Año 28 No. 102, 2023 ABRIL-JUNIO

Año 28 No. 102, 2023 ABRIL-JUNIO

Revista Venezolana de Gerencia

UNIVERSIDAD DEL ZULIA (LUZ)
Facultad de Ciencias Económicas y Sociales
Centro de Estudios de la Empresa

ISSN 1315-9984

Como citar: De La Torre Lascano, C. M., y Quiroz Peña, J. I. (2023). Ciberdelito y su asociación en el cometimiento de fraudes financieros en la pandemia de la COVID-19. *Revista Venezolana De Gerencia*, *28*(102), 609-628 https://doi.org/10.52080/rvgluz.28.102.11

Universidad del Zulia (LUZ)
Revista Venezolana de Gerencia (RVG)
Año 28 No. 102, 2023, 609-628
ISSN 1315-9984 / e-ISSN 2477-9423

Ciberdelito y su asociación en el cometimiento de fraudes financieros en la pandemia de la COVID-19

De La Torre Lascano, Carlos Mauricio*
Quiroz Peña, Jaime Iván**

Resumen

La COVID-19 afectó a millones de personas y organizaciones de todos los sectores y clases sociales, coadyuvando a que proliferen riesgos sociales, económicos, tecnológicos y financieros, incrementándose en el ámbito organizacional el ciberdelito y el fraude financiero. Estas actividades ilícitas tomaron protagonismo debido a la adopción de medios digitales que las organizaciones utilizaron para poder continuar con sus operaciones. Por ello, el objetivo de esta investigación fue evaluar la percepción del ciberdelito y del fraude financiero en organizaciones del sector público y privado ecuatoriano en la COVID-19. Para esto, se realizó un estudio de tipo descriptivo, bajo un enfoque cuantitativo de corte transversal, utilizando el estadístico chi-cuadrado como medio de asociación de las variables. Los resultados demostraron que la manipulación de datos económicos y estafas fue el principal ciberdelito incurrido durante la pandemia, siendo el fraude a los estados financieros el mayor esquema ejecutado por los perpetradores. Se identificaron a las funciones de control interno y auditoría interna como las principales líneas de prevención y aseguramiento frente a estas actividades criminales.

Palabras clave: COVID-19; ciberdelito; fraude financiero; control interno; auditoría interna.

Recibido: 08.11.22 **Aceptado**:03.02.23

* Doctor (Ph.D.) por la Universidad de Salamanca. Programa Doctoral Estado de Derecho y Gobernanza Global. Magíster en Gerencia Empresarial, MBA, mención Gerencia Financiera. Docente Investigador titular de la Universidad Central del Ecuador, Quito-Ecuador. Email: cdelatorre@uce.edu.ec. ORCID: https://orcid.org/0000-0003-0604-2845

** Magíster en Administración de Empresas mención Dirección Estratégica de Proyectos por la Universidad Central del Ecuador, Quito-Ecuador. Ingeniero en Contabilidad y Auditoría por la Universidad Central del Ecuador, Quito-Ecuador. Email: jiquiroz@uce.edu.ec. ORCID: https://orcid.org/0000-0001-8268-1169

Cybercrime and its association in the commission of financial fraud in COVID-19 pandemic

Abstract

COVID-19 affected millions of people and organizations from all sectors and social classes, contributing to the proliferation of social, economic, technological and financial risks, increasing cybercrime and financial fraud in the business field. These illicit activities took leadership due to the adoption of digital media that the organizations used to be able to continue their operations. Therefore, the goal of this research was to evaluate the perception of cybercrime and financial fraud in Ecuadorian public and private sector organizations in COVID-19. For this, a descriptive study was carried out, under a cross-sectional quantitative approach, using the chi-square statistic as a means of association of the variables. The results showed that the manipulation of economic data and fraud was the main cybercrime incurred during the pandemic, with financial statement fraud being the largest scheme executed by the perpetrators. The internal control and internal audit functions were identified as the main lines of prevention and assurance against these criminal activities.

Keywords: COVID-19; cybercrime; financial fraud; internal control; internal audit.

1. Introducción

El brote de la COVID-19 conmocionó al mundo entero, millones de personas y organizaciones de todo sector y toda clase social se vieron afectadas. Este fenómeno fue progresivamente propagándose desde Asia a Europa, Estados Unidos, hasta implantarse en América Latina, originando un impacto social dentro de la salud y generando una colosal crisis financiera que produjo cierres de negocios y dantescas pérdidas económicas (Buil-Gil et al, 2020).

Adicionalmente, la pandemia a nivel mundial coadyuvó a que proliferen riesgos sociales, económicos, biológicos, tecnológicos y financieros que condujeron a escenarios turbios de insalubridad, muertes, pobreza, delitos y en el ámbito organizacional se produjo una considerable recesión económica dentro del sector público y privado, por lo que proliferaron los delitos financieros (De La Torre y Quiroz, 2020). Este contexto sobrevino en conductas delictivas en ambientes tecnológicos, sociales y económicos que aumentaron a causa de la pandemia y las formas de trabajo remotas adoptadas por las organizaciones (Campedelli et al, 2020).

A nivel global, los gobiernos de cada país formularon normas que regulaban la interacción en el trabajo en las organizaciones, adoptándose el trabajo vía remota, dando como

resultado que las empresas implementen el uso de la tecnología en el desempeño de las operaciones y funciones de sus colaboradores (Gómez, 2020). Por lo que, las empresas se vieron en la necesidad de adoptar sistemas de información más sofisticados y robustos para ejecutar sus actividades, empleando el desarrollo de operaciones financieras totalmente dentro de sistemas informáticos (Barretto, 2022).

Con el incremento tecnológico que se instauró en las organizaciones en el transcurso de la pandemia, se generaron vacíos que dieron origen a la generación de actividades ilícitas como la corrupción, el ciberdelito y el fraude, aprovechando el uso de los sistemas de información para vulnerarlos y aprovecharse de ellos malintencionadamente (Buil-Gil et al, 2020). Estas actividades ilícitas fueron perpetradas en todos los niveles por funcionarios internos, usuarios externos, trabajadores de primera línea, empleados privados y altos directivos, que se beneficiaron de esta situación, aprovechando la tecnología ilícitamente rompieron las normas morales y éticas, manifestándose este fenómeno de manera nociva a nivel mundial (Rose-Ackerman, 2021; Ramos et al, 2019).

Las organizaciones criminales van innovándose en metodologías para efectuar lavado de dinero, fraude y delitos financieros, usando nuevas tecnologías, especialmente plataformas en línea y sistemas de información empresariales (Gerbrands et al, 2022). Gestándose ciberdelitos, que en la pandemia se manifestaron en las actividades rutinarias realizadas por las organizaciones en sistemas en línea, como el robo de identidad, falsificación de información bancaria, compras en línea fraudulentas y virus informáticos, que figuraron como comportamientos ilícitos que generaron millonarias pérdidas financieras y utilizando de manera efectiva delitos cibernéticos (Hawdon et al, 2020).

Otro riesgo latente en el conglomerado organizacional es el de fraude, que se presentó en mayores proporciones dentro de los canales e información de carácter económico y financiero, el cual tomó un papel protagónico dentro de las empresas e instituciones en la pandemia, generando el campo propicio para que se gesten actividades ilícitas corporativas, atacando los sistemas de información institucionales, ocasionando pérdidas económicas, humanas y financieras (Félix y Meza, 2021). Es así como el riesgo de fraude creció en niveles considerablemente altos en la pandemia de la COVID-19, el empleo de tecnología con el fin de atacar a los sistemas de información organizacionales condujo a que proliferen los riesgos de tipo tecnológico, económico y financiero (De La Torre y Quiroz, 2020; Buil-Gil et al, 2020; Qiu et al, 2021).

El reporte a las naciones, difundido por la Asociación de Examinadores de Fraude Certificados (ACFE, 2022) al estudiar a 133 países y analizar 2.110 casos entre enero de 2020 y septiembre de 2021, indica que a nivel mundial se produjeron pérdidas totales por más de USD 3,6 mil millones producto del fraude financiero, generando pérdidas en las empresas de hasta un 5% de sus ingresos por año, dando como resultado una pérdida promedio de USD 1.783.000 por cada caso, demostrando que se originó un incremento significativo del fraude financiero en la época de pandemia.

En este contexto, las organizaciones sufrieron pérdidas significativas y las estratagemas más comunes fueron:

uso de la información privada, fraude tributario, desvío de fondos, fraude en seguros corporativos y sistemas, redes de información, test fraudulentos, falsos proveedores, compras con sobreprecios, ciberamenazas y ciberdelincuencia (Salazar, 2021; Faraco, 2021). En Ecuador, entre los delitos más comunes en la emergencia sanitaria se encuentra el incumplimiento a las obligaciones designadas por los entes reguladores, malversación de la información financiera y fraude tributario (Loja, 2021). El fraude financiero en Ecuador se incrementó un 16%, el mismo que se gestó debido a proliferación del fraude financiero por medio de canales digitales (Deloitte, 2021).

Por lo expuesto, el objetivo de la presente investigación fue evaluar la percepción del ciberdelito y del fraude financiero en las empresas del sector público y privado ecuatoriano en la pandemia de la COVID-19, con el fin de describir las principales líneas de prevención que permitan asegurar los sistemas de información, para mitigar el riesgo tecnológico y financiero en las organizaciones.

Para esto, el planteamiento hipotético que se procedió a validar fue si las actividades ilícitas producto del ciberdelito en las redes y sistemas de información empresariales son incidentes en la proliferación de mayores fraudes financieros en las organizaciones.

La investigación desarrolló un estudio de tipo descriptivo, bajo un enfoque cuantitativo de corte transversal. De manera cuantitativa se midió la percepción del nivel de ciberdelito y del fraude financiero en empresas del sector público y privado ecuatoriano. Además, se utilizó el estadístico *chi-cuadrado* con el fin de observar la asociación del ciberdelito como actividad delictiva que coadyuva a la consecución de mayores fraudes financieros en las organizaciones del ámbito ecuatoriano. Los datos se recolectaron a través de la aplicación de encuestas dentro del período de octubre de 2021 a mayo de 2022, se encuestaron a 102 organizaciones de las ciudades de Quito, Guayaquil y Cuenca que se encuentran dentro del ranking empresarial proporcionado por la Superintendencia de Compañías, Valores y Seguros en su plataforma institucional.

Los participantes que representaron a sus organizaciones fueron gerentes, administradores, contadores, contralores, auditores internos, jefes de área de sistemas y/o directores financieros. La muestra estuvo conformada por 102 organizaciones escogidas a través de la técnica de muestreo aleatorio simple, se conformaron dos grupos según al sector que pertenecen (47 públicas y 55 privadas). La encuesta se dividió en siete secciones y 40 ítems, siendo validada por un grupo focal con la participación de los autores del estudio y dos expertos en Auditoría Informática. Los datos se procesaron en el software SPSS v.26.0., lo que permitió la obtención de resultados presentados objetivamente.

2. Riesgos e impactos en los sistemas de información organizacionales

El escenario empresarial debido a la pandemia generó la proliferación de riesgos tecnológicos y financieros, ocasionando en las organizaciones la pérdida de transparencia, vulneración de controles internos, alteración de los modelos de supervisión, incumplimiento de normas de aseguramiento,

pérdida de información y afectación financiera (Rose-Ackerman, 2021). Adicionalmente, la pandemia dio lugar a escándalos corporativos causados por la ineficiente acción y gestión de la salubridad en las organizaciones y gobiernos, el acto oportunista de muchas personas y organizaciones con el fin de beneficiarse de diferentes maneras como sobreprecios, venta de insumos en mal estado, negociaciones fraudulentas, alterando sistemas de información y en general creando estratagemas que vulneraron el control interno institucional en todos los niveles (Hail et al, 2018).

2.1. Ciberdelito y sus consecuencias en la COVID-19

El ciberdelito ataca a los sistemas y redes de información tanto personales, así como empresariales, constituyendo un tipo de riesgo tecnológico. Es el resultado de la conducta delictiva que los perpetradores ejercen con el fin de obtener un beneficio ilícito mediante la utilización de herramientas tecnológicas como los sistemas de información en línea, redes informáticas, modificando reportes en sistemas informáticos, alterando la información, afectando la confidencialidad de datos con fines de ocultamiento, enriquecimiento ilícito, estafas financieras y generando daños a la reputación institucional (Westerski et al, 2021). Los ciberdelitos se adaptan a los cambios sustanciales que dejó la pandemia en torno a su amplitud, diversidad y medios de ataque (Naidoo, 2020).

Las prácticas dolosas hacia los sistemas de información empresariales incluyen: destrucción de archivos *"ataques de virus informáticos"*, ocultamiento de información y cifras financieras, alteración de registros en origen, acceso a fuentes gubernamentales privadas *"Ciberespionaje",* manipulación de datos económicos *"estafas informáticas",* hackeo de contraseñas con fines de extorsión *"ransomware",* divulgación de información privada, apropiación indebida de identidad *"phishing"* (Solomón y Soltes, 2021). Otras formas de estafa y fraudes en los sistemas de información radican en el robo o clonaciones de tarjetas de crédito para compras fraudulentas en línea "*skimming*" (Dewi y Fadjarenie, 2020).

Los fraudes asociados con la piratería en redes informáticas corporativas efectuados en los sistemas informáticos, incluyeron la presentación de información incierta y falsa en los sistemas de comunicación institucionales, correos electrónicos, canales comunicacionales internos y externos. Esta práctica delictiva ha coadyuvado para que se distorsione la información financiera de manera fraudulenta, constituyendo arquetipos de fraude financiero y de delitos cibernéticos en auge en el transcurso de la pandemia (Buil-Gil et al, 2020).

Los ciberdelincuentes emulan plataformas corporativas de información empresariales, sistemas financieros, comunicaciones en línea, servicios de alojamiento en la nube, gestándose el hurto y robo de datos, atentando contra los sistemas de información organizacionales (Naidoo, 2020; Lu et al, 2020). El costo por pérdida reputacional debido a la realización de actos fraudulentos utilizando redes informáticas es elevado y altera el valor accionario de las organizaciones, inclusive pueden enfrentar sanciones según la jurisdicción de cada país, afectando negativamente su continuidad en el medio (Lai et al, 2019).

2.2. Visión global de Fraude Financiero

El fraude financiero consiste en el acto intencional de modificar la información financiera de las organizaciones, falsificar reportes financieros u observar la aplicación adecuada de estándares internacionales de contabilidad, con el fin de obtener beneficios que pueden incurrir en el hurto, sustracción, desviación, o apropiación ilícita de activos (Ramos et al, 2019). Albizri et al, (2019) indican que los esquemas de fraude financiero son: *i)* falsificación y alteración de registros contables, *ii)* omisiones y ocultamiento de información, *iii)* presentación de información errada, *iv)* aplicación intencional de principios contables erróneos, *v)* omisión a la normativa internacional, y *vi)* manipulación de prácticas contables.

La naturaleza del fraude se puede explicar mediante el denominado *triángulo del fraude,* el cual indica que el perpetrador muestra tres componentes en su conducta: *i) poder*, motivo o presión para generar actividades ilícitas; *ii) oportunidad,* determinación de vías para cometer el fraude; y *iii) racionalización,* creer que el fraude es aceptable (Cressey, 1961). Estos elementos son los originarios de la conducta antiética e ilegal, que fomentan la deslealtad, avaricia, engaño y hurto, con el fin de obtener ventajas desleales y deshonestas (Galvis y Santos, 2017). La conducta dolosa y fraudulenta en la presentación de información financiera generada por los perpetradores del fraude menoscaban la confianza de la ciudadanía, de directivos, accionistas, inversores, partes interesadas y organismos estatales; generan pérdidas económicas, rompen la seguridad de procesos institucionales y acrecentar el riesgo de fraude (Amiram et al, 2018).

El riesgo inherente que poseen los sistemas de información financiera de las organizaciones incluye el riesgo de fraude, que se define como la probabilidad que una entidad cometa actos fraudulentos e ilícitos en la gestión económica institucional (De La Torre, 2018). La acertada gestión y evaluación del riesgo de fraude permitirá mantener la razonabilidad y seguridad en los sistemas de información financiera institucionales (Qiu et al, 2021). Mientras existan procesos, políticas, funciones, lineamientos y procedimientos claramente definidos y suficientes, se mitigará en gran medida el riesgo de fraude presente en los sistemas de información financiera (Kazemian et al, 2019).

2.3. Medios de prevención para la protección de los sistemas de información organizacionales

El fortalecimiento y protección organizacional se presenta dentro de tres líneas de defensa: a) la gestión del gobierno de cada entidad para el cumplimiento de objetivos empresariales, b) el control interno institucional como gestor de riegos, y c) la función de Auditoría Interna como gestor de aseguramiento y garantía organizacional (Weekes-Marshall, 2020). La Auditoría Interna cumple la función principal de aseguramiento en la organización a todos sus componentes y procesos, así como garantizar que los sistemas informáticos corporativos ofrezcan información veraz, oportuna y de calidad (Nordin, 2022). Auditoría Interna asesora a la alta dirección, áreas,

departamentos, y órganos de gobierno con el fin de promover lineamientos de Control Interno que promuevan la gestión adecuada de riesgos y minimicen las actividades ilícitas (De La Torre, 2018). Por ello, se debe instaurar a la unidad Auditoría Interna como el principal medio de prevención de los sistemas de Información organizacionales (De La Torre y Quiroz, 2020).

Los principales análisis que ejerce Auditoría Interna radican en la examinación de estados financieros, control interno, gestión de riesgos, análisis, evaluación y aseguramiento de procesos internos, aseguramiento del sistema integrado de información corporativo, agregando valor y actúa como medio de prevención y detección de fraudes (Huq et al, 2022; Wu et al, 2022). En este sentido, una Auditoría Interna eficaz previene que se originen actividades ilícitas, para lograr la eficacia se debe instaurar un adecuado y eficiente Control Interno institucional como modelo de aseguramiento y evaluación, utilizando la tecnología en la gestión de procesos y evaluación de riesgos (Kasper y Alm, 2022; Werner et al, 2021; Rakipi et al, 2021).

2.4. Control Interno como mecanismo de aseguramiento

Otro desafío que dejó latente la pandemia de la COVID-19, fue establecer calidad y confiabilidad en la ejecución y procesos internos en los que intervienen los sistemas de información empresariales, a través de la implementación de un adecuado modelo de Control Interno (Baatwah y Al-Ansi, 2022). El control interno es un mecanismo y un sistema que asegura los procesos organizacionales, brinda confiabilidad sobre los sistemas de información, promueve la presentación de información financiera confiable, evalúa y gestiona riesgos institucionales, brinda aseguramiento a la alta dirección y a usuarios internos y externos, agregando valor a las actividades empresariales (Henk, 2020).

El control interno debe ser evaluado constantemente por la función de Auditoría Interna, debe promover la seguridad en los procesos de información organizacionales, promoviendo políticas robustas de Tecnologías de la Comunicación e Información (TI), gestión de riesgos tecnológicos, y evaluación de vulnerabilidades informáticas, debe ser una herramienta que detecte ataques, gestione el riesgo operativo y prevenga daños materiales financieros (Steinbart et al, 2018).

The Institute of Internal Auditors (IAI, 2020) indica que la función de Auditoría Interna debe trabajar en cinco componentes clave en su modelo de control interno, los cuales son: *i) ambiente de control, ii) evaluación de riesgos, iii) actividades de control, iv) información y comunicación, y v) actividades de monitoreo o supervisión.* Estos elementos deben coordinarse para que la función de gestión de riesgos financieros y tecnológicos aseguren eficaz y efectivamente a las organizaciones (De La Torre y Quiroz, 2020; Ge et al, 2020; Chahine et al, 2021).

2.5. Medios de detección del fraude en los sistemas de información organizacionales

Los mecanismos de detección

del fraude recaen principalmente en la función de Auditoría Forense, al realizar un examen especial para introducirse en actos delictivos (De La Torre, 2018). No obstante, la función de Auditoría Interna enfocada al análisis de Control Interno también posee real incidencia en la detección de hechos fraudulentos en las organizaciones (Gottschalk & Gunnesdal, 2018).

Auditoría Forense y Auditoría Interna han de ser los medios principales para identificar áreas clave de vulnerabilidad en los sistemas de información organizacionales, con el fin de detectar actividades inusuales e ilícitas, así como identificar delitos informáticos, económicos y financieros, con la finalidad de enmarcarlos en la gestión de Control Interno institucional y en los programas de aseguramiento propuestos por las organizaciones (De La Torre y Cáceres, 2017).

3. Percepción del ciberdelito y del fraude financiero en organizaciones del sector público y privado ecuatoriano en la COVID-19

En esta sección, se presenta el análisis de los resultados medidos porcentualmente, obtenidos en las 102 organizaciones de las ciudades de Quito, Guayaquil y Cuenca, considerando los sectores público y privado, sobre el nivel del ciberdelito en las organizaciones, sus causas y medios de detección de las actividades ilícitas, así como su incidencia en la aparición de fraude financiero.

3.1. Nivel de fraude en la pandemia de la COVID-19

Los resultados de manera global relacionados con la percepción general del fraude indican que el sector público con el 74,51% es donde se presentó mayor nivel de fraude organizacional en la pandemia, el sector privado presentó un 25,49%; la puntuación denota la percepción que tienen las organizaciones sobre el sector público, en donde su estructura presentó mayor indicio de actos delictivos en el transcurso de la pandemia. El sector privado con menor puntuación fue un sector que, a pesar de tener mayores controles internos, se vio también envuelto en actividades ilícitas.

La tabla 1, presenta la percepción de las principales tipologías de fraude que proliferaron en la pandemia, además de mostrar el nivel de fraude por sector y tipo de actividad económica. Se observa la corrupción como la principal estratagema de fraude, con un 28,43% considerando el poder de la autoridad pública y privada en la inadecuada utilización de sus instrumentos de gobierno; con un 25,49% se presenta el fraude a los estados financieros, cuyo objetivo es ocultar o modificar la información financiera presentada por las organizaciones a los usuarios internos y externos.

Tabla 1
Principales tipologías y nivel de fraude por sector y por actividad económica

Tipologías / Causas		Sectores		Total
		Privado	Público	
Tipos de fraude	Lavado de activos	4,90%	8,82%	13,73%
	Conflicto de intereses internos y externos	0,98%	7,84%	8,82%
	Corrupción	5,88%	22,55%	28,43%
	Fraude en los estados financieros	4,90%	20,59%	25,49%
	Sobornos	8,82%	14,71%	23,53%
Total percepción de fraude por sector		25,49%	74,51%	100,00%
Actividad económica	Agrícola y ganadero	0,98%	0,98%	1,96%
	Automotriz	2,94%	2,94%	5,88%
	Comercial	0,98%	5,88%	6,86%
	Comunicaciones	3,92%	9,80%	13,73%
	Educativo	2,94%	0,98%	3,92%
	Extractivista (petrolero y minero)	3,92%	7,84%	11,76%
	Financiero	2,94%	9,80%	12,75%
	Inmobiliario	0,00%	9,80%	9,80%
	Manufacturero y siderúrgico	1,96%	5,88%	7,84%
	Salud	4,90%	15,69%	20,59%
	Servicios varios (transporte, profesionales, comidas, etc.)	0,00%	4,90%	4,90%
Total percepción de fraude por sector		25,49%	74,51%	100,00%

Fuente: Elaboración propia

El tipo de actividad económica que mostró mayor nivel de presencia de fraude fue el de la salud, con un 20,59%; denotando cómo la pandemia menoscabó y dejó indefensos los controles de estas organizaciones a nivel público y privado. Quedando en manifiesto cómo las asociaciones ilícitas e individuos utilizaron este sector para cometer sus actividades ilegales. Siendo este sector donde se vieron envueltos actos de corrupción, sobreprecios, repartición de redes hospitalarias a grupos de poder, incluyendo actos de soborno. Los resultados están en contexto con el Informe de ACFE (2022), donde se señala que la principal tipología de fraude en el período 2020-2021 fue la corrupción, siendo el más común a nivel mundial.

3.2. Fraude financiero en las organizaciones

La tabla 2, muestra los principales esquemas de fraude financiero y cuáles fueron las actividades organizacionales que presentaron mayores riesgos. Los

resultados señalan que el fraude a los estados financieros fue el principal esquema ilícito que se evidenció en la pandemia de la COVID-19 con un 25,49%. Este resultado se relaciona con la manipulación de los sistemas de información, que fue el segundo esquema que presentó mayor puntuación según la percepción de los usuarios con un 23,53%. Ambas estratagemas inciden en la entrega de información a usuarios internos y externos, manipulando u ocultando información tanto financiera o dentro de los procesos institucionales. Además, la puntuación también indica como la falsificación de información, y evasión tributaria tomó un gran impulso en la emergencia sanitaria, los perpetradores engendraron métodos para evadir el pago al fisco con fines ilícitos y aprovechándose de la falta de controles eficientes de la Administración Tributaria.

Tabla 2
Principales esquemas de fraude financiero y actividades que representan mayor riesgo por sector

Esquemas / Actividades		Sectores		Total
		Privado	Público	
Esquemas de fraude financiero	Evasión y falsificación de impuestos	8,82%	13,73%	22,55%
	Fraude a los estados financieros	12,75%	12,75%	25,49%
	Fraude en manejo de RRHH	0,98%	0,98%	1,96%
	Fraude en operaciones financieras y skimming	5,88%	3,92%	9,80%
	Manipulación de sistemas de información	9,80%	13,73%	23,53%
	Sobreprecios, reembolsos y pagos fraudulentos	6,86%	9,80%	16,67%
Total fraude financiero por sector		45,10%	54,90%	100,00%
Actividades que representan mayor riesgo de fraude	Facturación	7,84%	7,84%	15,69%
	Noncash	0,98%	0,00%	0,98%
	Reembolsos de gastos	3,92%	2,94%	6,86%
	Skimming (robo de información de tarjetas de crédito)	8,82%	10,78%	19,61%
	Tenencia de efectivo	7,84%	14,71%	22,55%
	Manipulación de cheques y pagos	5,88%	8,82%	14,71%
	Nómina de sueldos	1,96%	0,00%	1,96%
	Hurto de efectivo	4,90%	6,86%	11,76%
	Registrar desembolsos	0,98%	0,98%	1,96%
	Cuentas por Cobrar	1,96%	1,96%	3,92%
Total fraude financiero por sector		45,10%	54,90%	100,00%

Fuente: Elaboración propia

La actividad con mayor riesgo de fraude financiero fue la tenencia del efectivo en custodia del personal con una puntuación del 22,55% que significa un alto riesgo dentro de los controles institucionales; la segunda actividad con mayor riesgo fue el robo de información de tarjetas de crédito (*skimming*), la misma que tomó auge gracias al crecimiento de los negocios y actividades en línea vía internet, donde los perpetradores buscaron mecanismos para robar la identidad de las personas y aprovecharse económicamente mediante estos actos ilícitos.

La tabla 3, indica los departamentos y áreas que presentaron mayor ocurrencia de fraude por sector según la percepción de los usuarios en estudio, donde el departamento de contabilidad con una puntuación del 31,37% fue la unidad con mayor ocurrencia de fraude, seguida de la unidad de Ventas y Facturación con un 21,57%; esto determina como el riesgo de fraude se presenta en un nivel avanzado en las áreas que generan la información económica organizacional.

Tabla 3
Departamentos y áreas de mayor ocurrencia de fraude financiero por sector

Departamentos / Áreas		Sectores		Total
		Privado	Público	
Departamentos de mayor riesgo de fraude	a) Operaciones	11,76%	5,88%	17,65%
	b) Contabilidad	11,76%	19,61%	31,37%
	c) Administración	5,88%	6,86%	12,75%
	d) Ejecutivos y Alta gerencia	2,94%	8,82%	11,76%
	e) Ventas	11,76%	9,80%	21,57%
	f) Control Interno	0,98%	3,92%	4,90%
Total fraude financiero por sector		45,10%	54,90%	100,00%
Área de mayor ocurrencia de fraude	a) Compras	18,63%	20,59%	39,22%
	b) Ingresos	6,86%	5,88%	12,75%
	c) Nómina	0,98%	0,00%	0,98%
	d) Inventarios	5,88%	6,86%	12,75%
	e) Partes relacionadas	3,92%	2,94%	6,86%
	f) Efectivo y sus Equivalentes	8,82%	15,69%	24,51%
	g) Elaboración de Estados Financieros	0,00%	2,94%	2,94%
Total fraude financiero por sector		45,10%	54,90%	100,00%

Fuente: Elaboración propia

Se evidencia que el área con mayor ocurrencia de fraude fueron las compras, con un 39,22% donde actividades como sobreprecios, sobornos y reembolsos fraudulentos tomaron impulso en la pandemia. La naturaleza del efectivo y sus equivalentes por tener alto riesgo financiero inherente obtuvo una percepción del 24,51% donde los usuarios indicaron se generaron mayor ocurrencia de actos delictivos.

3.3. El ciberdelito en las organizaciones

La tabla 4, muestra los principales delitos cometidos tanto en el sector público y privado. Se puede observar como la principal tipología de delitos es la manipulación de datos económicos y estafas con un 21,57% que significaron un incremento considerable, generadas en los sistemas de información. Estas fueron perpetradas por individuos que evaden las seguridades para efectuar este tipo de actos ilícitos, con el propósito de ocultar y modificar información con intenciones de beneficiarse.

Tabla 4
Principales ciberdelitos por sector

Principales ciberdelitos	Sectores		Total
	Privado	Público	
Ciber espionaje	3,92%	0,98%	4,90%
Divulgación de información privada	2,94%	0,98%	3,92%
Hackeo de contraseñas, extorsión y chantaje	6,86%	1,96%	8,82%
Manipulación de datos económicos y estafas	13,73%	7,84%	21,57%
Ocultamiento de información	2,94%	3,92%	6,86%
Phishing	8,82%	5,88%	14,71%
Skiming	14,71%	5,88%	20,59%
Virus informáticos	7,84%	10,78%	18,63%
Total percepción de ciberdelitos por sector	61,76%	38,24%	100,00%

Fuente: Elaboración propia.

Así también el skimming *"robo en tarjetas de crédito"*, mostró un considerable incremento dentro de las compras y negocios en línea y dentro de los canales de información empresariales, donde delincuentes internáuticos usaron esta estratagema para defraudar a organizaciones que perdieron valores financieros, donde los usuarios puntuaron con 20,59% este tipo de actos delictivos.

La aparición de virus informáticos se puntuó en 18,63% como un delito que tomó fuerza en la pandemia con el fin de dañar sistemas de información, los mismos que en asociación del phishing *"suplantación de identidad"*, fueron estrategias para robar identidad

en tarjetas de crédito, robo de accesos, adquisición ilícita de contraseñas bancarias y cuentas institucionales, usurpación de identidad en sistemas contables e informáticos, mismos que proliferaron en mayor cantidad debido al auge tecnológico que produjo la pandemia de la COVID-19 y debilitaron los sistemas de información empresariales.

Adicionalmente, los ciberdelitos en el sector privado ecuatoriano se ubican en el 61,76%, sector donde se desenvuelve un gran porcentaje del sector de la salud y de las comunicaciones. Sectores donde aumentó el fraude y donde los principales delitos cibernéticos fueron la manipulación de los sistemas de información y aparición de virus informáticos.

3.4. Causas y medios de detección de las actividades ilícitas

La tabla 5, muestra las causas que originaron fraude financiero y funciones que permitieron detectarlo por sector, entendiendo como detonantes para que se generen actos delictivos la ciberdelincuencia y el fraude financiero. Los resultados señalan que la principal causa fue la ausencia y/o deficiencia de control internos con un 33,33%; por lo que los procesos internos organizacionales fueron vulnerados al no contar con eficientes líneas de actuación en los componentes de Control Interno.

Tabla 5
Causas que originaron fraude financiero y funciones que permitieron detectarlo por sector

Causas / Funciones de detección		Sectores		Total
		Privado	Público	
Causas que originaron fraude	Ausencia y/o deficiencia de Auditoría Interna	11,76%	10,78%	22,55%
	Ausencia y/o deficiencia de Control Interno	17,65%	15,69%	33,33%
	Deficientes líneas de supervisión	0,98%	2,94%	3,92%
	Falta de cultura ética corporativa	4,90%	12,75%	17,65%
	Procesos y procedimientos no definidos	1,96%	1,96%	3,92%
	Sistemas de información ineficaces y vulnerables	7,84%	10,78%	18,63%
Total percepción de fraude por sector		45,10%	54,90%	100,00%
Funciones que permitieron detectar fraude	Actividades de Control Interno	13,73%	11,76%	25,49%
	Auditoría Externa	4,90%	4,90%	9,80%
	Control y gestión de la alta dirección	8,82%	7,84%	16,67%
	Controles externos a la organización	0,98%	2,94%	3,92%
	Denuncias de colaboradores internos	6,86%	12,75%	19,61%
	Funciones de Auditoría Interna	9,80%	14,71%	24,51%
Total percepción de fraude por sector		45,10%	54,90%	100,00%

Fuente: Elaboración propia.

Además, se muestra que otra causa fue la ausencia y/o deficiencia de Auditoría Interna con un 22,55%; cuya función principal es el aseguramiento institucional y la gestión de riesgos, siendo debilitados o ausentes los procesos de control, desembocó en que se generen actividades delictivas. En este contexto y en función a la percepción de los usuarios, se determina que la función de Auditoría Interna y los procesos de control interno son los lineamientos que en mayor medida permitieron detectar actividades ilícitas.

3.5. El ciberdelito y su incidencia en la aparición de fraude financiero

En base al estudio de la prueba no paramétrica *chi-cuadrado* en el software SPSS para las Ciencias Sociales, se realizó el análisis de la asociación de las variables del ciberdelito como medio y actor incidente en la aparición de mayor cantidad de fraudes financieros en la pandemia de la COVID-19. El análisis pretendió establecer diferencias significativas entre las variables nominales, para validar la hipótesis alternativa que presentó esta investigación. La tabla 6, indica el total del procesamiento de los casos, señalando la validez del 100% de los casos, que corresponden a las 102 respuestas obtenidas para cada variable producto de la encuesta aplicada a organizaciones públicas y privadas.

Tabla 6
Resumen de procesamiento de casos prueba chi-cuadrado

Variables / Casos	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
Ciberdelito como actor para fraude financiero * Fraude financiero en la COVID-19	102	100,00%	0,00	0,00%	102	100,00%

Fuente: Elaboración propia en base al análisis obtenido en SPSS.

La tabla 7, muestra la comparación cruzada de las variables del ciberdelito y el fraude financiero, establecidas en SPSS con valores relativos y con su frecuencia expresada en columnas. Los resultados muestran que, según la percepción de los usuarios, el ciberdelito es incidente en el cometimiento de fraudes financieros en un 69,61%; y establece la no incidencia en un 30,39%.

Tabla 7
Ciberdelito como vía para la consecución de fraude financiero, tabulación cruzada

Tabulación cruzada			Fraude financiero en la COVID-19		Total
			No	Si	
Ciberdelito como actor para fraude financiero	No	Recuento	15,00	16,00	31,00
		% dentro de Fraude financiero en la COVID-19	55,56%	21,33%	30,39%
	Si	Recuento	12,00	59,00	71,00
		% dentro de Fraude financiero en la COVID-19	44,44%	78,67%	69,61%
Total		Recuento	27,00	75,00	102,00
		% dentro de Fraude financiero en la COVID-19	100,00%	100,00%	100,00%

Fuente: Elaboración propia en base al análisis obtenido en SPSS.

La tabla 8, presenta el análisis de la prueba no paramétrica chi-cuadrado, señalando los resultados de la hipótesis alternativa en base a los datos de la chi-cuadrado de Pearson y tomando como en referencia para el establecimiento de la asociación de las variables el índice de corrección de continuidad señalados en la tabla. La hipótesis alternativa (H1) establece que la ciberdelincuencia y su tipología fueron instrumentos que generaron se originen mayor número de fraudes financieros en las organizaciones públicas y privadas ecuatorianas. El análisis muestra las diferencias significativas entre la percepción de los usuarios sobre ambas variables (ciberdelito y fraude financiero), conforme el grado de corrección de continuidad, ($x2(1)$ = 9,432, p< 0,05), donde gl = 1 y p = 0,021, en una significancia asintótica (2 caras).

Tabla 8
Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (2 caras)	Significación exacta (2 caras)	Significación exacta (1 cara)
Chi-cuadrado de Pearson	10,991[a]	1	,0009	,0015	0,0013
Corrección de continuidad[b]	9,432	1	,0021		
Razón de verosimilitud	10,440	1	,0012	,0028	0,0013
Prueba exacta de Fisher				,0015	0,0013
N de casos válidos	102,00				

Nota. a. 0 casillas (0,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es 8,21. b. Sólo se ha calculado para una tabla 2x2.
Fuente: Elaboración propia en base al análisis obtenido en SPSS.

Por lo tanto, como el nivel de significación exacta p = 0,021 es menor al de incidencia mínimo establecido de aceptación en las Ciencias Sociales 0,050; se establece la aceptación de la hipótesis alternativa, demostrando que existe asociación efectiva entre las variables del ciberdelito como incidente en el cometimiento de mayor cantidad de fraudes financieros. Adicionalmente, los resultados del análisis chi-cuadrado fueron los adecuados para una tabla de 2X2, denotando que 0 casillas (0,0%) han esperado un recuento menor que 5, lo que indica que esta prueba no paramétrica es suficiente para la adopción de la hipótesis alternativa.

4. Conclusiones

Los ciberdelitos tomaron auge en la pandemia de la COVID-19, debido a que los diferentes controles institucionales no estaban preparados para las medidas que obligatoriamente la pandemia hizo adoptar, como el uso de la tecnología bajo la necesidad de continuar sus operaciones. En este contexto, se incrementaron diversos tipos de ciberdelitos que tomaron fuerza en la pandemia como skimming, phishing, virus informáticos y manipulaciones a los sistemas de información institucionales.

Otros tipos de actividades ilícitas que proliferaron fueron los fraudes financieros, representados principalmente por la alteración de la información financiera, procesos de facturación y compras, y evasión tributaria; todos estos mecanismos abrumaron a las organizaciones tanto del sector público y privado, menoscabando su imagen reputacional, eficiente gestión, afectando inclusive la continuidad de sus actividades.

En la actualidad, empíricamente se determina que existe una asociación entre los ciberdelitos y las pérdidas financieras originadas por los fraudes financieros, sin embargo, no se pudo determinar un estudio como el actual, que demuestre efectivamente la asociación de ambas variables, según la percepción de las unidades directivas y de control institucionales.

Los resultados de esta investigación confirman que los diferentes tipos de ciberdelitos que se presentaron en la pandemia de la COVID-19 fueron incidentes para que se generen mayor número de casos de fraude financiero, los mismos que aparecieron principalmente en el sector público y en las actividades económicas como la salud y el sector de las telecomunicaciones.

Las principales funciones de aseguramiento organizacional frente al fraude financiero y delitos informático deben ser el control interno institucional y la Auditoría Interna, esta última debe ser vanguardista en el control institucional, generando valor agregado a la organización y trabajando en el establecimiento de controles internos eficaces y efectivos, puesto que como se señala en esta investigación fue su deficiente manejo o ausencia, lo que permitió se generen actos delictivos en mayor medida. La lucha contra actividades ilícitas debe ser permanente y más aún cuando el escenario donde se desarrollan las actividades empresariales sigue siendo incierto como resultado de la pandemia de la COVID-19.

Referencias bibliográficas

Albizri, A., Appelbaum, D., & Rizzotto, N. (2019). Evaluation of financial statements fraud detection research: a multi-disciplinary analysis. *International Journal of*

Disclosure and Governance, *16*(4), 206-241. https://doi.org/10.1057/s41310-019-00067-9

Amiram, D., Bozanic, Z., Cox, J. D., Dupont, Q., Karpoff, J. M., & Sloan, R. (2018). Financial reporting fraud and other forms of misconduct: a multidisciplinary review of the literature. *Review of Accounting Studies*, *23*(2), 732-783. https://doi.org/10.1007/s11142-017-9435-x

Association of Certified Fraud Examiners- ACFE (2022). *Report to the Nation on Occupational Fraud and Abuse*. https://acfepublic.s3.us-west- 2.amazonaws.com/2022+Report+to+the+Nations.pdf

Baatwah, S., & Al-Ansi, A. (2022). Dataset for understanding the effort and performance of external auditors during the COVID-19 crisis: A remote audit analysis. *Data in brief*, *42*, 108119. https://doi.org/10.1016/j.dib.2022.108119

Barretto, C., Drumond, G., & Méxas, M. (2022). Remote audit in the times of COVID-19: a successful process safety initiative. *Brazilian Journal of Operations & Production Management*, *19*(3). https://doi.org/10.14488/BJOPM.2021.048

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2020). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies*, *23*(sup1), S47-S59. https://doi.org/10.1080/14616696.2020.1804973

Campedelli, G., Favarin, S., Aziani, A., & Piquero, A. (2020). Disentangling community-level changes in crime trends during the COVID-19 pandemic in Chicago. *Crime Science*, *9*(1), 1-18. https://doi.org/10.1186/s40163-020-00131-8

Chahine, S., Fang, Y., Hasan, I., & Mazboudi, M. (2021). CEO Network Centrality and the Likelihood of Financial Reporting Fraud. *Abacus*, *57*(4), 654-678. https://doi.org/10.1111/abac.12219

Cressey, D. (1961). *The Prison: Studies in Institutional Organization and Change*. Holt.

De La Torre, C. (2018). Gestión del Riesgo Organizacional de Fraude y el rol de Auditoría Interna. *Revista Contabilidad y Negocios*, *13*(25), 57-69. https://doi.org/10.18800/contabilidad.201801.004

De la Torre, C., y Cáceres, G. (2017). Auditoría forense como medio para combatir la corrupción. *Revista Arje*, *11*(21), 88-97. http://www.arje.bc.uc.edu.ve/arj21/art05.pdf

De La Torre, C., y Quiroz, J. (2020). Fraude organizacional. Percepciones previas a la creación de un observatorio del fraude. *Economía coyuntural, 5*(3), 147-183. https://doi.org/10.5281/zenodo.4061902

Deloitte (2021). *Consideraciones de Auditoría Interna en respuesta al COVID-19*. DelloiteSLatam, S.C. https://www2.deloitte.com/content/dam/Deloitte/ec/Documents/strategy/Consideraciones-Auditoria-Interna-COVID19.pdf

Dewi, Y., & Fadjarenie, R. (2020). The effect of fraud specialist role on internal control using the mediation of credit card fraud detection (Case study of a state-owned bank). *International Journal of Scientific and Technology Research*, *9*(2), 6285-6292. http://www.ijstr.org/final-print/feb2020/The-Effect-Of-Fraud-Specialist-Role-On-Internal-Control-Using-The-Mediation-Of-Credit-Card-Fraud-Detection-case-Study-Of-A-State-owned-Bank.pdf

Faraco, F. (2021). Impacto del COVID-19 en la gestión del fraude en entidades financieras. *Deloitte*. https://www2.deloitte.com/es/es/pages/risk/articles/covid-19-gestion-fraude-entidades-financieras.html

Félix, C., & Meza, V. (2021). Riesgos de fraude en el sector minero en tiempos de COVID-19. *Revista Lidera*, (16), 33-38. https://revistas.pucp.edu.pe/index.php/revistalidera/article/view/24851/23639

Galvis, I., & Santos, J. (2017). Geometría del fraude. *Cuadernos de contabilidad*, *18*(45), 74-85. https://doi.org/10.11144/Javeriana.cc18-45.geof

Ge, W., Li, Z., Liu, Q., & McVay, S. (2021). Internal control over financial reporting and resource extraction: Evidence from China. *Contemporary Accounting Research*, *38*(2), 1274-1309. https://doi.org/10.1111/1911-3846.12653

Gerbrands, P., Unger, B., Getzner, M., & Ferwerda, J. (2022). The effect of anti-money laundering policies: an empirical network analysis. *EPJ Data Science*, *11*(1), 15. https://doi.org/10.1140/epjds/s13688-022-00328-8

Gómez, A. (2020). Retorno al trabajo y la COVID-19. *CienciAmérica*, *9*(2), 11-15. https://doi.org/10.33210/ca.v9i2.277

Gottschalk, P., & Gunnesdal, L. (2018). *White-collar crime in the shadow economy: Lack of detection, investigation and conviction compared to social security fraud*. Springer Nature. https://doi.org/10.1007/978-3-319-68916-6_3

Hail, L., Tahoun, A., & Wang, C. (2018). Corporate scandals and regulation. *Journal of Accounting Research*, *56*(2), 617-671. https://doi.org/10.1111/1475-679X.12201

Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amid COVID-19: The initial results from a natural experiment. *American Journal of Criminal Justice*, *45*(4), 546-562. https://doi.org/10.1007/s12103-020-09534-4

Henk, O. (2020). Internal control through the lens of institutional work: a systematic literature review. *Journal of Management Control*, *31*(3), 239-273. https://doi.org/10.1007/s00187-020-00301-4

Huq, A., Hartwig, F., & Rudholm, N. (2022). Do audited firms have a lower cost of debt?. *International Journal of Disclosure and Governance*, *19*(2), 153-175. https://doi.org/10.1057/s41310-021-00133-1

Kasper, M., & Alm, J. (2022). Audits, audit effectiveness, and post-audit tax compliance. *Journal of Economic Behavior & Organization*, *195*, 87-102. https://doi.org/10.1016/j.jebo.2022.01.003

Kazemian, S., Said, J., Nia, E., & Vakilifard, H. (2019). Examining fraud risk factors on asset misappropriation: evidence from the Iranian banking industry. *Journal of Financial Crime*. https://doi.org/10.1108/JFC-01-2018-0008

Lai, T., Lei, A., & Song, F. (2019). The impact of corporate fraud on director□interlocked firms: Evidence from bank loans. *Journal of Business Finance & Accounting*, *46*(1-2), 32-67. https://doi.org/10.1111/jbfa.12362

Loja, L. (2021). Delitos contra la eficiencia de la administración pública y la auditoría forense en el Ecuador. *Universidad Católica de Cuenca.* https://dspace.ucacue.edu.ec/bitstream/ucacue/12072/1/LUIS%20PATRICIO%20LOJA%20

GUALLPA.pdf

Lu, N., Zhang, Y., Shi, W., Kumari, S., & Choo, K. (2020). A secure and scalable data integrity auditing scheme based on hyperledger fabric. *Computers & Security*, *92*, 101741. https://doi.org/10.1016/j.cose.2020.101741

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, *29*(3), 306-321. https://doi.org/10.1080/0960085X.2020.1771222

Nordin, I. (2022). Narratives of internal audit: The Sisyphean work of becoming "independent". *Critical Perspectives on Accounting*, 102448. https://doi.org/10.1016/j.cpa.2022.102448

Qiu, S., Luo, Y., & Guo, H. (2021). Multisource evidence theory based fraud risk assessment of China's listed companies. *Journal of Forecasting*, *40*(8), 1524-1539. https://doi.org/10.1002/for.2782

Ramos, M., Sánchez, A., & Blázquez, F. (2019). Research topics in accounting fraud in the 21st century: A state of the art. *Sustainability*, *11*(6), 1570. https://doi.org/10.3390/su11061570

Rakipi, R., De Santis, F., & D'Onza, G. (2021). Correlates of the internal audit function's use of data analytics in the big data era: Global evidence. *Journal of International Accounting, Auditing and Taxation*, *42*, 100357. https://doi.org/10.1016/j.intaccaudtax.2020.100357

Rose-Ackerman, S. (2021). Corruption and COVID-19. *Eunomía: Revista en Cultura de la Legalidad*, (20), 16-36. https://doi.org/10.20318/eunomia.2021.6062

Salazar, J. (2021). La crisis por el Covid-19: 19 riesgos generados. *EY Building a better working world*. https://www.ey.com/es_ec/forensic-integrity-services/la-crisis-por-el-covid19--19-los-riesgos-generados

Solomón, D., & Soltes, E. (2021). Is "not guilty" the same as "innocent"? Evidence from SEC financial fraud investigations. *Journal of Empirical Legal Studies*, *18*(2), 287-327. https://doi.org/10.1111/jels.12282

Steinbart, P., Raschke, R., Gal, G., & Dilla, W. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society*, *71*, 15-29. https://doi.org/10.1016/j.aos.2018.04.005

The Institute of Internal Auditors- IIA (2020). *Definition of Internal Auditing.* Sitio web de theiia.org: https://global.theiia.org/standards-guidance/mandatoryguidance/Pages/Definition-of-Internal-Auditing.aspx

Weekes-Marshall, D. (2020). The role of internal audit in the risk management process: A developing economy perspective. *Journal of Corporate Accounting & Finance*, *31*(4), 154-165. https://doi.org/10.1002/jcaf.22471

Werner, M., Wiese, M., & Maas, A. (2021). Embedding process mining into financial statement audits. *International Journal of Accounting Information Systems*, *41*, 100514. https://doi.org/10.1016/j.accinf.2021.100514

Westerski, A., Kanagasabai, R., Shaham, E., Narayanan, A., Wong, J., & Singh, M. (2021). Explainable anomaly detection for procurement fraud identification—lessons from practical deployments. *International Transactions in Operational Research*, *28*(6), 3276-3302. https://

doi.org/10.1111/itor.12968

Wu, H., Chang, Y., Li, J., & Zhu, X. (2022). Financial fraud risk analysis based on audit information knowledge graph. *Procedia Computer Science*, *199*, 780-787. https://doi.org/10.1016/j.procs.2022.01.097