FOTRIEM TU META ES, NUESTRA META

Revista de ciencias empresariales, tributarias, comerciales y administrativas, Vol.1. N°2
Julio-Diciembre, 2022: 225-245
Doi: 10.58287/rcfotriem-1-2-2022-23
Artículo Original/Original Article
ISSN (online): 2958-2539 - ISSN (impreso): 2958-2520

Análisis de los riesgos por mitigar a través de la auditoría en operaciones electrónicas en Paraguay al 2022

Analysis of risks to mitigate through audit in electronic operations in Paraguay by 2022

Oñehesay`îjo umi riego ojejapo mitigasion rupive ha auditoria operasiones elektronikas Paraguáipe ary 2022- pe

Nélida Elena Zárate Arce* *https://orcid.org/0009-0006-3127-2246*
Instituto Superior de Formación Tributaria, Comercial y Administrativa (FOTRIEM). Asunción, Paraguay

Como citar:
Zarate Arce, N. E. (2022). Análisis de los riesgos por mitigar a través de la auditoría en operaciones electrónicas en Paraguay al 2022. *Revista de ciencias empresariales, tributarias, comerciales y administrativa*, 1(2), 225-245. https://doi.org/10.58287/rcfotriem-1-2-2022-23

Resumen
Si bien las operaciones electrónicas en Paraguay habían comenzado un proceso de adopción en el país, con la pandemia, la innovadora práctica experimentó una aceleración hasta acompañar e inyectar dinamismo al mercado. Además, se genera un cambio de hábito en los consumidores, quienes experimentan cada vez más los canales digitales para realizar compras y pagos de servicios, entre otros. Igualmente, las alternativas de pago también son un importante diferenciador en los canales de venta, brindan mayor transparencia y trazabilidad en transacciones y, se caracterizan por ofrecer rapidez e inmediatez al momento de realizar las operaciones, en el país se cuenta con un Marco legal Ley N° 6.822/2021 "De los servicios de confianza para las transacciones electrónicas, del documento electrónico y los documentos transmisibles electrónicos, Ley 4595/12 "Sistemas de Pagos y Liquidación de Valores, Ley N° 1015/1997 "Previene y Reprime los Actos Ilícitos Destinados a la Legitimación de Dinero o Bienes, tipifica el delito de lavado de dinero o bienes", Resolución N° 6 de fecha 13 de marzo de 2014 que aprueba el reglamento de los pagos electrónicos; asimismo con el aumento de estas operaciones en el sistema financiero digital en nuestro país aún no existe una gestión de riesgos asociados con las implementaciones de Operaciones Electrónicas en general, por lo que surge la siguiente pregunta: ¿Cómo se mitigan los riesgos a través de la auditoría en operaciones electrónicas en Paraguay año 20220? Entre las principales conclusiones a las que llega este estudio, es la importancia que toda entidad que opera a través de la modalidad electrónica identifique los riesgos existentes para reducir el impacto que pudiesen generar en las empresas; también que las operaciones electrónicas requieren que el auditor contable esté consciente que es necesario utilizar la tecnología de información para el desarrollo pleno de la profesión, ya que se considera una herramienta que les ayuda a profundizar su trabajo y a mejorar el alcance en sus procedimientos.
Palabras clave: Operaciones electrónicas, Servicios digitales, Riesgos, Lavado de dinero, Pagos electrónicos.

Abstract
Although electronic operations in Paraguay had begun a process of adoption in the country, with the pandemic, the innovative practice experienced an acceleration to accompany and inject dynamism into the market. In addition, a change of habit is generated in consumers, who increasingly experience digital channels to make purchases and pay for services, among others. Likewise, payment alternatives are also an important differentiator in sales channels, they provide greater transparency and traceability in transactions and are characterized by offering speed and immediacy at the time of carrying out operations, in the country there is a Legal Framework Law No. 6,822/2021 "On trust services for electronic transactions, electronic documents and electronic transferable documents, Law 4595/12 "Securities Settlement and Payment Systems, Law No. 1015/1997 "Prevents and Suppresses Illicit Acts Destined to the Legitimation of Money or Goods, typifies the crime of money or goods laundering", Resolution No. 6 dated March 13, 2014, which approves the regulation of electronic payments; Likewise, with the increase of these operations in the digital financial system in our country, there is still no risk management associated with the implementation of Electronic Operations in general, for which the following question arises: How are the risks mitigated through the audit in electronic operations in Paraguay year 2022?; For which, a qualitative approach, documentary design, analytical level is applied, using documentary analysis as a collection technique, with the use of documentary analysis sheets, and critical and compara-

Autor correspondiente: *nelida.z@hotmail.com*
Recibido: 20/09/2022 Aceptado: 12/10/2022

tive reading is used as an analysis technique. Among the main conclusions reached by this study is the importance that every entity that operates through the electronic modality identifies the existing risks to reduce the impact that they could generate in the companies; also that electronic operations require that the accounting auditor be aware that it is necessary to use information technology for the full development of the profession, since it is considered a tool that helps them deepen their work and improve the scope of their procedures
Keywords: Electronic operations, digital services, risks, money laundering, electronic payments.

Ñemombyky
Umi oprasiones elektronika ojeguerekóva Paraguaípe ojapokuri peteî proseso ñane retâme, pe pandemia ndive pe tembiaporâ ohechauka mba`éichapa imbarete ha avei ojehecha pirirî ñemuha rupi. Ha upéicha oogueru pe kambio orekóva umi konsumidorKuéra, ha`ekuéra oipurúve ára ha ára umi kanal digital ojepo haguâ mba`e jejogua ha avei jehepyme`ê pe servisio rupive, ambue mba`e ha oî pe ñembojoja ha heta laja ikatu ojepo umi pago, ha katu oreko avei mba`éichapa ndojojái umi kanal ojapóva jehepyme`ê, ome`ê avei tesakâ pe transparensia transasional ha mba`eichaitepa ipy`ae pe maba`e ojejapóva operasiones rupi, ñande retâme jaguereko peteî marko legal Léi Nº 6822/2021 Oñangarekóva umi servisio transasion elektronika rehegua, ha umi Kuatiakuéra elektroniko pe lèi Nº 4595/12 "Sistema oñehepyme`êha umi pago ha avei pe liquidasion orekóva valores.Léi Nº1015/1997 Omboguevi umi Aktos Ilisito Destinados pe Ligitimasion orekóva pirapire ha upéva otipifika pe delito ajapóva pirapire jejohéi pe Resolusion Nº 6 arange 13 jasyapy ary 2014- pe. Péva ojapo peteì norma ikatuhaguaicha ojeipuru pe pago elektroniko, péicha avei ombotuicháve ko operasion oipurúva pe sistema digital ñane retâme ndojeguerekombeterei pe gestión oîva atýpe guasúpe ha oipurúva pe implementasion operasiones elektronika, ha upévare ojejapo kóva ko porandu ¿Mba`éichapa ikatu oñemitiga umi riesgo auditoria ojejapóva operasiones elektronika Paraguaípe ary 2022- pe. Oñemohu`âme ko tembiapo ikatu oje`e ko`ápe ojehecha moôpa oguahê ha maba`éichapa oiporypytyvô opavave empresape oipurúava umi servisio elektroniko. Kóva rupive ikatu oñemomichîve umi riesgo empresa rupi, avei ikatu oje`e pe teKnologia ha`eha peteî herramienta oipurutáva pe auditor ikahaguâ omombaretéva haguâ pe hembaipo ojapóva ha ojupyty haguâ ohupytyséva.
Ñe`êkuaarâ: Operasiones Elektronika, Servisio Digital, Riesgos, Pirapire jejohéi, Pago elektroniko.

1. Introducción

En última década se ha visto un incremento en los servicios financieros digitales o electrónicos que tienen por objetivo atender a las poblaciones desbancarizadas en mercados emergentes. Individuos de bajos ingresos, microempresarios y poblaciones rurales que anteriormente habían sido excluidos del mercado debido a los altos costos de la expansión física, están teniendo acceso a servicios financieros a través de teléfonos móviles y redes de corresponsales que actúan como representantes de proveedores de servicios financieros. Esto ha resultado en un aumento asombrosamente rápido en la inclusión financiera en la gran mayoría de los países. (Servicios Financieros Digitales, 2016)

Sin embargo, con las amplias oportunidades ofrecidas por nuevas tecnologías y las operaciones de negocios innovadores, también vienen nuevos riesgos. Los riesgos relacionados con la implementación de los servicios financieros digitales se extienden mucho más allá de los riesgos operacionales y técnicos. Para que la industria de la inclusión financiera pueda capitalizar plenamente los beneficios de los servicios financieros digitales, es importante que los riesgos asociados sean entendidos y abordados en forma adecuada. El ritmo de las mejoras tecnológicas y la penetración de los teléfonos inteligentes determinará cómo se desarrollarán y ofrecerán los servicios al mercado, y las regulaciones seguirán cambiando según las dinámicas del mercado. (Servicios Financieros Digitales, 2016)

En Paraguay, Las Entidades de Medios de Pagos Electrónicos (EMPES) son sistemas que permiten hacer giros (envíos y recepción de efectivo) a través de celulares, ya sea solo con el número de la compañía telefónica o a través de aplicaciones, además de pagos de servicios y recarga de saldos. Este servicio se caracteriza por la facilidad y practicidad para operar en cualquier parte del país,

sin muchos requisitos. (Mendez Fiorella, 2021)

Las transferencias o envíos de dinero se realizan desde hace años a través de bancos y financieras, ya sea por transferencias bancarias o depósitos. Mediante el modelo de negocio de las EMPES, se posibilita estas operaciones a agentes que no son participantes del rubro bancario y financiero Desde diciembre del 2020, el Banco Central del Paraguay (BCP) ha incluido a las EMPES en el Boletín Estadístico Mensual, en el que se evidencian los datos como distribución geográfica por establecimiento de EMPES, los flujos de dinero de cada mes y cómo es utilizado, así como la cantidad de cuentas existentes y las variaciones mensuales

A inicios de la pandemia, las consecuencias de la crisis económica del coronavirus afectaron a trabajadores independientes, por cuenta propia e informales. En este contexto, se estableció el pago de subsidios gubernamentales a través de estas billeteras electrónicas, lo cual generó un incremento de clientes y de uso de este servicio. Cabe destacar que estas entidades también cuentan con un marco regulatorio establecido por el BCP y son sujetos obligados para la Secretaría de Prevención de Lavado de Dinero o Bienes SEPRELAD. Entre las normativas establecidas se encuentra el límite territorial, de saldo y operaciones, detección y reporte de operaciones, entre otras. (Mendez Fiorella, 2021)

Por lo expuesto, surgen las inquietudes por las cuales en nuestro país aún no existe una gestión de riesgos asociados con las implementaciones de Operaciones Electrónicas en general, por lo que surge la siguiente pregunta: ¿Cómo se mitigan los riesgos a través de la auditoría en operaciones electrónicas en Paraguay año 2022?

2. Descripción de riesgos de los instrumentos financieros electrónicos en las empresas

2.1. Riesgo Operacional

El riesgo operativo se genera del potencial de pérdida debida a deficiencias importantes en la confiabilidad e integridad del sistema. Los aspectos de seguridad son de la mayor importancia, ya que los bancos pueden sufrir ataques externos o internos a sus sistemas o productos. El riesgo operativo puede generarse también por el mal uso de los clientes, por sistemas de banca electrónica y dinero electrónico mal diseñados o ejecutados. Muchas de las manifestaciones específicas posibles de estos riesgos, se aplican tanto a la banca electrónica, como al dinero electrónico. (Basilea, 1998)

2.2. Riesgo Tecnológico

El riesgo tecnológico se genera en relación con los controles del acceso a los sistemas contables y de gestión de riesgos de la banca electrónica, a la información que transmite a terceros y, en el caso de dinero electrónico, las medidas que utiliza el banco para detectar y controlar dinero falso. Controlar el acceso a los sistemas de los bancos se ha vuelto cada vez más complejo, en vista del crecimiento de las capacidades de los sistemas de computación, la dispersión geográfica de los puntos de acceso y el uso de varias vías de comunicación, incluyendo redes públicas, como ser el Internet. Es importante hacer notar que, en el caso de dinero electrónico, una violación de seguridad puede dar como resultado la creación fraudulenta de obligaciones del banco. En el caso de otras formas de banca electrónica, el acceso no autorizado puede conducir a pérdidas directas, un incremento de las obligaciones de los clientes y otros problemas. (Basilea, 1998)

2.3. Riesgo Reputacional

El Riesgo Reputacional puede surgir a causa de problemas en las redes de comunicación, fallas técnicas de los sistemas que impidan a los clientes el acceso a sus fondos, o información sobre las cuentas, particularmente si no existen alternativas a este acceso. Así, por ejemplo, si una de las EMPES experimenta un daño importante a su reputación relacionado alguna alteración en sus sistemas que pueda resultar en la incapacidad de poder cumplir con sus obligaciones al momento de la realización de los pagos, la seguridad de los sistemas puede también ser cuestionada por los usuarios. En circunstancias extremas, una situación de esta naturaleza puede conducir a interrupciones sistémicas en las operaciones electrónicas en general. (Basilea, 1998)

2.4. Riesgo de Fraude

El fraude es un riesgo importante para los Servicios Financieros Digitales y es causa de mucha preocupación para los proveedores de Servicios Financieros Digitales. El riesgo de fraude es:

Multifacético y se relaciona con varios otros riesgos. El riesgo operacional y tecnológico puede causar riesgo de fraude y el fraude puede conducir a un riesgo financiero. El fraude también es un factor importante de riesgo reputacional. Grandes casos de fraude en dinero electrónico se han reportado en los últimos años que han causado daños financieros de millones de dólares. Estos han sido debido al fraude de clientes, corresponsales y empleados al crear cuentas fantasmas y realizar transacciones fraudulentas. Han sido robados fondos a proveedores, corresponsales y clientes. El fraude puede tener un gran impacto en la reputación de una institución y en la industria en su conjunto. Si los fondos son robados de cuentas de clientes por culpa del proveedor, los proveedores deben asegurarse de que los fondos se devuelven a los clientes de inmediato.

El proceso de prevención del fraude incluye el desarrollo de evaluaciones para entender dónde se puede detectar y prevenir el fraude, determinar el apetito de riesgo y establecer controles efectivos. En general, el fraude puede definirse como fraude mayor, que implica sumas muy grandes y generalmente se realiza contra la institución financiera, a menudo por parte del personal y el fraude menor, que involucra a corresponsales o clientes como víctimas o autores y sumas menores de dinero.

Hay muchas razones por las que las personas cometen fraude, pero un modelo común para juntar a una serie de estas es El Triángulo del Fraude. La premisa es que el fraude es probable que resulte de una combinación de tres factores generales: Presión (o motivación para cometer fraude); Oportunidad (típicamente debido a sistemas o procesos deficientes) y Racionalización (típicamente que no serán atrapados). (Servicios Financieros Digitales, 2016)

2.5. Riesgo Legal

Este riesgo hace referencia a un marco legal deficiente, del mismo modo cuando se realizan incumplimientos de las leyes, decretos, resoluciones o prácticas establecidas, o cuando los derechos y obligaciones legales de las partes de una transacción no están bien definidos. Dicho lo anterior los medios de pagos electrónicos son los más utilizados en el país desde los últimos años, precisamente posterior a la pandemia, consideremos ahora que los sistemas de dinero electrónico pueden ser atractivos para el lavado de dinero cuando ofrecen límites flexibles de saldos y disponen una posibilidad limitada de auditoría de las transacciones. La banca electrónica puede ser conducida a

distancia, los bancos pueden enfrentarse a mayores dificultades para aplicar métodos tradicionales de prevención de lavados de activos y detección de la actividad criminal. (Basilea, 1998)

2.6. Identificación de los Riesgos

Las operaciones electrónicas se considera actualmente una nueva unidad estratégica dentro del negocio de la banca tradicional, es imposible realizar una lista exhaustiva de los riesgos debido a los cambios rápidos de la tecnología de la información.

> A continuación, se describe una serie amplia y representativa de riesgos que sirva de base para una orientación general de la gestión de riesgos. Además de los ataques externos a los sistemas informáticos, las empresas se exponen frecuentemente a riesgos operativos relacionados con fraudes de empleados, podrían recuperar datos de autenticación a fin de acceder a las cuentas de clientes, o robar tarjetas de valor almacenado. Los errores involuntarios de los empleados pueden también comprometer los sistemas electrónicos. (Basilea, 1998)

2.7. Factores e indicadores de riesgo

Según la Guía General de la SEPRELAD 2020 presenta Guía General Antilavado de Activos y Contra el Financiamiento del Terrorismo para orientar a los Sujetos Obligados y para evaluar la exposición al riesgo respecto de cada factor deberán considerarse, entre otros elementos, los siguientes:

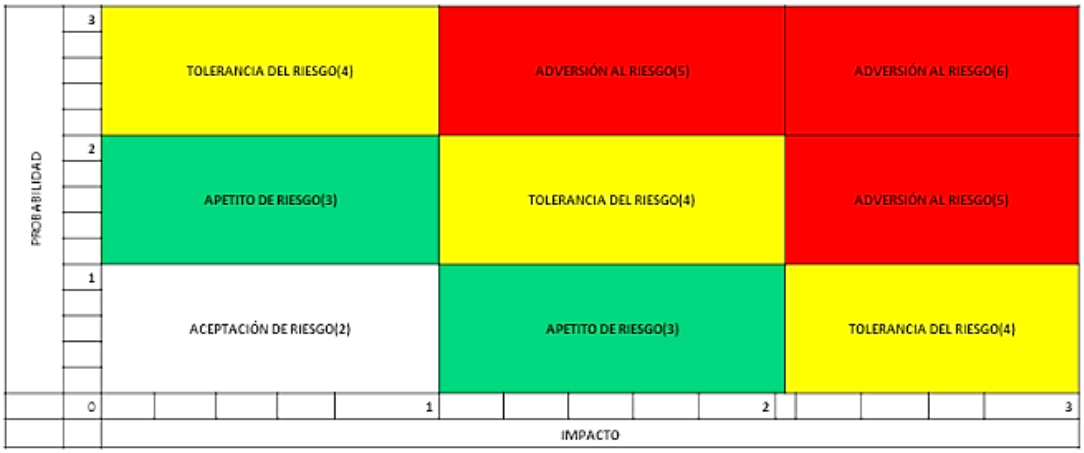
Se consideran a los clientes como criterio general, la admisión de un cliente requiere la adecuada acreditación de su identidad y la recopilación de los datos necesarios para la asignación de un perfil que establezca el nivel de riesgo, lo que, a su vez, determinará el procedimiento de debida diligencia aplicable a cada caso en concreto. En primer lugar y, en función a la información obtenida, se deberá realizar un primer análisis para descartar que el potencial cliente represente algún supuesto que requiera especial atención, como ser, de manera ejemplificativa, la utilización de un nombre ficticio, o la determinación de que este actúa por cuenta de otra persona. Verificada la identidad del cliente, se establecerá la calificación que corresponda, la asignación del perfil y el nivel de debida diligencia que, en principio, será administrado. Una vez que la relación comercial se encuentre en curso, corresponde establecer la periodicidad con la que se actualizarán los datos, a fin de comprobar que no existan causales que ameriten la recalificación del cliente, la aplicación de procedimientos específicos, o incluso en algunos casos, la conclusión de la relación comercial ya iniciada.

2.8. Medición de los riesgos

Una vez individualizados los factores e indicadores de riesgo, el siguiente paso consiste en asignarles una cuantificación, en atención a la importancia que le es atribuida de manera consistente con la descripción y comprensión de las probabilidades de materialización del riesgo. El método escogido deber ser lo suficientemente flexible, de modo a que permita ajustarlo cuando la dinámica operacional así lo amerite. Para medir o evaluar el riesgo, los SO deben establecer un rango o escala de calificación a cada indicador. A modo de ejemplo, una herramienta básica para realizar una medición puede ser implementada a través de una Matriz de Riesgos del tipo 3x3, constituida sobre 3 niveles para la probabilidad de ocurrencia del hecho y la gravedad del impacto para el SO. (SEPRELAD, Guía Anti Lavado de Activos y Lucha contra el Terrorismo, 2020)

Dicho modelo puede aplicarse para el mapeo de los riesgos ya sea de manera individual o en conjunto, de acuerdo con la metodología adoptada y los factores aplicables. (SEPRELAD, Guía Anti Lavado de Activos y Lucha contra el Terrorismo, 2020)

Figura 1. Ejemplo de Matriz de Riesgo 3x3



Fuente: Guía General ALA/CFT 2020.

Figura 2. Ejemplo de medición conforme a la Matriz de Riesgos puede ser la siguiente

RIESGO	MEDICIÓN	POLITICA DE RIESGOS
	0 a 2	ACEPTACIÓN DEL RIESGO
BAJO	2,1 a 3	APETITO DE RIESGO
MEDIO	3,1 a 4	TOLERANCIA DEL RIESGO
ALTO	4,1 a 6	ADVERSIÓN AL RIESGO

Fuente: Guía General ALA/CFT 2020.

Es importante recalcar que las recomendaciones internacionales y las reglamentaciones de SEPRELAD no prescriben una metodología para la realización de las autoevaluaciones, ni una determinada herramienta de apoyo, razones por las cuales su diseño, así como la política de gestión de los riesgos, son realizados por el SO. Los SO deben documentar adecuadamente el proceso, el resultado de su medición o evaluación y el porqué de la asignación del rango, así como las áreas que han proporcionado los datos analizados. (SEPRELAD, 2020)

2.9. Estrategias de mitigación del Riesgo

Servicios Financieros Digitales (2016) en su apartado referente a las estrategias para mitigar los riesgos describe que:

> Con base en los umbrales de aceptación de riesgos establecidos en el proceso de planific - ción, el equipo del proyecto ahora podrá identificar qué riesgos serán tolerados, tratados,

transferidos o terminados. Los riesgos con baja probabilidad y bajo impacto son propensos a ser tolerados y no se requiere ninguna acción adicional. Para aquellos riesgos que requieren tratamiento, transferencia o terminación, se debe desarrollar una estrategia, a continuación, se expone el análisis de algunos riesgos más importantes:

Tabla 1. Riesgo Operacional

Riesgo	Descripción	Tipo de Institución	Opciones de Política y Posibles Herramientas de Mitigación	Indicador Clave de Riesgo
Tarjeta SIM o teléfono móvil perdidos	El cliente no puede realizar transacciones debido a la pérdida de tarjeta de débito o tarjeta SIM.	Cualquiera	Políticas de sustitución de tarjetas. Call center para informes y resolución de problemas. Formación de corresponsales para proporcionar un servicio al cliente de primer nivel.	Tasas de sustitución de tarjetas Tasa de restablecimiento del PIN
Falta de manuales operativos y procesos de negocio	Los manuales de operación están incompletos, carecen de los procesos de excepción y no se actualizan regularmente, lo que resulta en que se sigan procedimientos inadecuados de operación	Cualquiera	Revisar el manual de operación en relación con la lista de procedimientos que se están llevando a cabo. Agregar cualquier procedimiento que falte, actualizando los procedimientos existentes según sea necesario y agregando los casos de uso de excepciones a todos. Asegúrese que los departamentos pertinentes firmen cada proceso Crear listas de verificación de procesos y asegurar que todos los procesos han sido documentados y actualizados si es necesario, y circulados al personal relevante.	Auditoría interna Revisiones de Riesgo y Cumplimiento Tiempo tomado para resolver disputas
Falta de auditorías operativas	Los procedimientos operativos actuales no están optimizados con respecto a la conciliación y procesamiento de ingresos.	Cualquiera	Es necesario realizar auditorías de riesgos para identificar problemas y garantizar la eficiencia e integridad operativas.	Auditoría interna Revisiones de Riesgo y Cumplimiento
Reestablecimiento de PINs	Los procedimientos de restablecimiento de PINs prolongados o complicados producen una mala experiencia del cliente	Cualquiera	Políticas eficaces para los procedimientos de restablecimiento de PIN	Tiempo tomado para resolver restablecimientos de PINs
Débito sin desembolso (DWD)	Cuando un cajero automático debita una cuenta de un cliente, pero no dispensa el efectivo correspondiente causando retrasos en el reembolso al cliente.	Cualquiera usando tarjetas habilitadas para cajeros automáticos	Profundizar en las relaciones con los sistemas de liquidación interbancaria para las transacciones fuera de la red. Mejorar los procedimientos operativos para las resoluciones. Aumentar los recursos humanos dedicados a la resolución de disputas. Actualizar cajeros automáticos.	Número de incidentes
Falta de controles internos, informes internos y monitoreo de datos	No hay procedimientos para supervisar la actividad del corresponsal, empleado o cliente. Incumplimiento potencial a los requisitos reglamentarios.	Cualquiera	Implementar controles internos para monitorear la actividad transaccional y de la entidad, a través de reportes internos y monitoreo de datos.	Auditoría interna Revisiones de Riesgo y Cumplimiento
Procesos de conciliación	Falta de procedimientos eficaces de conciliación que crean atrasos	Cualquiera	Tener procesos de conciliación eficientes claramente definidos que sean idealmente automatizados.	% de montos no conciliados Tiempo de conciliación
Errores de entrada de datos	Errores de entrada de datos, errores tipográficos, errores de digitación realizados por el personal del proveedor de back office.	Cualquiera	Utilizar separación de funciones para realizar tareas. Separación de funciones	Controles de conciliación Auditoría interna

Fuente: Servicios financieros digitales y Gestión de riesgo

Tabla 2. Riesgo Tecnológico

Riesgo	Descripción	Tipo de Institución	Opciones de Política y Posibles Herramientas de Mitigación	Indicador Clave de Riesgo
El cliente no puede acceder a la cuenta debido a la falta de disponibilidad del sistema y/o falla de la transacción.	El cliente no puede acceder a la cuenta a través de la aplicación o corresponsal debido a: La red móvil no está disponible El sistema del proveedor está sufriendo interrupciones temporales del sistema.	Cualquiera	El proveedor debe probar la disponibilidad de transacciones de punto a punto de forma periódica. Todas las interfaces de transacciones están definidas con límites claros de terminación, permitiendo así procedimientos claros de reversión en caso de incertidumbre. Acuerdos de nivel de servicio con proveedores y socios del sistema, y sanciones por incumplimiento Procesos acordados de escalamiento para resolver problemas. Actualizaciones del sistema. Utilizar USSD como respaldo a un POS habilitado con 3G para reducir la dependencia en la conectividad de datos	Tasa de éxito de transacciones de punto a punto
Malware	Los virus, troyanos o gusanos infectan archivos, obtienen acceso remoto, instalan software malicioso para robar datos, realizan transacciones no autorizadas o bloquean el uso autorizado.	Cualquiera	Utilizar una combinación de software antivirus, fire walls, sistemas de detección de intrusiones, servidores proxy, contenido web, filtros de adjuntos de correo electrónico y técnicas de encripción de datos. Desarrollar procedimientos para que el personal, corresponsales y clientes denuncien actividades sospechosas.	Informes de ataques exitosos en el servicio
Repetición de transacciones por la red	Los MNOs a menudo tienen solicitudes de reintento automático para entregar un SMS a un destino si no se tiene éxito en el primer intento. Cuando se utilizan en transacciones de dinero electrónico, algunos sistemas pueden interpretar esto como solicitudes de transacciones múltiples.	Cualquiera usando aplicaciones SMS	Deshabilitar peticiones de reintento. Utilizar recibos de SMS para las transacciones de los clientes con el objetivo de supervisar si hay duplicados	Informes del sistema sobre transacciones duplicadas
Retrasos de transacciones	Las demoras del sistema pueden causar retrasos en las transacciones o recibir recibos de SMS.	Cualquiera	Limitar la capacidad del sistema para reintentar las transacciones. Educar a los corresponsales y clientes para hacer revisiones de saldo si no reciben una confirmación vía SMS inmediatamente.	Quejas de transacciones duplicadas Llamadas a atención al cliente sobre SMS no recibidos
Fallos de hardware	Los dispositivos POS fallan debido a la mala construcción o incapacidad para conectarse al software	Banco, IMF o Proveedor de Servicios de Pago	Acuerdo de nivel de servicio con proveedores de hardware, incluyendo sanciones por incumplimiento. Acuerdo de mantenimiento con el proveedor de hardware.	Tasa de fallos de la transacción Tasa de fallos de POS
Pérdida de datos	Falla del almacenamiento principal y de la instalación de respaldo (incluidos los sistemas basados en la nube), lo que resulta en la pérdida de registros de transacciones.	Cualquiera	Proporcionar bases de datos espejo, separadas para documentar todas las transacciones en tiempo real. Exporte la información de transacciones al almacenamiento con regularidad.	Registros de transacciones perdidos
Fallo de entorno de hosting	El sistema no está disponible debido a problemas técnicos con el entorno de hosting de Servicios Financieros Digitales	Cualquiera	Auditoría técnica y financiera regular del entorno de hosting y del proveedor. Uso de acuerdos de nivel de servicio con el proveedor de hosting yde almacenamiento. Uso del software cloud-watch para monitorear la salud del proveedor de la nube. Procedimientos documentados para fallos de servicio y recuperación de desastres.	Disponibilidad del sistema Número de interrupciones Tiempo necesario para recuperarse de las interrupciones

Fuente: Servicios financieros digitales y Gestión de riesgo

Tabla 3. Riesgo de Fraude

Riesgo	Descripción	Tipo de Institución	Opciones de Política y Posibles Herramientas de Mitigación	Indicador Clave de Riesgo
Suplantación del proveedor o corresponsal	Un individuo se presenta como empleado o corresponsal del proveedor y acepta depósitos o logra acceso no autorizado a cuentas de clientes para llevar a cabo actividades fraudulentas.	Cualquiera	Educar a los clientes para que reciban una confirmación por SMS antes de entregar dinero en efectivo. Campañas de educación del cliente para identificar corresponsales válidos y mantener el PIN en secreto. Call centers para reclamaciones de clientes. Liberar escalamiento del cliente y el proceso de retroalimentación para reportar casos de fraude y activar la sensibilización del mercado sobre el fraude. Reconciliaciones diarias de pagos y recibos contra sistemas internos. Marca de corresponsal clara y consistente.	Registros de incumplimiento por parte de los administradores de corresponsales
Phishing	Los estafadores se presentan como representantes oficiales de corresponsales o proveedores para obtener acceso a PINs, capacidades de cuentas, registros de transacciones o saldos de cuentas de corresponsales o clientes.	Cualquiera	Minimizar la información reportada en los informes de transacciones sólo a lo que es absolutamente necesario. Solicitar a los clientes que denuncien cualquier amenaza y fraude a las autoridades policiales. Campañas de concienciación para educar a los corresponsales y clientes sobre la seguridad de las cuentas y mantener secretos el PIN, etc. Desarrollar procedimientos y directrices claros para la identificación, comunicación y gestión del fraude.	Registros de incumplimiento por parte de los administradores de corresponsales
Cambio de SIM	La tarjeta SIM de un cliente (o corresponsal) se cambia por una nueva sin autorización. El titular de la tarjeta SIM puede acceder a la cuenta del cliente y realizar transacciones sin su conocimiento.	Cualquiera que utilice Dispositivos Móviles	Documentar un proceso claro de intercambio de SIMs que limita a las personas/organizaciones que pueden realizar intercambios de SIM y establecer límites de tiempo entre el momento en que se realiza el intercambio de SIM y el momento en que se implementa. Mantener un registro de los cambios realizados a través de informes.	Registros de incumplimiento por parte de los administradores de corresponsales
Fraude de comprobates	Los comprobantes y códigos de transacción que se generan para permitir pagos a los comerciantes para bienes predefinidos o para retiros de efectivo, son robados y utilizados sin autorización.	Cualquiera	Desarrollar procesos claros que definan la generación de soportes, plazos de vencimiento y notificaciones al vencimiento. Los soportes no deben ser visibles para nadie, excepto para el destinatario y, cuando se extravía, el destinatario puede notificar al negocio y obtener los nuevos reeditados directamente. Preferentemente, en el caso de clientes no registrados, deben registrarse antes de acceder a los fondos.	Quejas de clientes
Cliente defraudado por el corresponsal				
Cuotas no autorizadas	El corresponsal puede cobrar excesivamente o cobrar una tarifa de efectivo adicional no autorizada al consumidor.	Cualquiera	Los proveedores usan contratos claros que revelan completamente todos los cargos que se cobrarán, adaptados a las diversas situaciones de los clientes, incluyendo diferentes idiomas y analfabetismo. Los cargos de servicio están claramente publicados en la ubicación de cada corresponsal. Divulgaciones razonablemente comprensibles para todos los grupos de clientes.	Quejas de clientes

Fuente: Servicios financieros digitales y Gestión de riesgo

3. Examen de los aspectos generales y los alcances de las operaciones electrónicas

3.1. Operaciones Electrónicas

El cambio tecnológico que se viene sucediendo en las últimas décadas en nuestras sociedades está teniendo un elevado impacto en el ámbito financiero. Desde el punto de la demanda, se evidencia un constante proceso de adquisición de competencias digitales para la gestión de las finanzas. Desde el lado de la oferta también se aprecia un considerable esfuerzo de las entidades bancarias por adaptar sus modelos de negocio a una economía digital. En ambos casos, la pandemia de la COVID-19 no ha hecho sino acelerar dicho proceso. Por lo que respecta a la demanda, diversos

estudios han examinado cómo se produce este tipo de digitalización.

Según (Carbo Valverde et.al, 2020) manifiestan que la adopción de la banca digital se produce a través de:

> Servicios basados en información (por ejemplo, consulta del saldo de la cuenta corriente), todo ello condicionado a que el consumidor sea consciente del abanico de servicios que ofrece la banca online. La realización de actividades transaccionales (pagos o transferencias) ocurre solamente tras el asentamiento de la frecuencia de uso por motivos informativos.

Actualmente, se han incrementado el acceso a tecnologías de la información y comunicación, sumados a los efectos de la pandemia COVID-19 y las restricciones que conllevó la misma, se ha acelerado el desarrollo y uso de las operaciones electrónicas, mediante el uso plataformas digitales, y, desafortunadamente se ha incrementado la cantidad de ciberdelincuentes que aprovechan la oportunidad para realizar estafas electrónicas y ha ganado especial protagonismo tanto por las cuantías defraudadas como por el número de víctimas que deja a su paso.

3.2. Sistema de Pagos

3.2.1. Sistema de Pagos Electrónicos en Paraguay

En el portal de Macro Finanzas (2017) referente a la Importancia de sistemas de pagos requiere mayor compromiso de autoridades monetarias, se publica que:

> Los sistemas de pagos han adquirido especial importancia en los últimos años, por ello las autoridades monetarias están más comprometidas a que estos sistemas se desarrollen de manera eficiente para reducir los riesgos de liquidez, de crédito y sistémico, principalmente y aumentar con ello la eficacia de la política monetaria. Sistema Integral de Pagos Automáticos del Paraguay (SIPAP) promovió la interacción ente las entidades financieras participantes, los clientes y el organismo de control. Este sistema, según los mismos mejoró radicalmente los movimientos financieros nacionales; permitiendo una ágil y confiable interacción de las transacciones comerciales.

El Paraguay actualmente cuenta con Ley N° 4595/2012 denominada “Sistemas de pagos y Liquidación de Valores”, la presente Ley tiene por objeto regular la validez de las operaciones de compensación y liquidación que se realizan en el sistema de pago; así como la custodia, liquidación y compensación de valores y las garantías que se prestan los participantes en los mismos; así como los efectos de los procedimientos de suspensión de pagos sobre tales operaciones y garantías.

Recientemente, el Banco Central del Paraguay (“BCP”), por Resolución N° 1 Acta N° 26 de fecha 17 de mayo de 2022, ha aprobado y dispuesto la entrada en vigor de un nuevo reglamento general de los sistemas de pago del Paraguay (“SIPAP”) El Reglamento provee un marco general de normas que regirán los sistemas que componen el SIPAP e incluye los lineamientos para su eficiente funcionamiento, de conformidad a lo establecido en la Ley N° 4595/2012 “SISTEMAS DE PAGOS Y LIQUIDACIÓN DE VALORES”, tiene por finalidad principal promover la eficiencia el normal funcionamiento del SIPAP, simplificando la normativa anterior aplicable, unificándola y

suprimiendo de su contenido cuestiones eminentemente operativas.

3.2.2. Ventajas y Desventajas de los medios de pagos electrónicos

En el portal Tus Finanzas (s.f.) se verifica que las ventajas de los medios de pago electrónicos son:

- Son más seguras que el uso del efectivo.
- Permiten pagar por bienes o servicios de una forma inmediata o más rápida.
- Permiten un fácil control sobre las operaciones y gastos realizados.
- Se pueden utilizar para hacer compras por Internet.
- En algunos casos, ayudan a construir un historial crediticio.
- Permiten tener acceso a productos y servicios financieros

Las desventajas son:

- Si no se conocen las medidas de seguridad y no se utilizan estos medios de pago con cautela, las personas pueden ser vulnerables a delitos financieros
- Estos sistemas están bajo la observación de todo tipo de hackers. Los sistemas de protección se perfilan como algo fundamental al usar este tipo de medios de pago, por lo que es necesario que la gente conozca cómo proteger sus dispositivos.
- Si no se educa a los usuarios sobre el uso y ventajas de estos medios de pago y si este tipo de métodos de pago son más complicados de usar que los ya existentes, las personas preferirán seguir utilizando medios de pago tradicionales.

3.2.3. Provisión De Dinero Electrónico

Además de establecer sus características principales y enumerar las operaciones que se pueden realizar con el dinero electrónico, el reglamento define al dinero electrónico como el valor monetario almacenado electrónicamente en una cuenta de dinero electrónica, previa recepción de fondos en moneda local y que es aceptado como medio de pago por personas distintas a la EMPE y por esta misma y que es reconvertible a dinero en efectivo.

Con respecto a la cuenta electrónica, el reglamento establece que los usuarios solo podrán tener una cuenta de dinero electrónico por cada EMPE y cuyo saldo no podrá superar en ningún momento el equivalente a 40 jornales mínimos para actividades diversas no especificadas de la capital de la República, monto que en la actualidad equivale a G 2.806. 238.En caso de que se supere este monto, las operaciones deberán ser canalizadas a través de una cuenta básica de ahorro en una entidad financiera. (Gaona Ojeda, 2017

3.2.4. Transferencias electrónicas no bancarias

En el caso particular de las transferencias electrónicas no bancarias, el reglamento incluye límites territoriales, temporales, transaccionales y operacionales aplicables a estas operaciones.

En cuanto a los límites territoriales, se establece que las transferencias no bancarias solo podrán ser ordenadas y retiradas dentro del territorio nacional. Los límites temporales, por su parte, disponen que las transferencias no retiradas por el beneficiario en un plazo de 4 días contados, desde el momento del envío de la transferencia, deberá ser transferida por la EMPE nuevamente al remitente. (Gaona Ojeda, 2017)

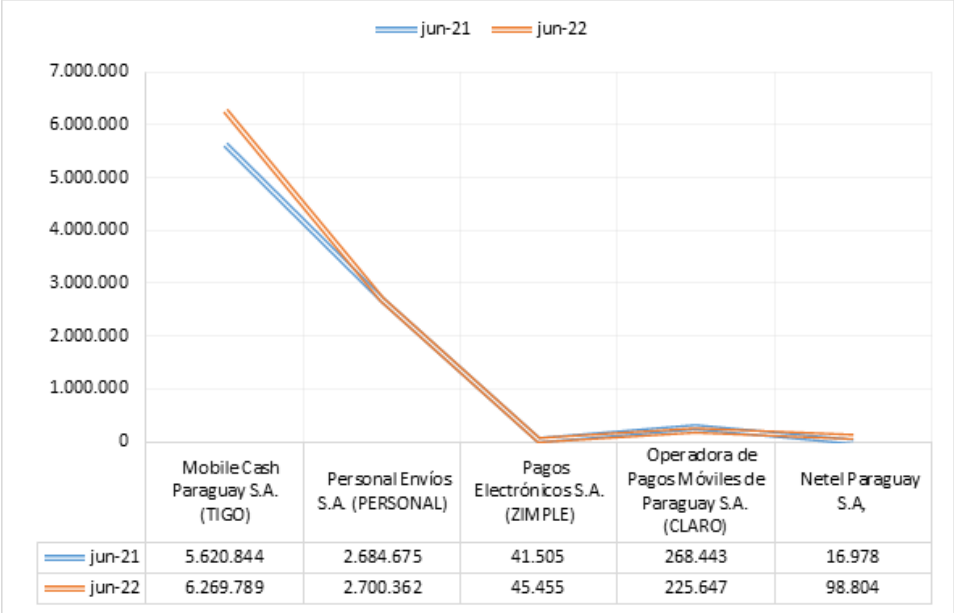
3.3. Medios de Pagos Electrónicos en Paraguay

Pese a la difícil coyuntura económica que atraviesa el país, el comercio a través de medios electrónicos sigue creciendo y demuestra con números sólidos por qué sigue se va consolidando como uno de los sistemas predilectos de los paraguayos a la hora de realizar transacciones tal es así, que los pagos por medios electrónicos aumentaron en un 8,8%.

En el mes de Julio del 2022 el Banco Central del Paraguay (BCP) dio a conocer en su boletín estadístico y financiero que las Entidades de Medios de Pagos Electrónicos (EMPES) y según el análisis realizado al desglose de servicios de diversas formas como lo son la cantidad de transacciones y cantidad de transacciones, a continuación, se expone un cuadro comparativo entre diciembre 2021 y junio 2022:

3.3.1. Informe Evolutivo de las Entidades de Medios de Pagos Electrónico en Paraguay 2022

Figura 3. Cantidad de Transacciones a través de Billeteras Electrónicas



	Mobile Cash Paraguay S.A. (TIGO)	Personal Envíos S.A. (PERSONAL)	Pagos Electrónicos S.A. (ZIMPLE)	Operadora de Pagos Móviles de Paraguay S.A. (CLARO)	Netel Paraguay S.A,
jun-21	5.620.844	2.684.675	41.505	268.443	16.978
jun-22	6.269.789	2.700.362	45.455	225.647	98.804

Fuente: Boletín Estadístico de la Superintendencia de Bancos – BCP 2022.

3.3.2. Análisis e Interpretación del Informe Estadístico Financiero del BCP sobre las Cantidades de Transacciones, Cuentas y Montos

En definitiva, conforme al Boletín Estadístico y Financiero publicado por el BCP que detalla el volumen de las transacciones electrónicas en Paraguay al mes junio 2022, referente a las entidades (EMPE) correspondiente al mes de junio de 2022, las billeteras electrónicas en nuestro país movieron un monto de G 1.133.442.000 en el mes de junio 2022, según se desprende de los números oficiales. En lo que respecta a la cantidad de operaciones registradas a través de las EMPE, resaltamos que puntualmente en el mes junio pasado se llegó a la cifra de 8,6 millones, lo cual se traduce en un aumento interanual (con relación a junio de 2021) de casi 8%.

Esta cantidad también marca un salto con relación a los meses anteriores de 2022, recordando que en enero hubo 8,5 millones de transacciones, mientras que en febrero pasado 8,4 millones de operaciones, siempre conforme a los reportes que publica el ente financiero matriz. En promedio, cada mes se registran alrededor de 9 millones de transacciones por medio de las billeteras electrónicas.

Al observar los diferentes tipos de operaciones que se realizan por medio de las cuentas habilitadas en las diferentes EMPE del mercado, destaca que las principales son las de cash in (que es la conversión de efectivo a dinero electrónico) y cash out (a la inversa), seguidos de los giros nacionales. En términos de montos, estas tres operaciones específicas representan el 80% del total alcanzado en marzo de 2022, mientras que en cuanto a cantidad de operaciones equivalen al 44% de todo lo contabilizado.

Por otro lado, la cantidad de cuentas existentes en nuestro país, según la información del Banco Central del Paraguay (BCP), llegó a 6,2 millones al cierre del primer trimestre de 2022. No obstante, la cifra de cuentas activas se ubicó en 2,3 millones.

Durante el año 2020, la crisis por Covid-19 motivó a elevar la utilización de las billeteras electrónicas, que se habilitan a través de las EMPE. Datos brindados anteriormente por la Cámara Paraguaya de Medios de Pago (CPMP) demostraban que el mayor crecimiento en esta modalidad se dio en coincidencia con la época más estricta de la cuarentena.

Asimismo, el año pasado, las billeteras digitales movieron casi USD 1.900 millones. El mayor movimiento de operaciones se reporta tradicionalmente en el mes de diciembre, en coincidencia con la época donde se tiene mayor dinero circulante dentro de la economía por la época de fin de año

4. Determinación de los procedimientos de auditoría forense en operaciones electrónicas

4.1. Auditoria Forense

Las Normas Internacionales de Auditoría (NIA's) se refieren al "Fraude y error, a la evidencia de auditoría, las consideraciones adicionales sobre partidas específicas, con respecto a las revelaciones de los Estados Financieros, a la observación de inventarios físicos, confirmación de cuentas por cobrar, indagación sobre litigios y reclamos.

Como bien es sabido, en la actualidad existen personas que delinquen para obtener los máximos beneficios posibles provenientes de actividades ilícitas, los cuales son difíciles de disfrutar ante los

ojos de la sociedad sin ningún tipo de cuestionamiento; es de esta manera como los delincuentes han ideado la forma de gozar de tales ganancias a través de la colocación en la economía de esas grandes sumas de dinero; comprometiendo en este proceso a muchos personas con conocimientos del área administrativa y contable e incluso del ámbito legal especializados que hacen posible el disfrute final del mismo. Las entidades emisoras de créditos son uno de los blancos más buscados para lavar grandes sumas de dinero, siendo así la auditoría forense la herramienta que fortalece el mecanismos de control y prevención de este delito; de allí parte un gran interés en evaluar sí estas herramientas están siendo utilizadas para tal fin o por el contrario el desconocimiento de las mismas ayuda a que estas entidades sean llamativas a los delincuentes para dar apariencia de legalidad a los recursos generados de manera ilícita.

El lavado de activos en Paraguay contribuye al incremento de la inflación y se asocia a los delitos contra el patrimonio, afectando la legalidad financier , la desvalorización de la economía y la base socioeconómica del país.

4.2. Riesgos de Auditoría

El riesgo en auditoría, existe en todo momento por lo cual se genera la posibilidad que el auditor emita una información errónea por el hecho de no haber detectado errores o faltas significativas que podría modificar por completo la opinión, el auditor siempre cuenta con escepticismo profesional y un cierto nivel de incertidumbre al realizar su tarea, la misma está relacionada con la calidad y competencia de las evidencias, la eficacia de las actividades de control y la presentación de los estados financieros. Los riesgos que debe enfrentar el auditor en su trabajo afectan la planificación de la auditoría, de allí la importancia de poder reconocerlos y medirlos previamente en la etapa de la planificación

La NIA 400 denominada “Evaluación de riesgos y control interno” menciona que:

> El auditor puede obtener un conocimiento del sistema de contabilidad y de control interno. Debe considerarse si hay ciertos controles internos que el auditor quizá quiera evaluar y poner a prueba y que pueden, a su vez, afectar la naturaleza, oportunidad y alcance de los procedimientos sustantivos de auditoría

4.3. Herramientas de la Auditoría Forense

4.3.1. Técnicas de Auditoría Forense

Romero Posso (2018), hace referencia a los procesos más importantes como lo detallado a continuación:

1. **Documentología:** Es el conjunto de procedimientos científicos utilizados para la comprobación del origen y las modificaciones que haya tenido un documento. La documentología tiene por finalidad el estudio analítico del grafismo (papel soporte y elemento escrito) para así establecer con absoluta certeza la autenticidad o falsedad de un documento. Estas adulteraciones y 99 falsificaci nes pueden ser de orden químico o físico, así como el examen comparativo para determinar la autenticidad de este. La documentología estudia:

- Grafismos y escrituras de origen manual (manuscritos, holografías o autografías).
- Textos mecanográficos, escritos con impresoras de computado .
- Impresos (tipografía, offset, flexografía, etc.
- Sellos de todo tipo
- Copias fotográficas
- Cheques, títulos-valores, sellos de correos, documentos de identificación, billetes de banco y de lotería, tarjetas de crédito, pasaportes, pases, tarjetas militares.
- Escritos en soportes no convencionales (tatuajes, pintadas o grafitis, marcas de ganado

Este proceso es de suma importancia, considerando que mediante la documentología se puede detectar la absoluta certeza o la falsedad de los documentos, es por lo que la autora expone estudios como ser grafismos, impresos, copias entre otros

2. **Dactiloscopia:** Es la ciencia que se propone identificar a las personas físicamente consideradas por medio de la impresión o reproducción física de los dibujos formados por las crestas papilares en las yemas de los dedos de las manos, se lleva a cabo las siguientes aplicaciones:

- Tomar impresiones con propósitos administrativos y judiciales.
- Clasifica , ubicar o localizar las fichas decadactilares en los archivos.
- Buscar impresiones dermopapilares en el lugar de los hechos (huellas latentes)
- Hacer investigaciones decadactilares.
- Hacer investigaciones nominales.
- Confrontar eliminatorias
- Analizar y cotejar huellas plantares (aplicable principalmente en recién nacidos).
- Emitir dictámenes.

En otras palabras, la Dactiloscopia es el sistema de identificación mediante la comparación de las huellas digitales, para ello se lleva a cabo diferentes aplicaciones mencionadas precedentemente.

3. **Caligrafía:** Arte de escribir con letra legible y buena. Su importancia en lo jurídico reside en los documentos manuscritos, aun cuando el uso progresivo de medios mecánicos, vaya tornando cada vez más raros los problemas de interpretación en la materia, precisamente, en los casos de mala caligrafía si la expresión es admisible. Sus campos de acción se basan en:

- Pericia caligráfica y documentoscopia.
- Pericia caligráfica y documentoscopia
- Análisis de falsificaciones.
- Investigación de anónimos.
- Grafopsicología judicial.

En resumen, la caligrafía es un conjunto de rasgos que caracterizan la escritura de una persona o de un documento, posee varios campos de acción que se deben tener en cuenta al momento de realizar una investigación referente a la caligrafía.

4. **Grafología Forense:** Es el estudio de los manuscritos, con el fin de establecer la veracidad o falsedad del escrito e identificar el autor. El estudio grafológico se basa en el análisis sistemático, pormenorizado, crítico y evaluativo de las características morfológicas y dinámicas del gesto grafico el análisis sistemático, pormenorizado, crítico y evaluativo de las características morfológicas y dinámicas del gesto gráfico Dentro de las actividades del grafólogo se encuentran las siguientes:

    - Determinación de autoría de firmas y escrituras. Detección de Falsificacione
    - Estudio de Escritos Mecanográficos, sellos e Impresiones.
    - Secuencia de Escritura.
    - Examen de tintas y papel.
    - Detección de Forjamientos, Alteraciones, agregados Físicos o Químicos.
    - Estudio de Anónimos.

5. **Informática forense:** Es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional. El auditor forense utiliza la informática forense ya no solo para recuperar información, sino como una herramienta de descubrir hechos ilícitos, dado que la falla de dispositivos no es por errores humanos sino por actividades fraudulentas para borrar, ocultar o adulterar información. La Informática Forense siempre ha jugado un papel fundamental en la investigación, considerando que su objetivo principal es la obtención de evidencias relativas a algún crimen digital.

5. Procedimientos de Auditoria Forense orientados a la detección de Lavado de Activo

Según Romero Posso (2018) expresa que:

> Para las investigaciones de lavado de dinero y activos se deben adelantar de acuerdo con una metodología de tipo general que se pueden ir adaptando a los requerimientos de cada

> caso y en ello juegan un papel importante las muestras y documentos que se analizan. Así mismo, el proceso investigativo para ese tipo de situaciones, presentan unas características de común concurrencia, lo que permite formular procedimientos básicos para la planeación y ejecución del trabajo y para la presentación de informes y conclusiones, aplicando procedimientos metodológicos propios de la Auditoria Financiera, que los investigadores deben armonizar con las normas legales sustantivas y procesales que regulen este tipo de investigaciones.
>
> Es así, que un elemento fundamental, es el uso de papeles de trabajo o ayudas de memoria para ir dejando plasmados o registrados aspectos importantes que contienen los diferentes documentos y pruebas allegadas al proceso, de manera que facilite la elaboración del informe final, la explicación y justificación de la información en él contenida y la ubicación de los documentos que lo soportan.

Y, detalla que para la detección del lavado de activos en las entidades de crédito es necesario investigar aspectos y documentos que permitan respaldar y desarrollar el trabajo del auditor forense:

Conocimiento del negocio: información interna, información legal, información financiera, sistemas de información, información comercial, etc.

Conocimiento del sector económico y sus características: posicionamientos y tipo de mercado, principales competidores y manejo de clientes y proveedores.

Fuentes externas de consulta: cámaras de comercio, gremios, instituciones de control, entre otras.

5.1. Procedimientos válidos para obtener pruebas en la detección del lavado de activos

Romero Posso (2018) menciona que:

> La Auditoría Forense debe desarrollarse en el cumplimiento de una serie de procedimientos en un orden lógico y secuencial con el propósito de practicar una auditoria eficiente y cumplir con los objetivos establecidos en forma oportuna. Para detectar el lavado activo se deben realizar procedimientos basados en las normas de auditoría generalmente aceptadas para que sea efectiva ante las autoridades competentes. La auditoría forense es un examen o revisión de carácter pericial y para ello es necesaria la evaluación e investigación de políticas, normas, prácticas y procedimientos e informes utilizados con el fin de emitir una opinión profesional imparcial, es fundamental determinar cada una de las fases se deben cumplir en el transcurso de la investigación y establecer el procedimiento a seguir. Los procedimientos generales son:

Analizar los alcances de los términos contractuales de la Auditoría Forense con la finalidad de que todos los auditores que participan conozcan el propósito de la auditoría, de tal manera que no existan dudas y se pueda alcanzar los fines propuestos y obtener conocimiento apropiado de la materia y del ambiente específico del compromiso en el que se realizará la Auditoría Forense, de manera que permitan preparar procedimientos de auditoría que proporcionen conclusiones valederas y apropiadas que permitan sustentar ante las partes involucradas el informe correspondiente. Este conocimiento se adquiere con las discusiones con el cliente y abogados, revisando las hipótesis del

problema, entrevistas y documentación involucrada.

Evaluar el control interno utilizando bajo el esquema COSO 40 (Committee Of Sponsoring Organizations). Este modelo consiste en tener un esquema gerencial basado en el manejo del riesgo que permite pensar estratégicamente y actuar a tiempo para visualizar, identificar y cuantificar todos los riesgos posibles de manera preventiva y a generar controles antes de que sucedan los hechos.

- Coordinar en forma permanente con los asesores legales con la finalidad de no incurrir en faltas que invaliden la opinión.
- Establecer una estrategia que permita obtener en forma detallada las declaraciones de las partes involucradas, debiéndose tener la precaución de obtener la declaración escrita y siendo complementada por videos, grabaciones etc.

A continuación, se presenta un modelo propuesto de Programa de Auditoria para evaluar las operaciones electrónicas y de esta manera obtener mayor seguridad al momento de la realización de operaciones electrónicas en las entidades:

Tabla 4. Programa de Auditoría propuesto para evaluar las operaciones electrónicas

PROGRAMA DE AUDITORÍA
PARA EVALUAR LAS OPERACIONES ELECTRONICAS

Cliente: _____
Periodo de auditoría: _____
Objetivos de la evaluación:

a. Evaluar la seguridad que poseen los sistemas bancarios que se acceden online, para realizar operaciones transferencias bancarias.
b. Verificar que las medidas de seguridad que la empresa ha implementado para controlar los accesos otorgados a los usuarios que ingresan a los sistemas bancarios, sean adecuadas.
c. Revisar el control interno relacionado con las operaciones bancarias que se realizan a través de Internet; así como también que la documentación que se deja de soporte en dichas operaciones sean adecuadas.

Nro.	Procedimientos	Hecho por	Fecha	Ref.
1	Solicite los manuales que el Banco ha proporcionado a la empresa por el servicio contratado y verifique que estos contengan: • Condiciones de uso • Políticas de seguridad • Políticas de privacidad			
2	Al revisar el sistema verifique que la dirección que este presenta registre el protocolo https en lugar de http://, lo cual indica que el lugar al que se accede es seguro.			

Nro.	Procedimientos	Hecho por	Fecha	Ref.
3	Verifique la existencia de políticas de seguridad y revise que estas consideren como mínimo lo siguiente: a. Políticas de contraseña, las cuales deben contener: • La longitud mínima y máxima • El período de vigencia de esta (mínimo 30 días) • Composición de la contraseña (letras, números, caracteres especiales, mezcla de mayúsculas y minúsculas, etc. • Que el momento de cambiar la contraseña no permita utilizar ninguna de las últimas 10 contraseñas anteriores. • Que el sistema exija cambio de contraseña en el primer inicio de sesión. b. Solicite acceso al sistema bancario y verifique que la cuenta de usuario se bloquee al ingresar una contraseña incorrecta. (máximo 3 intentos erróneos). c. Verifique que el sistema deshabilite las cuentas de usuario que no ingresan al sistema en un periodo de tiempo determinado (30,60, 90 días) d. Verificar que el sistema desconecte la sesión del usuario que pasa inactivo durante un lapso. (3 minutos mínimos). e. Verificar que el sistema permita recuperar la contraseña en caso de olvido, a través de: enviando la nueva contraseña a una dirección de correo electrónico del cliente o mediante mecanismos de preguntas y respuestas secretas. f. Comprobar que los accesos de los sistemas bancarios se realicen digitando en la barra de dirección del browser la dirección del sitio de internet respectivo (evitando acceder a través de vínculos enviados en mensajes de correo electrónico.)			
4.	Comprobar que, para procesar pagos de préstamos, proveedores, planillas y transferencias, se haya creado un usuario que ingrese y otro que autorice.			
5	Solicite a la empresa un detalle de los usuarios que realizan operaciones bancarias por internet.			
6	Verificar que al final de cada pago a proveedores y planillas se efectúe una revisión, para confirmar que todas las operaciones fueron efectuadas.			

Nro.	Procedimientos	Hecho por	Fecha	Ref.
7	Observe el proceso de pago de servicios, préstamos, impuestos, proveedores, planillas y transferencias, y verificar que cada operación se deje documentada con la confirm - ción que genera el sistema bancario.			
8	Solicite a la empresa le efectúe una circularización de saldos bancarios y cotéjelos con los saldos contables.			
9	Solicite a un usuario le genere un estado de cuenta del sistema bancario y seleccione algunas operaciones realizadas a través de internet, para verificar que estén registradas en dicho estado de cuenta.			
10	Solicite el contrato firmado con el Banco por el servicio prestado, y verifique que este haya sido firmado por las personas autorizadas en las cuentas bancarias.			
11	Elabore el correspondiente informe			

Fuente: Elaboración propia (2022).

6. Conclusiones

Se analizaron los riesgos y los diferentes tipos de estos, describiéndose así las medidas de acciones para mitigarlos y cómo se pueden aplicar en las empresas. Para ejemplificar este concepto, se toma en cuenta el caso de un manual de riesgos en Bogotá, Colombia, lo que se compara con el Paraguay y se detecta que el país no posee estas herramientas en las empresas similares a las operaciones electrónicas, servicios financieros digitales, entre otros. Es por ello, que se recomienda que se englobe el paso a paso para disminuir los riesgos en el uso de los instrumentos financieros electrónicos, así como, aquellas señales de alerta para las transacciones y operaciones electrónicas. En definitiva, las operaciones electrónicas en el país cada día van en aumento, además de la inclusión financiera de la ciudadanía en general, pues, los sistemas de pagos electrónicos son los más utilizados actualmente. Con la entrada en vigencia de la Ley N° 6822/2021 “De los servicios de confianza para las transacciones electrónicas”, el Paraguay va ampliando el marco regulatorio con relación a este tipo de operaciones ofreciendo una herramienta que busca generar la confianza y seguridad jurídica.

Asimismo, se encuentran las definiciones de las operaciones electrónicas, sus características, ejemplos y reportes estadísticos y económicos, además, se analizan los gráficos según el boletín mensual del Banco Central del Paraguay a junio del 2022. En ese reporte, se detalla en números de forma válida y real que transforman conceptos en la visualización de los resultados de las operaciones y cómo se movilizan en el país. Plasmando un aumento significativo de su crecimiento e incidencias en la economía para todos los sectores que hacen vida activa en la sociedad.

Finalmente, se observó que las operaciones electrónicas estimulan a la rotación de dinero, lo que promueve el crecimiento económico. En conclusión, las operaciones electrónicas requieren que el auditor contable esté consciente de que es necesario utilizar las tecnologías de información para el desarrollo pleno de la profesión, ya que se considera una herramienta que les ayudará a profundizar su trabajo y a mejorar el alcance en sus procedimientos, así como los resultados de estos.

Conflicto de Interés

La autora declara no tener conflicto de interés

Referencias

Alamo Cerrillo, R., & Lagos Rodríguez, M. (2013). *Retos fiscales del Comercio Electrónico. La Neutralidad en las operaciones comerciales electrónicos*.

Cano, M., & Lugo, D. (2005). *Auditoría Forense en la Investigación criminal del lavado de dinero y activos*. Ecoe Ediciones.

Maruri-Arcentales, J., Casquete-Baidal, N., & Arcos-Coba, J. (2020). *La auditoría de transacciones electrónicas. Como tener control en la era de la globalización*. Revista Científica Dominio de las Ciencias (4). http://dx.doi.org/10.23857/dc.v6i4.1474

Rojas, I. (2020). *Pandemia disparó la utilización de transferencias electrónicas como medio de pago, en Paraguay*.

Romero, C., & Aguilar, E. (2014). *Diseño de un sistema de control interno basado en la auditoría operativa, para contrarrestar estafas electrónicas, en empresas que realizan operaciones de compra y venta, mediante comercio electrónico, en la ciudad de Chiclayo 2013* [Tesis de pregrado, Universidad Católica Santo Toribio de Mogrovejo]. https://tesis.usat.edu.pe/handle/20.500.12423/184

Romero Posso, J. (2018). *La auditoría forense como herramienta en la detección del lavado de activos en el sector bancario en la Ciudad de Palmira Valle*.

Sistema de Información. (s.f.). *Compliance Catálogo de Señales de alerta para la Prevención del Lavado de Activos de Compliance*. https://www.compliance.com.co/catalogo-de-senales-de-alerta-para-la-prevencion-del-lavado-de-activos-de-compliance/