Facultad de Ciencias Económicas | UNIVERSIDAD NACIONAL DE LA PLATA

CECIN
Centro de Estudios en Contabilidad Internacional

“Visualizando lo invisible: Dashboards de datos para prevenir el Lavado de Activos”

Candela S. Caprarulo
Alejandro A. Barbei

Documento de trabajo Nro. 082
Diciembre, 2024

ISSN 2545-7896

Visualizando lo invisible: Dashboards de datos para prevenir el Lavado de Activos*

Candela S. Caprarulo
Alejandro A. Barbei

Universidad Nacional de La Plata

Diciembre, 2024

* Trabajo presentado en el 20° Simposio Regional de Investigación Contable. La Plata, Buenos Aires, Argentina.

RESUMEN

Mediante una revisión no sistemática de la literatura, este trabajo de investigación se centra en explorar la aplicación de la herramienta de Visualización de Datos en el contexto de la prevención del lavado de activos de origen delictivo y financiación del terrorismo.

Se investiga cómo esta herramienta tecnológica puede optimizar los procedimientos de auditoría, proporcionando una mejor comprensión de los datos y permitiendo una detección más precisa de posibles irregularidades. Este estudio brinda una visión de cómo la herramienta de Data Visualization puede revolucionar la práctica de la auditoría contable y mejorar la calidad de la información para los usuarios interesados en tomar decisiones.

PALABRAS CLAVE: Visualización de datos; Lavado de activos; Auditoría.

1. INTRODUCCIÓN

Tal como mencionan los autores Singh y Best (2019), anualmente las actividades de lavado de dinero amenazan la economía global, ya que los ingresos de estas pueden utilizarse para financiar otras actividades delictivas y socavar la integridad de los sistemas financieros en todo el mundo, es por ello que se reconocen como un riesgo crítico en muchos países. Además, debido a la gran cantidad de transacciones que ocurren diariamente en el sistema financiero, encontrar casos específicos de operaciones ilícitas se convierte en una tarea no trivial (LópezRojas y Axelsson, 2012).

Por otro lado, es importante remarcar que las instituciones financieras se enfrentan a un desafío constante en la prevención del lavado de dinero de origen delictivo y financiación del terrorismo debido a la sofisticación de las técnicas delictivas y al volumen de las transacciones. Los métodos tradicionales basados en reglas suelen generar una alta tasa de falsos positivos, lo que incrementa significativamente los costos operativos al requerir una mayor inversión en la investigación de dichas alertas. La calidad de los datos subyacentes también influye en la generación de falsos positivos, afectando la eficiencia y eficacia de los sistemas de monitoreo. Esta situación obliga a las instituciones a buscar soluciones innovadoras que permitan optimizar sus procesos de detección y reducir el impacto de las alertas falsas (Oztas, et al. 2024; Pontes, et. al 2022).

Otro problema que resulta relevante es que la información proveniente del Know your customer (KYC) o “conozca a su cliente” a menudo está desactualizada e inexacta, lo que lleva a alertar en exceso o en defecto a individuos específicos. Esto afecta negativamente al proceso de segmentación de clientes y reduce la precisión del proceso general. Además, los departamentos o áreas que se encargan de las tareas tendientes a la prevención del lavado de dinero, deberían estar integradas en el monitoreo de las transacciones y trabajar juntos, no de forma aislada. Es por esta razón que los datos son un desafío para las instituciones y existe la necesidad de una única fuente de datos internos de los clientes que proporcione información precisa y actualizada sobre los mismos. Tal como comenta Oztas, et. (2024), el hecho de que los bancos a menudo tengan múltiples fuentes de datos de varios departamentos y productos se suma al problema de la falta de una fuente única de datos.

Dado el cambio constante en las regulaciones y normativas sobre la prevención del lavado de activos con origen en operación ilícitas, junto con casos recientes de este tipo de actividades por parte de algunas de las instituciones financieras más grandes, se ha puesto de relieve la necesidad de una mejor tecnología en la gestión de prevención de las mismas. De hecho, se considera que las soluciones tecnológicas eficaces son un elemento esencial en el blanqueo de capitales, ya que los datos y los análisis mejorados son claves para ayudar

a los profesionales a centrarse en actividades sospechosas. Actualmente, existe un interés emergente tanto por parte de investigadores como de profesionales, en relación con el uso de herramientas de software para mejorar la detección de actividades provenientes de lavado de dinero (Singh y Best, 2019).

En este sentido, el presente trabajo de investigación explora el potencial de las herramientas tecnológicas de análisis y visualización de datos para complementar los procesos de auditoría contable y fortalecer la lucha contra el lavado de dinero. Al combinar datos contables con otras fuentes de información, se busca identificar nuevas tendencias y patrones que puedan indicar actividades ilícitas.

2. OBJETIVO GENERAL

El objetivo general de esta investigación es analizar la utilidad de las herramientas tecnológicas de los dashboards, o tableros de visualización de datos, para detectar operaciones inusuales y sospechosas relacionadas con el lavado de activos de origen delictivo y financiación del terrorismo. Se explora cómo estas herramientas ayudan a los auditores contables, al momento de llevar a cabo su trabajo, y presentar mejor la información a los usuarios finales, para que les sea de utilidad al momento de tomar decisiones.

3. OBJETIVOS ESPECÍFICOS

1. Explorar la importancia de los dashboards de visualización de datos en la auditoría contable, específicamente en la prevención del lavado de activos.

2. Descubrir las características esenciales de un tablero de visualización de datos eficaz para detectar operaciones inusuales y sospechosas.

4. METODOLOGÍA

Para poder avanzar con los objetivos específicos de la presente investigación, se realiza una revisión no sistemática de la literatura sobre la utilidad de los dashbords o tableros de visualización de datos aplicados a la detección de operaciones inusuales y sospechosas sobre el lavado de activos de origen delictivo y financiación del terrorismo. En consecuencia, siguiendo las pautas de las Técnicas de Investigación Social propuestas por Bravo, R.S. (2001) podemos afirmar que, de acuerdo con los objetivos de esta investigación, esta se

clasifica como aplicada; en términos de su duración, es de naturaleza seccional; en relación con su enfoque, se caracteriza como exploratoria; en lo que respecta a su alcance, se enfoca en la microsociología; y en cuanto a las fuentes utilizadas, se basa en datos secundarios derivados de la revisión de la literatura.

5. DESARROLLO

5.1. Operaciones inusuales y sospechosas – Lavado de Activos

Teniendo en consideración que en esta investigación se busca explorar el uso de la visualización de datos en la prevención de lavado de activos, y descubrir las características esenciales que deberían tener los tableros de visualización para poder detectar operaciones inusuales y sospechosas, se considera necesario, para adentrarse en el tema de esta investigación, brindar una introducción teórica que contenga la definición del lavado de activos, sus etapas, y los organismos de contralor que existen actualmente a nivel global y también a nivel local.

Existen múltiples definiciones para el término de lavado de dinero, una de ellas es la que da Slosse et. (2008), definiéndolo como la simulación de la licitud de activos originados en un hecho ilícito. Por otro lado, la autora Albanese (2012), menciona que este tipo de actividades es la consecuencia de otros accionares delictivos aberrantes, tales como tráfico de armas, de estupefacientes y sustancias psicotrópicas, secuestro de personas, entre otras. El objetivo final es ocultar el verdadero origen del dinero o de los activos para hacerlos circular legalmente en el sistema financiero y económico de un país.

Siguiendo con la introducción teórica, el autor Wainstein (2004) divide a las etapas del proceso del lavado de activos en tres momentos:

1. Colocación: las actividades delictivas previas al lavado de activos generan grandes montos de dinero en efectivo. Ante esta situación, se tratan de transformar sumas voluminosas en activos fáciles de manejar, dividiéndolas en montos pequeños para introducirlos en el circuito económico-financiero legal. De este modo, se busca otorgar apariencia legítima a ingresos provenientes de otros delitos (tráfico de armas, de personas, secuestros, narcotráfico, pedofilia, etc.).

2. Decantación o estratificación: una vez que el dinero ha sido colocado, el objetivo es borrar las evidencias de su origen mediante la realización de reiteradas operaciones, en su mayoría complejas y utilizando diversos instrumentos financieros. Esto es encubrir el origen

ilícito de los recursos mediante operaciones aparentemente lícitas, desviando la atención, dejando evidencias falsas, y presentando documentación apócrifa.

3. Integración: se incorpora el dinero de origen delictivo al circuito económico legal. En esta fase se trata de invertir en negocios con grandes movimientos de efectivo para simular ingresos que en realidad se originan en una actividad ilícita. Es decir que se oculta dinero de origen ilegal y, en actos siguientes, se le otorga apariencia de legítimo.

Ahora bien, teniendo en cuenta que el lavado de activos es un delito complejo y transversal que afecta a diversos sectores de la economía, para poder combatirlo de manera efectiva, se requiere de una respuesta coordinada y multidisciplinaria. En este sentido, el Grupo de Acción Financiera Internacional (GAFI), organismo intergubernamental con sede en París, elaboró un documento con recomendaciones destinadas a promover medidas para combatir el delito y que a su vez constituyen principios de acción que sirven como base a los países para la elaboración de su propia legislación. En Argentina, con la sanción de la ley 25.246 se creó la Unidad de Información Financiera (UIF), organismo autárquico que actúa en jurisdicción del Ministerio de Justicia y Derechos Humanos de la Nación, destinado a elaborar y difundir normas y procedimientos orientados a prevenir el delito. Dicho organismo se encarga de recepcionar las denuncias emanadas de personas físicas o jurídicas designadas por la propia ley como sujetos obligados a reportar operaciones sospechosas. Posteriormente en junio del 2011 se sancionó la Ley 26.683, modificatoria de la Ley 25.246, que otorga al lavado de activos el rango de delito autónomo calificándolo como un delito contra el orden económico y financiero. Diversos organismos de contralor –Banco Central de la República Argentina (BCRA), Consejos Profesionales, Comisión Nacional de Valores, entre otros–, han emitido normas específicas orientando a los entes bajo su control para implementar planes globales de prevención frente al delito, donde es esencial una política integral de conocimiento del cliente (Albanese, 2012). Actualmente, a partir de marzo del año 2024 entró en vigencia en Argentina la Ley 27.739 (cuyo Decreto es el 254/2024) que sustituye e incorpora determinados artículos a la Ley 25.246.

La Ley última mencionada define a las operaciones inusuales como aquellas “operaciones tentadas o realizadas en forma aislada o reiterada, con independencia del monto, que carecen de justificación económica y/o jurídica, y/o no guardan relación con el nivel de riesgo del cliente o su perfil transaccional, y/o que, por su frecuencia, habitualidad, monto, complejidad, naturaleza y/u otras características particulares, se desvían de los usos y costumbres en las prácticas de mercado”. Asimismo define a las operaciones sospechosas como “aquellas tentadas o realizadas que ocasionan sospecha o motivos razonables para sospechar que los bienes o activos involucrados provienen o están vinculados con un ilícito

penal o están relacionados a la financiación del terrorismo, o a el financiamiento de la proliferación de armas de destrucción masiva o que, habiéndose identificado previamente como inusuales, luego del análisis y evaluación realizados por el sujeto obligado, no permitan justificar la inusualidad".

En base a todas estas definiciones, y sin perder de vista el problema que atraviesan actualmente las entidades financieras y el resto de las entidades en cuanto al volumen colosal de las bases de datos que contienen toda la información sobre las diferentes transacciones que realizan los usuarios, resulta imprescindible poder tener un buen sustento del conocimiento de los clientes, es decir, que las entidades deberían armar un correcto "perfil del cliente" que pueda responder a preguntas como: ¿Quién es su cliente? ¿Qué hace? ¿Cuál es su actividad económica? ¿Cuál es su patrimonio? ¿Es justificado? ¿Se cuenta con información suficiente y verificada? (Albanese, 2012); ya que de esta forma se parte de una base sumamente importante para poder procesar la información y proceder luego con las herramientas de visualización de datos. Es importante no perder de vista que toda herramienta tecnológica será de utilidad, siempre y cuando los datos que se carguen en ella sean correctos y seamos capaces de interpretar los resultados arrojados por las mismas.

5.2. Dashboards y su uso en la auditoría externa contable

En el contexto actual, caracterizado por la generación exponencial de los datos, y la necesidad de identificar patrones transaccionales en los mismos, se ha vuelto cada vez más acuciante. La visualización de datos, un término que engloba una variedad de tecnologías diseñadas para representar información de manera visual, ha surgido como una solución eficaz para este desafío (Singh y Best, 2016). La visualización de datos (DV por sus siglas en inglés), es una tecnología que presenta cantidades masivas de datos en formatos gráficos que facilitan al usuario su comprensión. Esta forma de presentación es accesible y permite prescindir de consultas complejas y manipulaciones que requieran mucho tiempo. Con el software de visualización de datos se pueden crear múltiples gráficos, tablas y demás visualizaciones a partir de grandes conjuntos de datos para que los usuarios puedan visualizarlos rápidamente de la manera más eficiente y efectiva. Estas visualizaciones pueden ir cambiando según la información que se combine, permitiendo generar fácilmente nueva información o para analizar los datos de manera diferente (Hoelscher, J., y Mortimer, A. 2018).

Al permitir a los usuarios visualizar y explorar grandes volúmenes de datos de manera intuitiva, estas tecnologías aprovechan la capacidad innata del cerebro humano para comprender información compleja, facilitando así la extracción de conocimientos valiosos y la toma de decisiones basadas en datos. La aplicación innovadora de técnicas de visualización de datos en diversos campos ha cobrado impulso en la última década (Bolton y Hand, 2002;

Chang et al., 2008; Didimo et al., 2011; Singh y Best, 2016). Sin embargo, es importante remarcar que la calidad de las visualizaciones producidas depende directamente de la calidad de los datos subyacentes, ya que Los datos inexactos e incompletos pueden impedir la eficacia de los métodos de monitoreo de transacciones.

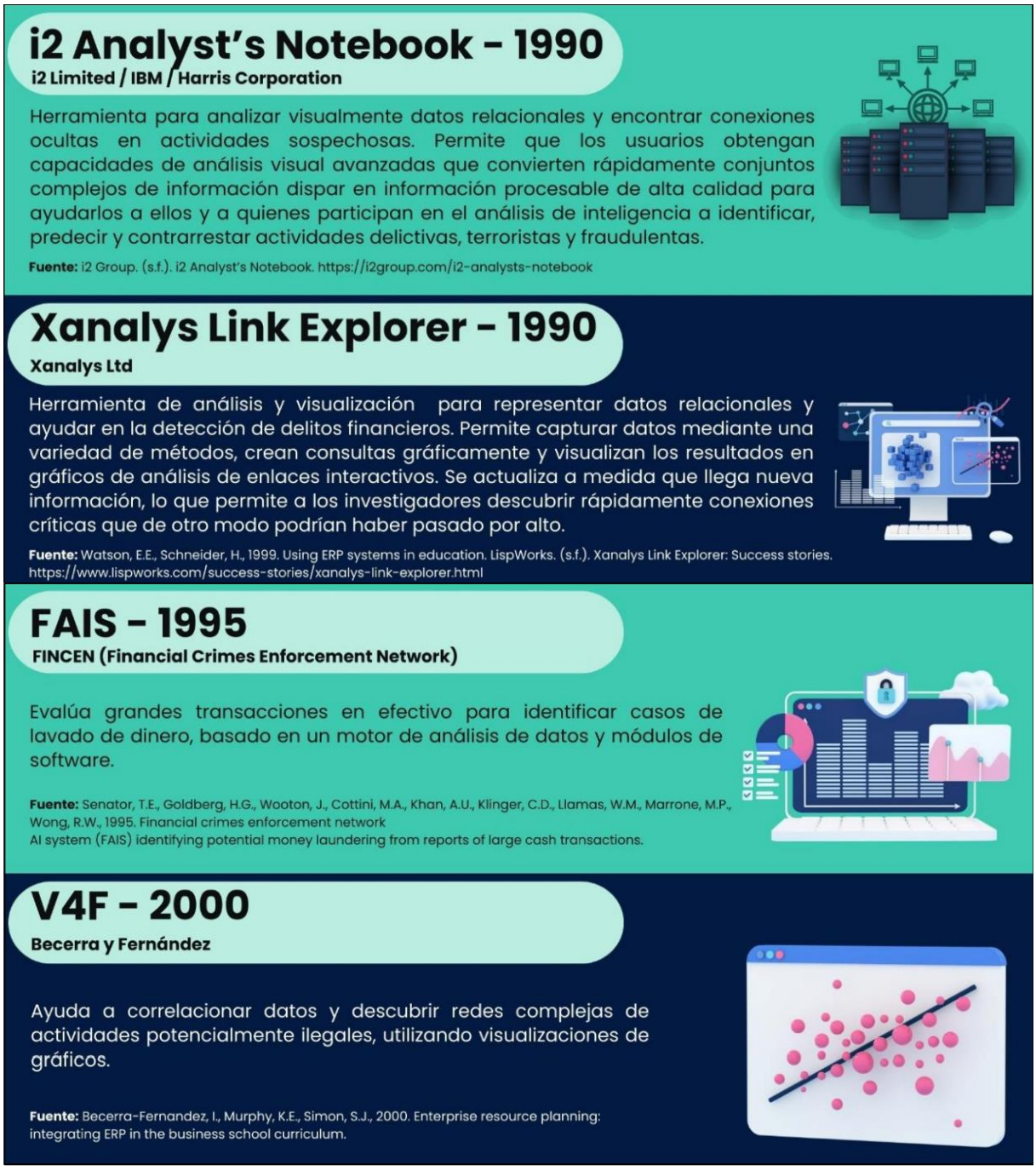
Muchos analistas utilizan hojas de cálculo para examinar tablas de datos de gran tamaño, aunque las hojas de cálculo brindan una visión detallada de las transacciones, no ofrecen una visión clara de las tendencias y correlaciones (Chang et al., 2007). Herramientas tales como Table Lens (Seo y Shneiderman, 2002) y hojas de datos (Eick, 2000) proporcionan vistas mejoradas de grandes volúmenes de datos tabulares. El aprendizaje automático parece haber mejorado la identificación de transacciones sospechosas en comparación con un método de umbral simple (Yue et al., 2007; Zhang et al., 2003). Ahora bien, relacionando esta herramienta tecnológica con la prevención del lavado de activos, los autores Gao y Ye (2007) desarrollaron un marco para combatir el lavado de dinero utilizando una serie de patrones transaccionales, estos patrones van desde lo “legal” a lo “habitual”, “inusual/anormal/anómalo”, “sospechoso” e “ilegal”, donde “habitual” significa “muy probablemente, pero no necesariamente legítimo”, mientras que “sospechoso” implica “una mayor probabilidad de ser ilegal”.

Por otro lado, Bolton y Hand (2002) propusieron que las transacciones financieras ilegales pueden identificarse marcando a los individuos según el riesgo percibido y restringiendo sus transacciones utilizando umbrales. Las transacciones que superen umbrales predeterminados requieren un escrutinio. Una consecuencia indeseable es que los delincuentes adaptan su comportamiento para evitar este control, por ejemplo, depositan cantidades más pequeñas importes que están por debajo del umbral (estructuración). De ahí que este control exclusivamente sea inadecuado para detectar transacciones sospechosas (Harvey y Magnusson, 2009).

Un investigador destina, en promedio, casi el 50% de su tiempo a examinar alertas que resultan ser falsas, lo que constituye una pérdida significativa de recursos. La necesidad de optimizar los procesos de investigación y reducir el número de falsos positivos ha impulsado la búsqueda de nuevas herramientas y técnicas de análisis de datos (Newman, 2007). El análisis de redes complejas, también denominadas gráficas en la literatura científica, ha demostrado ser una herramienta eficaz para la detección temprana y precisa de actividades anómalas (BecerraFernandez et al., 2000). La visualización de estas redes permite a los investigadores identificar patrones y relaciones ocultas en los datos, facilitando así la detección de actividades sospechosas (Hawking et al., 2005).

5.3. Aplicaciones y sistemas tecnológicos utilizados en la prevención del lavado de activos

Luego de haber dado estas introducciones teóricas, y teniendo en cuenta la importancia de la herramienta de visualización de datos en la prevención de lavados de activos de origen delictivo, y teniendo en cuenta además lo importante que resulta en la actualidad que los auditores y las entidades puedan tener la capacidad de analizar grandes volúmenes de datos para detectar operaciones inusuales y sospechosas, se elaboró la siguiente infografía a fin de sintetizar las diferentes aplicaciones/sistemas que existen en la actualidad que permiten detectar operaciones provenientes de actividades ilícitas:



Netmap- 2001

Tracy et al.

Implementa algoritmos gráficos para representar relaciones y datos en la lucha contra el crimen financiero.

Fuente: Tracy, S., Stewart, G., Boykin, R., Najm, M., Rosemann, M., Carpinetti, L., 2001. SAP Student Marketplace for the Advancement of Research and Teaching (SAP Smart)

- sin nombre - 2004

Johnson et al.

Método de análisis de redes sociales para detectar delitos financieros, encontrando actividades sospechosas a través del análisis de relaciones en línea.

Fuente: Johnson, T., Lorents, A.C., Morgan, J., Ozmun, J., 2004. A customized ERP/SAP model for business curriculum integration.

Palantir Gotham - 2005

Palantir Technologies

Análisis de grandes volúmenes de datos, detección de patrones de comportamiento inusual, visualización de redes de relaciones. Es una plataforma de software diseñada para ayudar a las agencias de inteligencia y defensa a detectar patrones ocultos en grandes conjuntos de datos. Se utiliza para integrar, visualizar y analizar datos de múltiples fuentes, como informes de inteligencia, registros financieros y comunicaciones.

Fuente: Palantir Technologies. (s.f.). Gotham platform. Palantir Technologies. https://www.palantir.com/platforms/gotham/

WireVis - 2008

Chang et al.

Sistema de análisis visual de transacciones financieras por cable, ayudando a los analistas a explorar un gran volumen de transacciones electrónicas.

Fuente: Chang, R., Ghoniem, M., Kosara, R., Ribarsky, W., Jing, Y., Suma, E., Ziemkiewicz, C., Kern, D., Sudjianto, A., 2007. WireVis: visualization of categorical, time-varying data from financial transactions.

-sin nombre - 2011

Salamon, T.

Utiliza agentes autónomos para modelar sistemas complejos, generando comportamientos emergentes para analizar redes sociales y el comportamiento social.

Fuente: Salamon, T., 2011. Design of Agent-Based Models.

(Esta infografía es de fuente propia, la misma fue elaborada en base a la lectura de diferentes autores y páginas webs que fueron debidamente mencionadas).

En base a la información de la infografía, se puede concluir los siguientes ***aspectos claves*** a modo de resumen:

1. Análisis visual relacional: estas herramientas permiten encontrar conexiones ocultas en grandes conjuntos de datos, ayudando a identificar actividades sospechosas. Por ejemplo, i2 Analyst's Notebook facilita la conversión de datos complejos en información procesable para detectar actividades delictivas, terroristas o fraudulentas.

2. Actualización en tiempo real: herramientas como Xanalys Link Explorer permiten que las visualizaciones se actualicen conforme llegan nuevos datos, lo que ayuda a los investigadores a descubrir conexiones que podrían pasar desapercibidas por el ojo humano.

3. Algoritmos gráficos y análisis de redes: utilizan visualizaciones de redes sociales y relaciones de datos para detectar delitos financieros. Un ejemplo es Netmap, que emplea algoritmos para representar relaciones y datos complejos.

4. Análisis de grandes volúmenes de datos: plataformas como Palantir Gotham están diseñadas para analizar grandes volúmenes de datos y detectar patrones ocultos de comportamiento inusual, integrando datos de múltiples fuentes.

5. Sistemas de alerta automatizados: algunas herramientas, como ComplyAdvantage Fraud Detection, utilizan inteligencia artificial y aprendizaje automático para generar alertas basadas en el análisis de comportamiento, identificando amenazas y anomalías en transacciones financieras.

Dentro de las ***principales características*** que debería tener un tablero de visualización de datos para detectar operaciones inusuales y sospechosas se encuentran las siguientes:

• **Capacidad de procesamiento de grandes volúmenes de datos:** es fundamental que el tablero pueda procesar grandes cantidades de datos, como transacciones financieras y reportes de actividad sospechosa, en tiempo real.

• **Detección de patrones anómalos:** el tablero debe poder identificar patrones de comportamiento inusual o cambios repentinos en las transacciones financieras, que puedan ser indicativos de lavado de activos. Es por eso que es sumamente importante que previamente a esto, el auditor haya definido correctamente el perfil de cliente, para que la herramienta tecnológica pueda detectar todas aquellas operaciones que salen de ese perfil, y podrían ser inusuales o sospechosas.

• **Integración de fuentes de datos múltiples:** la capacidad de combinar datos de diferentes fuentes, como informes financieros, bases de datos de transacciones y registros bancarios, es crucial para una visión integral del comportamiento financiero.

• **Generación de alertas automáticas:** el tablero debería emitir señales de alerta basadas en reglas predefinidas o por medio de algoritmos de inteligencia artificial que identifiquen riesgos. La clasificación de las alertas según el nivel de riesgo es importante para la priorización de las investigaciones.

• **Visualización de redes de relaciones:** debe mostrar relaciones entre entidades y transacciones para identificar conexiones ocultas, como redes de personas o empresas involucradas en actividades ilícitas.

• **Actualización en tiempo real:** es esencial que la herramienta pueda actualizarse con nuevos datos en tiempo real, permitiendo que los analistas detecten rápidamente operaciones sospechosas a medida que ocurren.

6. COMENTARIOS FINALES

Con el objetivo de dar una conclusión a esta investigación, se menciona como comentarios finales que luego de haber realizado la correspondiente revisión de la literatura, se concluye que los autores sugieren y son optimistas sobre el uso de la herramienta de visualización de datos para la detección de operaciones inusuales y sospechosas para prevenir el lavado de activos de origen delictivo. De esta forma se podrá brindar un servicio más eficiente y eficaz a los usuarios de la información y se podrá contribuir a la disminución de todas aquellas actividades ilícitas que se intentan cubrir. Se considera importante para seguir con esta línea de investigación en trabajos futuros, tener en cuenta lo que establecen las normas contables profesionales vigentes y las respectivas resoluciones actualizadas respecto a la prevención del lavado de activos de origen delictivo y financiación del terrorismo. Así como también, resoluciones que regulen la utilización de herramientas tecnológicas a ser incorporadas en las tareas del auditor.

REFERENCIAS BIBLIOGRÁFICAS

Albanese, D. (2012). Análisis y evaluación de riesgos: aplicación de una matriz de riesgo en el marco de un plan de prevención contra el lavado de activos.

Becerra-Fernandez, I., Murphy, K.E., Simon, S.J., 2000. Enterprise resource planning: integrating ERP in the business school curriculum. Commun. ACM 43 (4), 39–41.

Bolton, R.J., Hand, D.J., 2002. Statistical fraud detection: a review. Stat. Sci. 17 (3), 235–249 Institute of Mathematical Statistics.

Chang, R., Ghoniem, M., Kosara, R., Ribarsky, W., Jing, Y., Suma, E., Ziemkiewicz, C., Kern, D., Sudjianto, A., 2007. WireVis: visualization of categorical, time-varying data from financial transactions. Visual Analytics Science and Technology, 2007. VAST 2007. IEEE Symposium on.

Chang, R., Lee, A., Ghoniem, M., Kosara, R., Ribarsky, W., Yang, J., Suma, E., Ziemkiewicz, C., Kern, D., Sudjianto, A., 2008. Scalable and interactive visual analysis of financial wire transactions for fraud detection. Inf. Vis. 7 (1), 63–76.

Didimo, W., Liotta, G., Montecchiani, F., Palladino, P., 2011. An Advanced Network Visualization System for Financial Crime Detection. Pacific Visualization Symposium. 2011. IEEE. IEEE, PacificVis.

Eick, S.G., 2000. Visual discovery and analysis. IEEE Trans. Vis. Comput. Graph. 6 (1), 44–58.

Gao, Z., Ye, M., 2007. A framework for data mining-based anti-money laundering research. J. Money Laund. Control 10 (2), 170–179.

Harvey, J., Magnusson, D., 2009. The costs of implementing the anti-money laundering regulations in Sweden. J. Money Laund. Control 12 (2), 101–112.

Hawking, P., McCarthy, B., Stein, A., 2005. Integrating ERP's second wave into higher education curriculum. PACIS 2005 Proceedings, p. 83.

Hoelscher, J., & Mortimer, A. (2018). Using Tableau to visualize data and drive decision-making. Journal of Accounting Education, 44, 49-59.

Johnson, T., Lorents, A.C., Morgan, J., Ozmun, J., 2004. A customized ERP/SAP model for business curriculum integration. J. Inf. Syst. Educ. 15 (3), 245–254.

Liu, J., Bier, E., Wilson, A., Guerra-Gomez, J.A., Honda, T., Sricharan, K., Gilpin, L., Davies, D., 2016. Graph analysis for detecting fraud, waste, and abuse in health-care data. (Report). AI Mag. 37 (2), 33.

Lopez-Rojas, E.A., Axelsson, S., 2012. Multi agent based simulation (mabs) of financial transactions for anti money laundering (aml). Nordic Conference on Secure IT Systems. Blekinge Institute of Technology.

Ministerio Público Fiscal. (2000). Ley 25.246. Modificación. Encubrimiento y Lavado de Activos de origen delictivo. Unidad de Información Financiera. Deber de informar.

Sujetos obligados. Régimen Penal Administrativo. Recuperado de https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/62977/texact.htm

Newman, L., 2007. Making the most of anti-money laundering systems. J. Superannuat. Manag. 1 (2), 31.

Oztas, B., Cetinkaya, D., Adedoyin, F., Budka, M., Aksu, G., & Dogan, H. (2024). Transaction monitoring in anti-money laundering: A qualitative analysis and points of view from industry. Future Generation Computer Systems, 159, 161-171.

Pavón, J., Arroyo, M., Hassan, S., Sansores, C., 2008. Agent-based modelling and simulation for the analysis of social patterns. Pattern Recogn. Lett. 29 (8), 1039–1048.

Pontes, R., Lewis, N., McFarlane, P., & Craig, P. (2022). Anti-money laundering in the United Kingdom: new directions for a more effective regime. Journal of Money Laundering Control, 25(2), 401- 413.

Salamon, T., 2011. Design of Agent-Based Models. Eva & Tomas Bruckner Publishing.

Seo, J., Shneiderman, B., 2002. Interactively exploring hierarchical clustering results [gene identification]. Computer 35 (7), 80–86.

Senator, T.E., Goldberg, H.G., Wooton, J., Cottini, M.A., Khan, A.U., Klinger, C.D., Llamas, W.M., Marrone, M.P., Wong, R.W., 1995. Financial crimes enforcement network AI system (FAIS) identifying potential money laundering from reports of large cash transactions. AI Mag. 16 (4), 21.

Singh, K., Best, P., 2016. Interactive visual analysis of anomalous accounts payable transactions in SAP enterprise systems. Manag. Audit. J. 31 (1), 35–63.

Singh, K., & Best, P. 2019. Anti-money laundering: Using data visualization to identify suspicious activity. International Journal of Accounting Information Systems, 34, 100418.

Slosse, C.A.; Gordicz, J.C.; Gamondés, S. 2008. Auditoría. Buenos Aires, La Ley, 742 p.

Thomas, J.J., Cook, K.A., 2006. A visual analytics agenda. IEEE Comput. Graph. Appl. 26 (1), 10–13.

Tracy, S., Stewart, G., Boykin, R., Najm, M., Rosemann, M., Carpinetti, L., 2001. SAP Student Marketplace for the Advancement of Research and Teaching (SAP Smart). AMCIS 2001 Proceedings. p. 195.

Wainstein, M. 2004. La corrupción y la actividad del contador público. Buenos Aires, Errepar, 427 p.

Watson, E.E., Schneider, H., 1999. Using ERP systems in education. Comm. AIS 1 (2es), 3

Yue, D., Wu, X., Wang, Y., Li, Y., Chu, C.-H., 2007. A Review of Data Mining-Based Financial Fraud Detection Research. Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on. IEEE.

Zhang, Z.M., Salerno, J.J., Yu, P.S., 2003. Applying data mining in investigating money laundering crimes. Proceedings of the Ninth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM.