente en el cual los empleados evitaron cuestionar decisiones que reconocían como incorrectas. Este fenómeno, identificado como "culto a la personalidad," otorgó a Bankman-Fried una influencia indebida sobre su equipo, normalizando prácticas que contravenían principios fundamentales de gestión financiera y control corporativo. Mackenzie observa que “el propio SBF no tomó en serio los riesgos involucrados en su enfoque ilegal para manejar las finanzas de FTX” (Mackenzie, 2024).

¹⁶ Esta propuesta de marco regulatorio se encuentra explicada en el Anexo II: Propuesta de un marco regulatorio para criptomonedas según Jennifer J. Schulp.



En el ámbito de la auditoría, el colapso de FTX destaca la imperiosa necesidad de revisar y actualizar las normativas actuales. Las normas deben evolucionar para incorporar procedimientos mucho más rigurosos en la evaluación de la evidencia electrónica, lo que es crucial para que los auditores puedan rastrear y verificar transacciones en entornos cada vez más digitales y descentralizados. Para los inversores que confiaron en FTX, esta situación ha resultado en procesos de quiebra prolongados, con pocas garantías de recuperar sus fondos. En muchos casos, estos inversores pueden no recuperar sus fondos, esta realidad plantea interrogantes esenciales sobre el nivel de riesgo al que están expuestos los inversores en mercados sin regulación suficiente y sobre el rol crucial que las auditorías deben asumir en la prevención de fraudes dentro del ámbito de los criptoactivos.¹⁷

Cumplimiento de los objetivos para el caso de estudio

Suficiencia y adecuación

La evaluación de los principios fundamentales en las normas ISA 500, SAS 142 y AS 1105, aplicados al caso de Exchange FTX, evidencia implicancias críticas para la práctica de la auditoría.

La ISA 500 establece criterios rigurosos. Busca asegurar que la evidencia obtenida cumpla con los principios de suficiencia y adecuación. La calidad y la cantidad de la evidencia son elementos esenciales. Estos deben soportar las conclusiones y la opinión de auditoría. Sin embargo, en el caso de FTX, se observaron fallas significativas. Las deficiencias en la evidencia electrónica representaron un obstáculo considerable. La validación y verificación de transacciones digitales resultaron inadecuadas. Además, la naturaleza compleja de los criptoactivos complicó aún más el cumplimiento de la suficiencia establecida por la norma.

La SAS 142 enfatiza la relevancia y la fiabilidad como atributos de la evidencia. Este enfoque complementa la ISA 500. Sin embargo, se presentaron limitaciones evidentes en el contexto tecnológico de FTX. La manipulación de la evidencia electrónica

¹⁷ El caso Exchange FTX se puede ver de forma resumida en el Anexo VII: Caso Exchange FTX – Mapa Mental.



comprometió su fiabilidad. Los auditores encontraron obstáculos para evaluar la adecuación. La opacidad en la información dificultó cumplir con los principios de suficiencia.

Por otro lado, la AS 1105, establecida por el PCAOB, resalta la importancia de la evidencia cualitativa y cuantitativa. Busca que esta sea suficiente para soportar la opinión del auditor. Pero en el contexto de FTX, surgieron limitaciones claras. La falta de control sobre las claves privadas reveló vulnerabilidades. La gobernanza corporativa deficiente agravó la situación. Las barreras para corroborar la integridad y fiabilidad de los datos electrónicos complicaron la práctica de la auditoría.

En resumen, aunque estas normas pretenden garantizar rigor y suficiencia, su aplicación enfrentó retos notables. Las operaciones digitales y la tecnología avanzada de FTX resaltaron las limitaciones. Cumplir con los principios de suficiencia y adecuación en entornos digitales demostró ser problemático. Las auditorías en escenarios de alta complejidad tecnológica mostraron vulnerabilidades significativas.

[Evaluación de la calidad de la evidencia](#)

En el caso de Exchange FTX, la comparación de cómo cada normativa aborda la evaluación de la calidad de la evidencia revela matices importantes. Cada marco normativo tiene un enfoque particular que afecta el proceso de auditoría y plantea desafíos distintos.

ISA 500 prioriza dos elementos clave: suficiencia y adecuación de la evidencia. Esta norma obliga al auditor a verificar la calidad por medio de la relevancia y fiabilidad de la información obtenida. Para un caso como FTX, en el que la evidencia electrónica es central, la ISA 500 impone la validación rigurosa de fuentes digitales. Y así, el auditor debería revisar si los registros y bases de datos eran íntegros y auténticos. También evaluar si los controles de acceso eran lo suficientemente sólidos para evitar manipulaciones.

Por otro lado, SAS 142 introduce un enfoque que profundiza en la naturaleza y origen de la evidencia. Su énfasis recae en características como la relevancia y la fiabilidad de la información usada. Esto es crucial en un entorno como el de FTX. En un escenario donde los sistemas digitales pueden ser manipulados, SAS 142 exigiría que los



auditores analicen las fuentes electrónicas y su resistencia a manipulaciones. Esto incluiría el estudio de los controles internos y las debilidades en la gestión de claves privadas.

AS 1105 aporta un enfoque que enfatiza la cantidad y la calidad de la evidencia. Busca una perspectiva crítica y pragmática. En un caso complejo como FTX, la AS 1105 subrayaría la necesidad de pruebas corroborativas. Esto es vital cuando se observan irregularidades en los registros. La norma también destacaría la importancia de contrastar la evidencia con otras fuentes para confirmar su validez. Esto es especialmente relevante en un entorno de criptoactivos. Estos son conocidos por su limitada transparencia y trazabilidad.

La comparación de los efectos de estas normas en el caso FTX sugiere diferentes consecuencias. La ISA 500 requeriría controles estrictos sobre la autenticidad y la trazabilidad de la evidencia. De no cumplirse, la evidencia se consideraría insuficiente. SAS 142 obligaría a los auditores a evaluar más a fondo la fuente de la información. Esto es especialmente relevante ante la posibilidad de manipulación. Por último, AS 1105 resaltaría la necesidad de obtener evidencia adicional y suficiente. Esto sería para corroborar la integridad de los registros. Un enfoque indispensable en el caso de irregularidades.

La combinación de los tres enfoques podría haber llevado a una detección más temprana de las fallas en FTX. La ISA 500 ofrece una estructura general. SAS 142 añade un análisis de la calidad más profundo. AS 1105 refuerza la necesidad de evidencia robusta y crítica. Todo ello habría potenciado la capacidad de los auditores para identificar inconsistencias y mitigar riesgos en un entorno complejo como el de los criptoactivos.



Evidencia electrónica en los casos de estudio - comparación de la ISA 500, SAS 142 y AS 1105

Evidencia de Auditoria	Caso Madoff	Caso Olympus	Caso Peregrine	Caso Theranos	Caso FTX
ISA 500	El aplicar ISA 500 habría resaltado la urgencia de implementar procesos robustos para evaluar evidencia de fuentes electrónicas. La revisión insuficiente de registros digitales permitió que se ocultaran irregularidades clave en el esquema Ponzi.	La implementación de la ISA 500 habría resaltado, en primer lugar, la importancia de la suficiencia de la evidencia, también, habría subrayado la necesidad de su adecuación. Este enfoque, en consecuencia, podría haber detectado inconsistencias en los registros contables, y, además, habría revelado transacciones estructuradas usadas para ocultar pérdidas.	Habría destacado la importancia de evaluar la suficiencia y adecuación de la evidencia electrónica. La falta de validación permitió ocultar activos y cuentas falsas. Esta norma subraya la necesidad de confirmar la autenticidad de las fuentes electrónicas.	Habría destacado la necesidad de obtener evidencia suficiente y adecuada. La falta de validación externa permitió la presentación de resultados falsos, mostrando la importancia de verificar fuentes internas.	Habría enfatizado la validación de la autenticidad y seguridad de la evidencia digital, destacando deficiencias en los controles de acceso y la trazabilidad de registros, lo que habría facilitado la detección de irregularidades en transacciones cripto y contabilidad.
SAS 142	Una revisión bajo SAS 142 habría exigido	La aplicación de SAS 142 habría	Un enfoque bajo SAS 142 habría exigido	Habría exigido una revisión rigurosa de la	Requeriría evaluar la fiabilidad de



	<p>que los auditores cuestionaran la fiabilidad de la evidencia digital. ¿Resultado en Madoff? La manipulación de registros electrónicos pasó inadvertida, en parte, por no validar correctamente la autenticidad según las directrices de SAS 142.</p>	<p>requerido una revisión exhaustiva de la fiabilidad de la evidencia presentada. Esto sería crítico para detectar transacciones simuladas y verificar que los documentos respaldaran fielmente las operaciones financieras reportadas.</p>	<p>una verificación más estricta de la fiabilidad de la evidencia digital. Su aplicación implicaría validar rigurosamente documentos y balances para detectar manipulaciones. La norma resalta la relevancia de corroborar que las pruebas apoyen fielmente las operaciones.</p>	<p>fiabilidad de la evidencia presentada, detectando inconsistencias en los resultados tecnológicos y médicos.</p>	<p>las fuentes electrónicas, instando a los auditores a verificar la integridad de los registros digitales para descubrir manipulaciones ocultas en sistemas contables y activos cripto.</p>
AS 1105	<p>La AS 1105 habría subrayado la revisión profunda de los controles internos sobre los sistemas digitales. ¿Por qué fue relevante? La falta de evaluación y pruebas de software facilitó la</p>	<p>La AS 1105 habría implicado un análisis detallado de la calidad y cantidad de la evidencia, incluyendo la procedencia de los registros electrónicos. Esto habría ayudado a descubrir irregularidades</p>	<p>AS 1105 habría requerido un análisis detallado de los controles internos de los sistemas electrónicos. La ausencia de pruebas adecuadas permitió cuentas fraudulentas. Esta norma enfatiza la</p>	<p>Habría requerido un examen detallado de los controles internos y la calidad de la evidencia digital, subrayando la necesidad de corroborar los procesos y evitar manipulaciones.</p>	<p>Subrayaría la revisión de controles internos y la calidad de la evidencia. La norma habría destacado la necesidad de corroborar registros y reportes digitales para evitar manipulaciones y garantizar la</p>



	manipulación de registros financieros, un punto que AS 1105 aborda al recomendar la corroboración de datos digitales.	en los informes y a confirmar la autenticidad de las transacciones, evaluando las prácticas de control interno de la compañía.	revisión profunda y la corroboración de la calidad de la evidencia presentada.		integridad de la información financiera.
--	---	--	--	--	--

Fuente: elaboración propia.



Conclusión Final

En el presente análisis se investigaron dos hipótesis que delinearon el rumbo de la investigación. En primer lugar, se formuló que la heterogeneidad en los lineamientos para evaluar la evidencia electrónica, entre los marcos regulatorios de US GAAP y NIIF, introduce obstáculos críticos en la auditoría internacional, dificultando en particular la identificación de fraudes contables. Además, se propuso que estas normativas abordan de manera dispar la calidad de dicha evidencia, afectando tanto la uniformidad como la eficiencia de las auditorías en un contexto global. El análisis incluyó un estudio comparativo basado en normativas clave, como la ISA 500, la SAS 142 y la AS 1105. Este enfoque se complementó con la evaluación de casos emblemáticos de fraudes financieros. Así, se buscó identificar cómo las diferencias normativas afectan, de manera concreta, el desempeño profesional en la práctica de auditoría en entornos digitales.

Los resultados obtenidos en este estudio permiten confirmar parcialmente la primera hipótesis y valida por completo la segunda.

La primera hipótesis confirmó parcialmente que las divergencias en los lineamientos sobre evidencia electrónica entre US GAAP y NIIF generan importantes retos en la auditoría internacional, aunque ciertos principios compartidos mitigan parcialmente estas dificultades. Sin embargo, estos desafíos se amortiguan parcialmente debido a ciertos principios generales que ambas normativas comparten; el estudio subrayó que la falta de uniformidad en los criterios aplicados para valorar la suficiencia y la adecuación de la evidencia electrónica complica la ejecución de auditorías consistentes en un entorno globalizado, particularmente en organizaciones con operaciones transnacionales que deben cumplir regulaciones diversas. Aun así, los principios fundamentales relacionados con la relevancia y fiabilidad de la evidencia ofrecen una base común que, en algunos casos, facilita la superación de estas limitaciones.

Respecto a la segunda hipótesis, los hallazgos la corroboran de manera integral. Las diferencias en el tratamiento de la calidad de la evidencia electrónica entre US GAAP y NIIF tienen un impacto directo en la consistencia y eficacia de las auditorías. En primer lugar, se evidenció una mayor confianza otorgada por US GAAP a las fuentes externas en contraste con el enfoque más equilibrado de las NIIF, que consideran tanto fuentes



internas como externas. En segundo lugar, los estudios de casos, como los fraudes de Madoff y Theranos, demostraron cómo estas diferencias normativas generaron inconsistencias en la interpretación y aplicación de la evidencia electrónica dentro de auditorías internacionales.

Asimismo, el análisis reveló que la falta de directrices uniformes sobre herramientas tecnológicas y prácticas de análisis forense digital amplifica las dificultades para la detección temprana de irregularidades. El uso limitado de tecnología y las discrepancias en los requerimientos de documentación y validación de la evidencia electrónica entre ambos marcos regulatorios representan obstáculos críticos para establecer estándares efectivos a nivel global.

Los resultados subrayan la necesidad de avanzar hacia una mayor armonización entre US GAAP y NIIF con el fin de fortalecer la eficacia y consistencia de las auditorías internacionales y facilitar la identificación oportuna de fraudes en un entorno globalizado.

En este estudio se planteó que las diferencias entre US GAAP y NIIF en los requerimientos y la calidad de la evidencia electrónica generan desafíos para la auditoría internacional, especialmente en la detección de fraudes contables y en la consistencia de las prácticas globales. Como líneas de investigación futura, la primera propuesta sugiere evaluar el impacto de la capacitación del auditor en la adopción de tecnología. Se analizaría cómo la formación en herramientas digitales, como análisis de datos, inteligencia artificial y sistemas automatizados, influye en la calidad de la evidencia auditada. Identificar brechas en competencias facilitaría el diseño de programas de capacitación que optimicen la adaptación del auditor al entorno digital, mejorando su desempeño en la detección y prevención de fraudes contables. La segunda línea plantea un análisis de las implicaciones regulatorias en la auditoría de criptoactivos y Blockchain. A partir del caso FTX Exchange, resulta crucial desarrollar marcos normativos robustos que permitan auditorías efectivas en entornos descentralizados, abordando su complejidad y ausencia de controles tradicionales para garantizar mayor transparencia y seguridad en operaciones con criptomonedas. Se propone ahondar en el análisis de lo puntualizado en futuras investigaciones para ampliar y complementar el análisis.



Referencias bibliográficas

- AICPA. (2020). *SAS No. 142, Audit Evidence*. (A. I. Accountants, Ed.) New York: American Institute of Certified Public Accountants. Retrieved from <https://www.aicpa-cima.com/resources/download/audit-evidence-sas-142>
- Allen, R. D., Gramling, A. A., & Hermanson, D. R. (2023, December). Thinking Like an Auditor: Evaluating Information to Arrive at Evidence-Based Conclusions. *Accounting horizons*, 37(4), 1-8. doi:<https://doi.org/10.2308/HORIZONS-2022-182>
- Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017, November). Big Data and Analytics in the Modern Audit Engagement: Research Needs. *Auditing: a journal of practice & theory*, 36(4), 1-27. doi:<https://doi.org/10.2308/ajpt-51684>
- BBVA. (n.d.). *¿Cómo funciona un esquema Ponzi?* Retrieved from BBVA: <https://www.bbva.com/es/economia-y-finanzas/como-funciona-un-sistema-ponzi-conocelo-para-protegerlo/>
- Bermúdez, Á. (2019, 01 19). *La rocambolesca vida de Carlo Ponzi, el negociante italiano que inventó la estafa piramidal*. Retrieved from BBC news mundo: <https://www.bbc.com/mundo/noticias-46909825>
- Boland, C. M., Caster, P., Elder, R. J., & Janvrin, D. (2023). Comments by the Ad Hoc Task Force of the Auditing Standards Committee of the Auditing Section of the American Accounting Association on the Proposed Auditing Standard. *Current issues in auditing*, 17(2), C1-C13. doi:<https://doi.org/10.2308/CIIA-2023-006>
- Boland, C. M., Hermanson, D. R., Higgs, J. L., Pyzoha, J. S., & Zhang, Y. (2024). Comments of the Auditing Standards Committee of the Auditing Section of the American Accounting Association on the PCAOB's Proposed Amendments Related to Aspects of Designing and Performing Audit Procedures That Involve Technology-Assisted Analysis of Inf. *Current issues in auditing*, 18(1), C27-C37. doi:<https://doi.org/10.2308/CIIA-2023-019>
- Bundy, J., & Ndu, I. (2023). An analytical view on the Theranos fraud and the way forward - an accounting perspective. *International Journal of Business and Management*, 18(1), 100-107. doi:[doi:10.5539/ijbm.v18n1p100](https://doi.org/10.5539/ijbm.v18n1p100)
- Cambaza, E. M. (2024). Theranos: the ethics of innovation and deception in healthcare technology. *REVES - Revista Relaciones Sociais*, 07(02), 1-21. doi:[10.18540/revesv17iss2pp19792](https://doi.org/10.18540/revesv17iss2pp19792)
- Carreyrou, J. (2018). *Bad Blood: Secrets and Lies in a Silicon Valley Startup* (First Edition ed.). New York: Alfred A. Knoff.
- Chen, J. (2024, June 10). *Ponzi Scheme: Definition, Examples, and Origins*. Retrieved from Investopedia: <https://www.investopedia.com/terms/p/ponziscHEME.asp>



- Cheong, A., Duan, H. K., Huang, Q., Vasarhelyi, M. A., & Zhang, C. A. (2022). The rise of accounting: making accounting information relevant again with exogenous data. *Journal of emerging technologies in accounting*, 19(1), 1-20.
doi:10.2308/jeta-10812
- Choo, F., & Tan, K. B. (2022). Cash Theft Investigation and Evidence Documentation. (A. A. Association, Ed.) *Journal of forensic accounting research*, 7(1), 1-15.
doi:https://doi.org/10.2308/JFAR-2019-507
- Conlon, T., Corbet, S., & Hu, Y. (2023, November 11). The collapse of the FTX exchange: The end of cryptocurrency's age of innocence. (B. A. Association, Ed.) *The British accounting review*, 1-13.
doi:https://doi.org/10.1016/j.bar.2023.101277
- Crypto crash: why the FTX bubble burst and the harm to consumers, S. HRG. 117–757 (United States Senate December 14, 2022). Retrieved from
<https://www.govinfo.gov/content/pkg/CHRG-117shrg53797/pdf/CHRG-117shrg53797.pdf>
- Dai, Y., & Handley-Schachler, M. (2015). A Fundamental Weakness in Auditing: The Need for a Conspiracy Theory. *7th International Conference on Financial Criminology 2015* (pp. 1-6). Oxford: Wadham College.
doi:https://doi.org/10.1016/S2212-5671(15)01074-6
- Das, R. K., & Drolet, B. C. (2022). Lessons from Theranos – Restructuring Biomedical Innovation. *Journal of Medical Systems*, 24-25.
doi:https://doi.org/10.1007/s10916-022-01813-3
- Disclosure Statement for Debtors' Joint Chapter 11 Plan of Reorganization of FTX Trading Ltd. and its Affiliated Debtors and Debtors-in-Possession, 22-11068 (JTD) (United States Bankruptcy Court for the District of Delaware June 27, 2024).
- Dupuis, D., Smith, D., Gleason, K., & Kannan, Y. (2023). Bitcoing and beyond: crypto asset considerations for auditors/forensic accountants. *Journal of Forensic and Investigative Accounting*, 15(3), 489-510.
- Dutta, S. K., Caplan, D. H., & Marcinko, D. J. (2014). Blurred vision, perilous future: management fraud at Olympus. *Issues in Accounting Education*, 29(3), 459-480.
doi:https://doi.org/10.2308/iace-50787
- Elam, D., Madrigal, M., & Jackson, M. (2014). Olympus imaging fraud scandal: a case study. *American Journal of Business Education*, 7(4), 325-332.
- Elder, R. J., Janvrin, D. J., & Caster, P. (2014). Peregrine—Twenty Years of Fraudulent Cash Balances. *ISSUES IN ACCOUNTING EDUCATION*, 29(2), 337-348.
doi:https://doi.org/10.2308/iace-50690



- Esparcia, C., Escribano, A., & Jareño, F. (2024). Assessing the crypto market stability after the FTX collapse: A study of high frequency volatility and connectedness. *International Review of Financial Analysis*, 94, 1-14.
doi:<https://doi.org/10.1016/j.irfa.2024.103287>
- EY. (2022). *Crypto derivatives are becoming a major digital asset class*. Ernst & Young LLP. Retrieved from https://www.ey.com/content/dam/ey-unified-site/ey-com/en-us/insights/financial-services/documents/ey-crypto-derivatives-pov_final4.pdf
- Frendy, & Dan, H. (2012). Japanese stock market reaction to the announcements of news affecting auditors' reputation: The case of Olympus fraud. *Nagoya University*.
- FTX Cryptocurrency Exchange Collapse Litigation, 23-md-03076-KMM (UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF FLORIDA 08 08, 2023).
- Fu, S., Wang, Q., Yu, J., & Chen, S. (2022). *FTX Collapse: A Ponzi Story*. Cornell University. doi:<https://doi.org/10.48550/arXiv.2212.09436>
- Fukukawa, H., Mock, T. J., & Srivastava, R. P. (2014). Assessing the Risk of Fraud at Olympus and Identifying an Effective Audit Plan. *The Japanese Accounting Review*, 1-25. doi:10.11640/tjar.4.2014.01
- Hossain, U. (2021). *An Analysis of Madoff Investment Securities: How The Biggest Financial Scam Took Place and The Failure of Assurance Services*. Dhaka: University of Dhaka. Retrieved from <https://ssrn.com/abstract=4365065>
- IAASB. (2021). *International Standard on Auditing 500 Audit Evidence (Vol. I)*. (I. A. Board, Ed.) New York: International Federation of Accountants. Retrieved from https://www.iaasb.org/_flysystem/azure-private/publications/files/IAASB-2021-Handbook-Volume-1.pdf
- IIA. (2023). *Global Perspectives & Insights*. Lake Mary: The Institute of Internal Auditors, Inc. Retrieved from <https://www.theiia.org/en/content/articles/global-perspectives-and-insights/2023/global-perspectives--insights-fraud/>
- Infobae. (2022, Febrero 24). *Llegó a Estados Unidos con menos de tres dólares y murió pobre en Brasil: Ponzi, el italiano que creó la estafa piramidal*. Retrieved from Infobae: Historias: <https://www.infobae.com/historias/2022/02/24/llego-a-estados-unidos-con-menos-de-tres-dolares-y-murio-pobre-en-brasil-ponzi-el-italiano-que-creo-la-estafa-piramidal/>
- Integrity Line. (2023, 11 22). *Elizabeth Holmes and the Theranos Case: History of a Fraud Scandal*. Retrieved 09 12, 2024, from Integrity Line: <https://www.integrityline.com/expertise/blog/elizabeth-holmes-theranos/>



- Jeske, M. (2020). Lessos from Theranos: changing narratives of individual ethics in science and engineering. *Engaging Science, Technology, and Society*, 6, 306-311. doi:DOI:10.17351/ests2020.411
- Mackenzie, S. (2024). Crypto collapse: the cult of personality and the normalization of fraud in FTX and Celsius. *Journal of Financial Crime*, ahead-of-print(ahead-of-print). doi:http://dx.doi.org/10.1108/JFC-01-2024-0054
- Manda, V. K., & Yadav, A. (2023). The aftermath of the FTX cryptocurrency exchange collapse. 104-109. Retrieved from <https://www.researchgate.net/publication/375923823>
- Miller, T. C., Cipriano, M., & Ramsay, R. J. (2012). Do auditors assess inherent risk as if there are no controls? *Managerial Auditing Journal*, 27(5), 448-461. doi:https://doi.org/10.1108/02686901211227931
- Morgan, A. R., & Burnside, C. (2014). Olympus Corporation Financial Statement Fraud Case Study: The Role That National Culture Plays On Detecting And Deterring Fraud. *Journal of Business Case Studies*, 10(2), 175-184. doi:10.19030/JBCS.V10I2.8506
- Office of Investigations. (2009). *Investigation of failure of the SEC to uncover Bernard Madoff's Ponzi scheme - Public Version* -. U.S. Securities and Exchange Commission.
- PCAOB. (2023). *AS 1105: Audit Evidence*. Retrieved from Public Company Accounting Oversight Board: <https://pcaobus.org/oversight/standards/auditing-standards/details/AS1105>
- Peterson, P. (2014). *Peregrine Financial Group: Two Years and Counting*. farmdocDAILY, Department of Agricultural and Consumer Economics. Illinois: University of Illinois Urbana-Champaign. Retrieved 9 25, 2024, from <http://farmdocdaily.illinois.edu/2014/07/peregrine-financial-group-two-years-and-counting.html>
- Ragothaman, S. C. (2014). The Madoff Debacle: What are the Lessons? *ISSUES IN ACCOUNTING EDUCATION*, 29(1), 271-285. doi:https://doi.org/10.2308/iace-50597
- Rogal, L. (2021, August). Secrets, lies, and lessons from the Theranos scandal. *Hastings Law Journal*, 72(7), 1663-1702.
- Roy, D., Anand, P., & Chandra, S. (2022). FTX Collapse: The chronicle and the implications. *NIBM Explainer*(2), 1-6.
- Sala, A. (2022, octubre 20). *Charles Ponzi, la gran estafa americana*. Retrieved from Historia National Geographic:



https://historia.nationalgeographic.com.es/a/charles-ponzi-gran-estafa-americana_16669

- Snachez, M. H., & Dunne, K. (2017). An Empire Built on a Lie – the Peregrine Fraud: A Case Study on Confirmations as Audit Evidence. *Review of Business & Finance Studies*, 8(1), 49-55. Retrieved from <https://ssrn.com/abstract=3028301>
- Trautman, L. J., & Foster II, L. D. (2023). The FTX crypto debacle: Largest fraud since Madoff? *The University of Memphis Law Review*, 54, 289-373.
- United States Attorney's Office. (2022). *U.S. v. Elizabeth Holmes, et al.* Northern District of California: United States Attorney's Office. Retrieved from <https://www.justice.gov/usao-ndca/us-v-elizabeth-holmes-et-al>
- United States Bankruptcy Court for the Northern District of Illinois. (2014). *Trustee's Status Report of September 29, 2014*. Illinois: Illinois State. Retrieved 09 30, 2024, from <https://digitalprairie.ok.gov/digital/api/collection/p16807coll4/id/15177/download>
- Verschoor, C. C. (2012, February). Olympus Scandal Shows Need for U.S. Standards. *Strategir Finance*, 13-15,61. Retrieved 9 22, 2024, from https://sfmagazine.com/~media/sfmag/legacy-site/_historic/2012/02/ethicsolympusscandalshowsneedforusstandards.pdf
- Vinod, H. D. (2009). *Preventing Madoff-style Ponzi enabled by Jewish Reputation, Incompetent Regulators and Auditors*. Bronx: Fordham University. Retrieved from <https://ssrn.com/abstract=1320069>



Siglas y Acrónimos

AICPA: American Institute of Certified Public Accountants (Instituto Americano de Contadores Públicos Certificados)

AS: Auditing Standards (Estándar de Auditoría).

AS 1105: Auditoría sobre la calidad y cantidad de la evidencia.

ASB: Auditing Standards Board (Junta de Normas de Auditoría del Instituto Americano de Contadores Públicos Certificados)

BLMIS: Bernard L. Madoff Investment Securities.

CAATs: Computer-Assisted Audit Techniques (Técnicas de Auditoría Asistidas por Computadora).

CEO: Chief Executive Officer (Director Ejecutivo o Director General)

CFTC: Commodity Futures Trading Commission (Comisión de Comercio de Futuros de Productos Básicos).

CMS: Centers for Medicare & Medicaid Services (Centro de Servicios de Medicare y Medicaid).

DTC: Depository Trust Company (Empresa de custodia y liquidación de valores en EE.UU.).

DTCC: Depository Trust & Clearing Corporation (Corporación de Depósito y Liquidación de Valores)

ERP: Enterprise Resource Planning (Planificación de Recursos Empresariales).

EY: Ernst & Young.

FASB: Financial Accounting Standards Board (Consejo de Normas de Contabilidad Financiera de EE.UU.).

FDA: Food and Drug Administration (Administración de Alimentos y Medicamentos de Estados Unidos).

FTX: Futures Exchange (Intercambio de Futuros).

IA: Inteligencia Artificial.

IAASB: International Auditing and Assurance Standards Board (Consejo de Normas Internacionales de Auditoría y Aseguramiento)

IASB: International Accounting Standards Board (Consejo de Normas Internacionales de Contabilidad).



IFAC: International Federation of Accountants (Federación Internacional de Contadores)

IIA: Institute of Internal Auditors (Instituto de Auditores Internos)

IoT: Internet of Things (Internet de las Cosas).

ISA: International Standards on Auditing.

ISA 500: International Standard on Auditing 500, Norma sobre evidencia de auditoría.

KPMG: Klynveld Peat Marwick Goerdeler

KYC: Know Your Customer (Conoce a tu cliente)

NFA: National Futures Association (Asociación Nacional de Futuros en EE.UU.).

NASDAQ: National Association of Securities Dealers Automated Quotations.

NFA: National Futures Association (Asociación Nacional de Futuros).

NIIF: Normas Internacionales de Información Financiera.

NSCC: National Securities Clearing Corporation (Corporación Nacional de Compensación de Valores)

NYSE: New York Stock Exchange.

OIG: Office of Inspector General (Oficina del Inspector General).

PCAOB: Public Company Accounting Oversight Board (Consejo de Supervisión Contable de Empresas Públicas).

PFG: Peregrine Financial Group.

PwC: PricewaterhouseCoopers.

SAS: Statements on Auditing Standards.

SAS 142: Statement on Auditing Standards, Norma sobre fiabilidad de la evidencia de auditoría.

SBF: Sam Bankman-Fried

SEC: Comisión de Valores de EE. UU.

SPV: Special Purpose Vehicle (Vehículo de Propósito Especial).

US GAAP: Generally Accepted Accounting Principles (Principios de Contabilidad Generalmente Aceptados en EE.UU.).



Anexo I: El esquema ponzi y la figura de Carlo Ponzi

El esquema Ponzi, aún vigente como una de las estafas financieras más comunes, recibe su nombre de Carlo Ponzi. Este inmigrante italiano, quien llegó a los EE. UU. en 1903, explotó un sistema a una escala impresionante. ¿Por qué entonces su nombre se convirtió en sinónimo de este fraude y no el de otro de su tiempo? La explicación es directa: él fue quien llevó esta práctica al extremo, aunque su prestigio se desplomara tras el colapso de su artimaña. (Bermúdez, 2019)

La estructura de un esquema Ponzi consiste en usar el capital de los nuevos inversores para remunerar a los anteriores, generando una falsa percepción de ganancias. Aunque aparente ser un negocio rentable, en realidad es un artificio vacío, pues no existe una inversión subyacente real. (Chen, 2024)

Esta falta de inversión productiva convierte al esquema en insostenible a largo plazo. ¿Se puede identificar fácilmente cuando uno está involucrado en un esquema Ponzi? Lamentablemente, no siempre es obvio. La promesa de rendimientos elevados, en plazos cortos, en un escenario económico incierto, es algo que, en principio, parece suficientemente persuasivo. No solo a inversores sofisticados, sino a cualquier persona (BBVA, s.f.) ¿Quién no caería? Ponzi, valiéndose de un supuesto diferencial de precios en cupones de respuesta internacional, sostenía que era posible comprarlos en países con monedas débiles para luego venderlos en Estados Unidos a precios considerablemente mayores. A simple vista, una lógica impecable. Sin embargo, el mercado real de estos cupones era, ¿sostenible? No, era demasiado pequeño e inviable para garantizar esos rendimientos masivos que prometía (Chen, 2024) El tamaño del esquema se multiplicaba exponencialmente, más inversores llegaban, más convencidos estaban por esos pagos iniciales que parecían confirmar la viabilidad del negocio. En realidad, esos pagos no provenían de las utilidades de los cupones, el capital de los nuevos inversores era lo que financiaba el ciclo. ¿Es sostenible un esquema basado en deuda interna constante? Pregunta sin respuesta fácil. Uno de los elementos más asombrosos fue la velocidad. ¿Cuántos, en menos de ocho meses, han pasado de ser unos completos desconocidos a ser considerados magnates financieros? Ponzi lo hizo en Boston, pero ¿por qué nadie lo detectó? La falta de regulaciones específicas, combinada con la confianza irracional, actuó como un escudo. No existían mecanismos claros, que



podieran fiscalizar estos movimientos financieros en su momento (Sala, 2022). Además, su carisma. ¿Qué tan potente puede ser una personalidad carismática? Esa retórica seductora que logró captar miles de inversores: desde ciudadanos corrientes hasta miembros destacados de la sociedad, manipulaba con maestría (Infobae, 2022). Se presentó como una solución en tiempos de crisis. Una promesa, pero ¿qué sucede cuando la realidad es diametralmente opuesta a la promesa? (Sala, 2022) lo subraya, finalmente, es curioso, Ponzi no inventó este mecanismo, ya existían otros fraudes similares en Europa, aunque nunca de esta magnitud. ¿Fue él un innovador o simplemente un oportunista?

Es interesante notar que Ponzi no inventó este tipo de esquema, pero sí fue el que lo popularizó. Antes de él, se habían utilizado mecanismos similares en Europa, aunque nunca a la escala que Ponzi logró alcanzar (Sala, 2022). Su fraude sirvió como lección para la creación de futuras leyes de regulación financiera, y hoy en día, muchas legislaciones consideran este tipo de prácticas como un delito grave.



Anexo II: Propuesta de un marco regulatorio para criptomonedas según Jennifer J. Schulp

En su testimonio ante el Senado, Jennifer J. Schulp subrayó la urgencia de un marco regulatorio diseñado exclusivamente para criptomonedas. Propone que las particularidades de estos activos digitales se reconozcan. No deberían ser forzadas dentro de normativas ya existentes, pensadas para productos financieros convencionales como valores y títulos. Su análisis es pertinente, en especial al considerar el caso FTX, que evidencia cómo la falta de un marco diferenciado favoreció el colapso de la plataforma.

Un punto clave en la propuesta de Schulp es separar entidades centralizadas de proyectos descentralizados. Destaca que intermediarios centralizados como FTX actúan de manera similar a bancos o corredores de bolsa, gestionando activos de clientes. Por ello, necesitan regulación específica que incluya custodia de activos, transparencia y gestión de riesgos. Schulp subraya que "FTX es un intermediario tradicional centralizado", debiendo haberse sometido a regulaciones como otros intermediarios financieros. Sin embargo, la falta de normativas específicas permitió operaciones riesgosas sin supervisión.

En contraste, los proyectos descentralizados o DeFi funcionan sin un control central, registrando transacciones en blockchain y permitiendo a los usuarios custodiar sus activos. Para Schulp, aplicar ciegamente las normativas de entidades centralizadas sería no solo ineficaz, sino perjudicial para la innovación.

Schulp plantea que la regulación de criptomonedas debe considerar los riesgos de cada tipo de entidad. Las plataformas centralizadas, como FTX, deberían registrarse y seguir las normativas de intermediarios financieros tradicionales. Esto aseguraría la protección de activos y la transparencia, evitando transacciones no autorizadas y el uso indebido de fondos.

Por otro lado, los proyectos descentralizados podrían tener la opción de registrarse para acceder a ciertos mercados. Dado que la tecnología blockchain reduce la intermediación, estos proyectos enfrentan menos riesgos de custodia de activos.

Otro aspecto crucial es la claridad en la definición de los criptoactivos. Schulp señala que, aunque algunos activos podrían parecerse a valores tradicionales (según el Howey

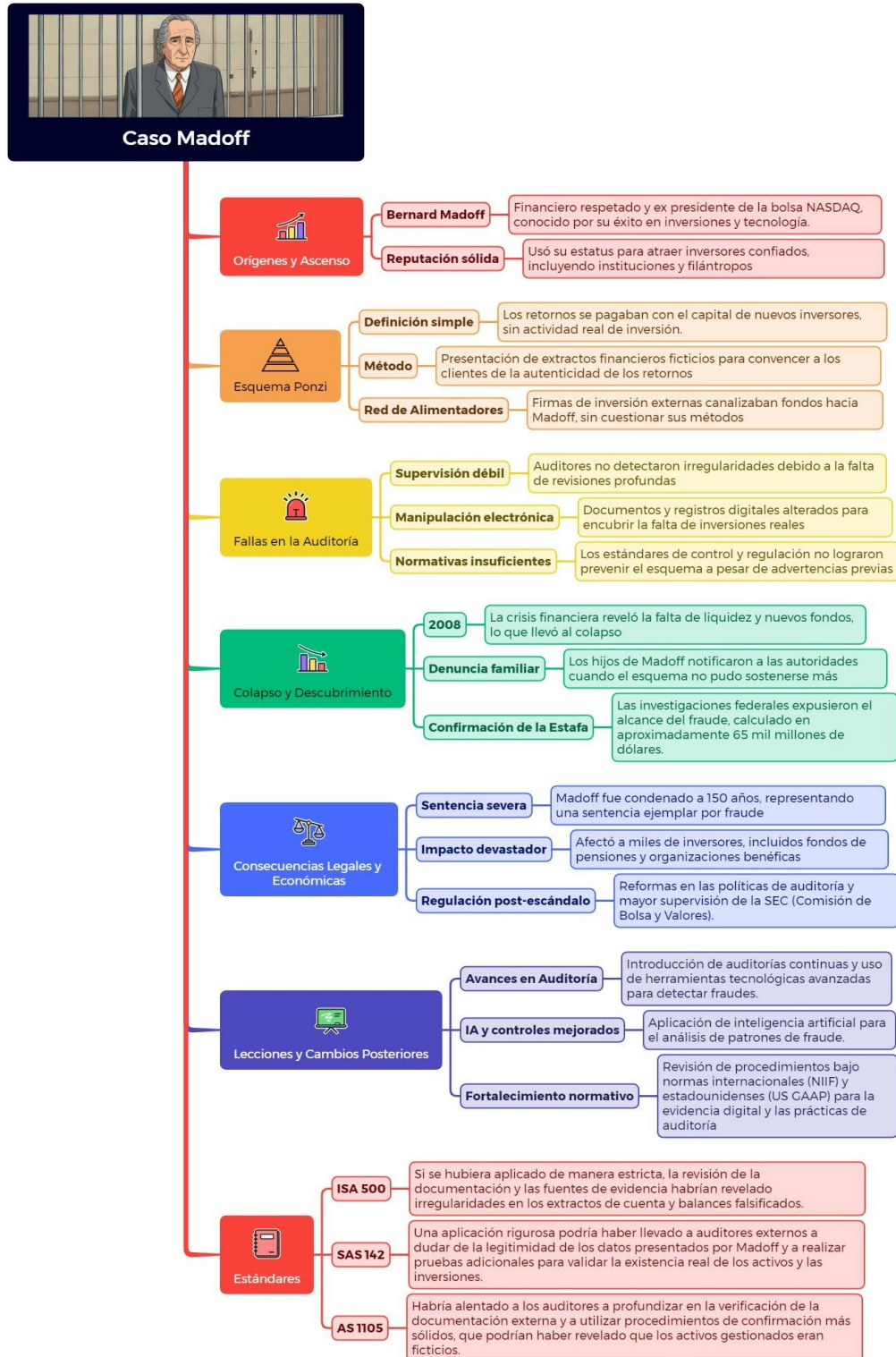


Test), no todos deberían regirse por las mismas leyes. Para aquellos sin un gerente o entidad central, la regulación de valores no es aplicable.

Schulp reconoce que los proyectos descentralizados podrían beneficiarse de un marco de divulgación simplificado, para que los inversores puedan tomar decisiones informadas sin perder la transparencia. Un sistema de divulgación voluntario sería ideal para evaluar riesgos, sin frenar la innovación con regulaciones rígidas.

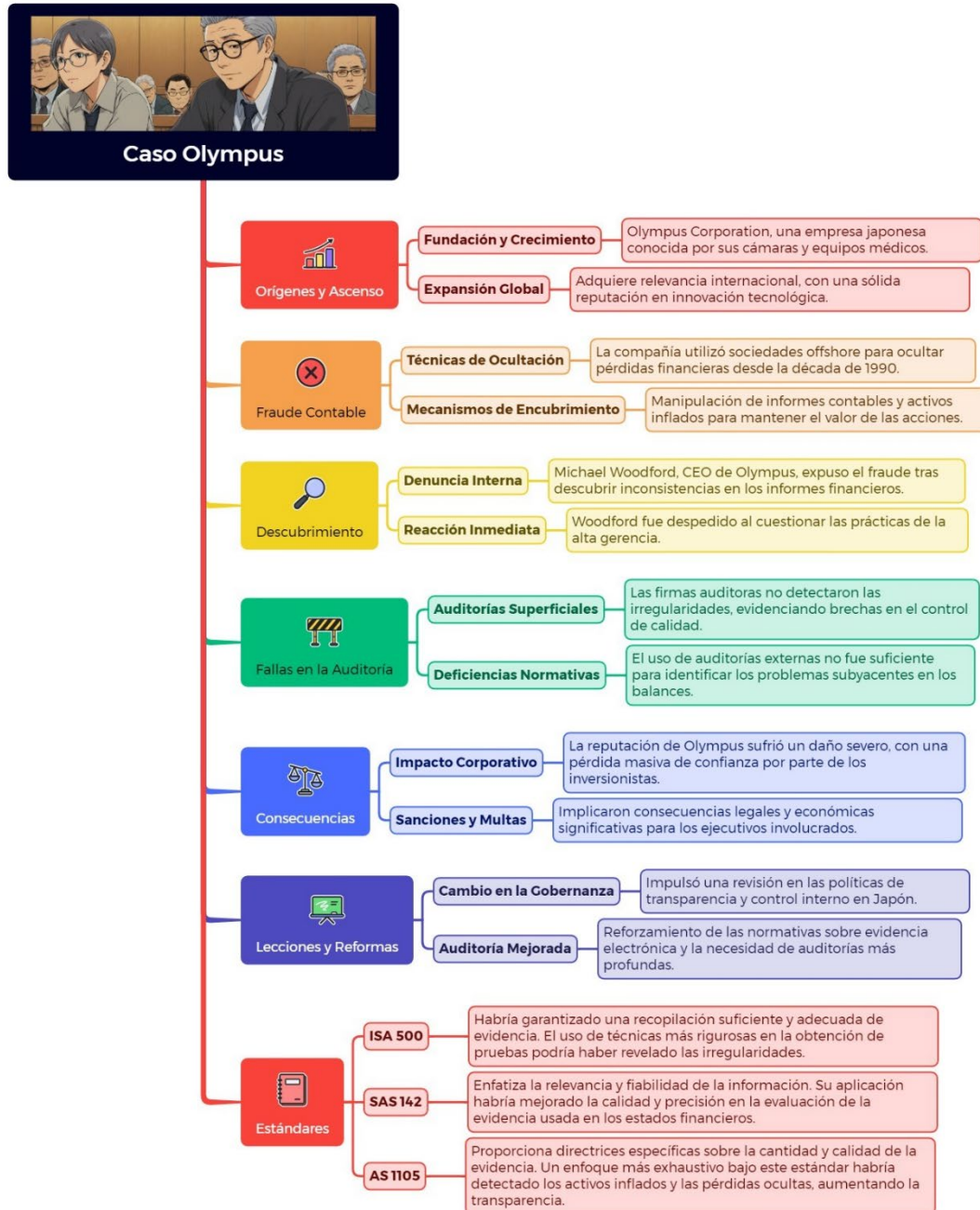
Schulp propone un enfoque regulatorio que debe adaptarse, asegurando la protección de los consumidores mientras se promueve la innovación. Un marco regulatorio balanceado facilitaría la incorporación segura de las criptomonedas al sistema financiero global.

Anexo III: caso Madoff – mapa mental



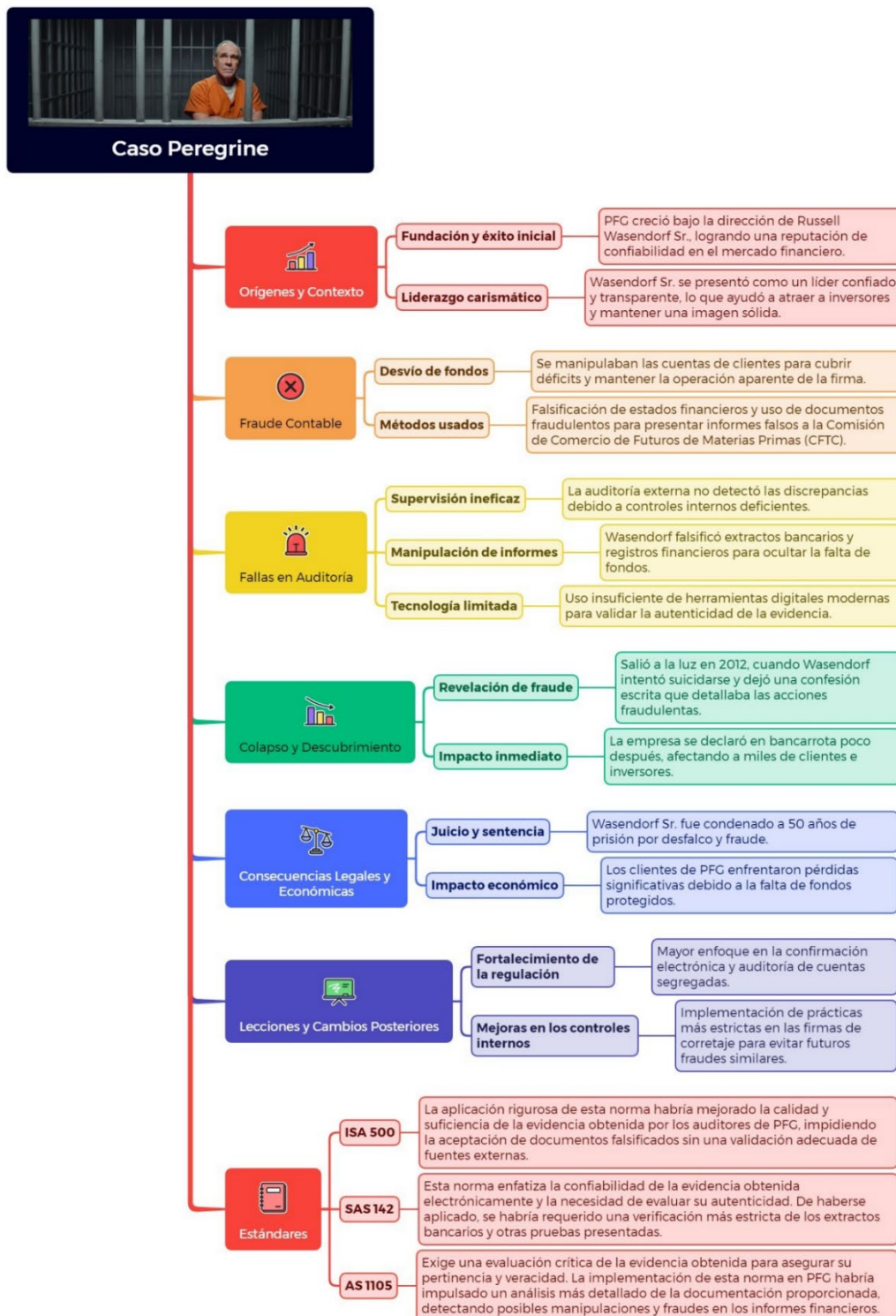
Fuente: Elaboración propia

Anexo IV: caso Olympus – mapa mental



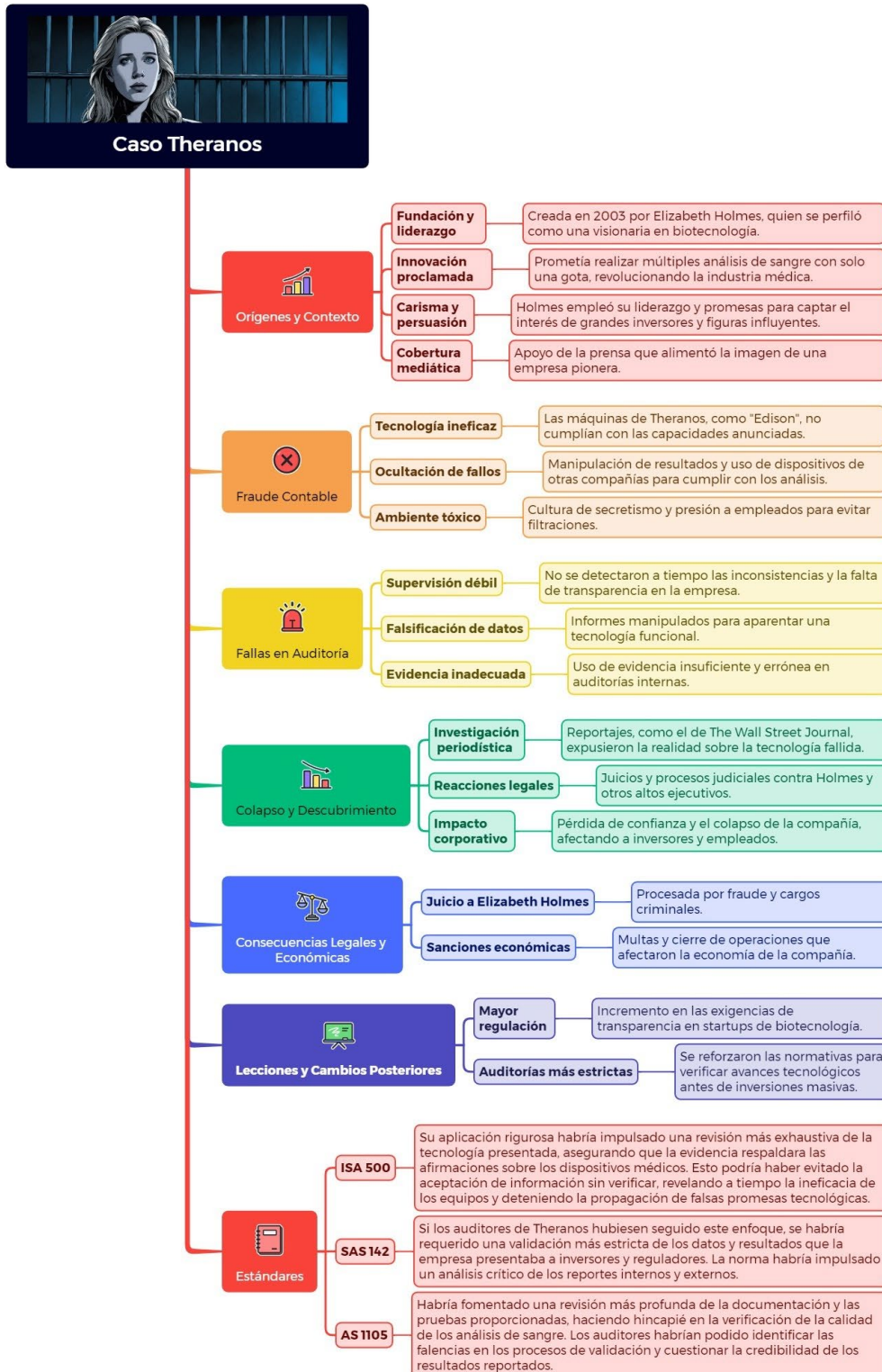
Fuente: Elaboración propia

Anexo V: caso Peregrine – mapa mental



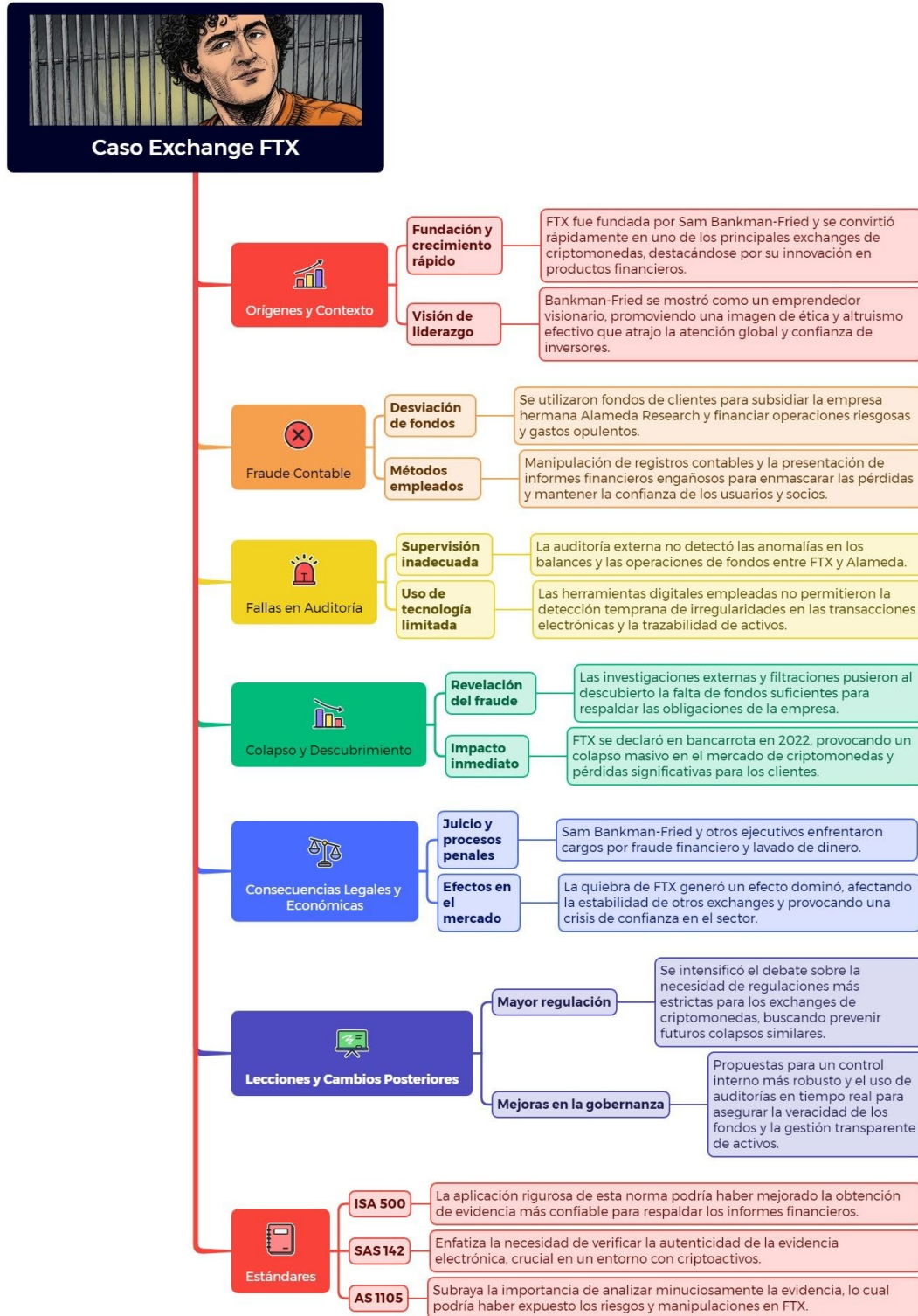
Fuente: Elaboración propia

Anexo VI: caso Theranos – mapa mental



Fuente: Elaboración propia

Anexo VII: caso Exchange FTX – mapa mental



Fuente: Elaboración propia