UNIVERSIDAD DEL AZUAY

DEPARTAMENTO DE POSGRADOS

MAESTRÍA EN AUDITORÍA INTEGRAL Y GESTIÓN DE RIESGOS FINANCIEROS

VERSIÓN III

"Análisis de los procedimientos utilizados por la auditoría forense aplicada a la Prevención de Lavado de Activos en el sector de la Banca Privada en la ciudad de Cuenca en el periodo 2018"

Trabajo de graduación previo a la obtención del título de:

Magister en Auditoría Integral y Gestión de Riesgos Financieros

Autor:

Ing. María Eugenia Pesántez Coyago

Director:

MBA, MSc. Esteban Crespo Martínez

Cuenca - Ecuador

Diciembre 2020

DEDICATORIA

Este trabajo de graduación lo dedico a Dios, a mis padres Homero y Aidita, a mis hermanas Tatiana y Gabriela, quienes me han apoyado y motivado a cumplir este objetivo.

María Eugenia

AGRADECIMIENTO

Agradezco en primer lugar a Dios por ser mi fortaleza en todo momento. A mis padres, por el sacrificio y apoyo que me han brindado en esta etapa de estudios. Al Magister Esteban Crespo, por el tiempo, dedicación y conocimientos aportados para la realización de este trabajo de grado.

María Eugenia

Resumen

En la actualidad, la tecnología aplicada a la auditoría forense en el sector bancario exige el desarrollo de nuevas técnicas de fraude y amenazas que se presentan y que pueden afectar a las instituciones bancarias. El objetivo general de este trabajo de investigación es analizar los procedimientos utilizados por la auditoría forense aplicada a la prevención de lavado de activos en el sector de la banca privada de la ciudad de Cuenca en el periodo 2018. Para ello, se revisaron 12 casos relacionados al fraude y posible lavado de activos en el sector de la banca privada, método de investigación que ha resultado útil para recabar información en contextos de la vida real. En conclusión, la auditoría forense aplicada en las empresas aporta, a través de una propuesta y revisión de una guía metodológica para la prevención de fraude electrónico, en la evaluación de los riesgos de fraude, aplicando los procesos y controles necesarios para reducir los riesgos.

Palabras Clave: Auditoría forense, Delitos financieros, Fraude, Lavado de activos, Sector financiero, Banca.

Abstract

In the world we live today, applied technology used in forensic auditing in the banking sector demands the development of new techniques to stop fraud and threats that present and affect banking institutions. The general objective of this case study was to analyze the procedures use in forensic auditing to prevent money laundering in the private banking sector of Cuenca during 2018. For that, 12 cases were reviewed in relation to fraud and possible money laundering in the private banking sector. The method of investigation provided useful results to receive contextual information from real life. In conclusion, forensic auditing applied to these companies contributes to a proposal and review from a methodical guide to prevent electronic fraud, in the evaluation of the risks of fraud by applying steps and control to reduce these risks.

Key Words: Forensic auditing, financial crimes, fraud, money laundering, financial sector, banking.

Traslated by:

María Eugenia Pesántez

Análisis de los procedimientos utilizados por la auditoría forense aplicada a la prevención de lavado de activos en el sector de la banca privada en la ciudad de Cuenca en el periodo 2018

Pesántez Coyago María Eugenia
Universidad del Azuay
Azuay, Ecuador
mariupesantez@es.uazuay.edu.ec

Crespo Martínez Paúl Esteban
Universidad del Azuay
Azuay, Ecuador
ecrespo@uazuay.edu.ec

***Resumen*—** En la actualidad, la tecnología aplicada a la auditoría forense en el sector bancario exige el desarrollo de nuevas técnicas de fraude y amenazas que se presentan y que pueden afectar a las instituciones bancarias. El objetivo general de este trabajo de investigación es analizar los procedimientos utilizados por la auditoría forense aplicada a la prevención de lavado de activos en el sector de la banca privada de la ciudad de Cuenca en el periodo 2018. Para ello, se revisaron 12 casos relacionados al fraude y posible lavado de activos en el sector de la banca privada, método de investigación que ha resultado útil para recabar información en contextos de la vida real. En conclusión, la auditoría forense aplicada en las empresas aporta, a través de una propuesta y revisión de una guía metodológica para la prevención de fraude electrónico, en la evaluación de los riesgos de fraude, aplicando los procesos y controles necesarios para reducir los riesgos.

Palabras Claves: Auditoría forense, Delitos financieros, Fraude, Lavado de activos, Sector financiero, Banca.

I. INTRODUCCIÓN

En la actualidad, la tecnología aplicada a la auditoría forense en el sector bancario exige el desarrollo de nuevas técnicas de fraude y amenazas que se presentan y que pueden afectar a las instituciones bancarias implicando daños significativos en las organizaciones, pérdidas financieras, multas o acciones legales, afectación de la imagen lo que puede ocasionar inconvenientes a nivel operativo y estratégico. Según un reciente informe elaborado por el Fondo Monetario Internacional [1] titulado "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment", los ataques informáticos podrían representar para el sector financiero mundial pérdidas cercanas a los 100 mil millones de dólares, indicando que el 80% de los ataques informáticos provienen del interior de la organización, es decir, provocada de forma deliberada por los empleados o funcionarios de la misma, mientras que el 20% restante proviene del exterior, a los que el autor los denomina "Hackers". En este sentido, la revisión de las políticas establecidas en el campo de la auditoría, específicamente en el sector bancario, establece que los procedimientos aplicados deben ser adecuados para prevenir el lavado de activos y financiamiento de delitos.

Por esta razón, se desarrolla como objetivo general de esta investigación, proponer una guía metodológica para la prevención de lavado de activos y fraude electrónico basada en las normas ISO 31000, ISO 9001:2015, ISO 27005, ISO 37001 y en el marco de gobierno COBIT 5, en el sector bancario, considerando que la norma ISO 27005 es aplicable dentro de las instituciones financieras, ya que permite gestionar el lavado de activos, basada en la Gestión de Seguridad de la Información y la tecnología de las comunicaciones, la cual incluye recomendaciones para la gestión de riesgo en Sistemas de Gestión de Seguridad de la Información, agregando aspectos de identificación de activos y riesgos.

A través del método cualitativo, con relación al alcance del estudio se analizaron, los procedimientos más utilizados en la auditoría forense que permiten detectar posibles actos ilícitos que conllevan al fraude, así como el lavado de activos, para así aplicar los correctivos más adecuados que contribuyan con la prevención de estos., considerando las mejores prácticas de la industria resumidas en las normas ISO 31000, ISO 9001:2015, ISO 27005, ISO 37001 y el marco de gobierno de Tecnologías de Información COBIT 5, en base al estudio de casos financieros y procedimientos utilizados por las entidades financieras para la prevención de delitos y fraudes.

La técnica de la auditoría forense permite detectar y determinar fraudes y delitos y se enfoca en la prevención, control y monitoreo mediante múltiples procedimientos, para obtener evidencia suficiente de auditoría y extraer conclusiones razonables que servirán como pruebas que esclarezcan hechos inusuales o ilícitos [2]. El auditor especializado debe utilizar toda la experiencia, capacidades, conocimientos y habilidades investigativas para la detección de anomalías que puedan ser informadas a la Ley para su posterior análisis [3].

Las entidades financieras están obligadas a adoptar medidas de control, orientadas a prevenir y mitigar los riesgos que, en la realización de sus transacciones, puedan ser utilizadas como instrumento para lavar activos, financiar el terrorismo y otros delitos [4].

Además, dentro de las instituciones financieras es obligatorio que el personal conozca las políticas para prevenir el lavado de activos y financiamiento de delitos, e identificar mecanismos que eviten involucrarse con dinero de dudosa procedencia basados en las políticas de "Conozca a su cliente", "Conozca a su Proveedor", "Conozca su mercado", Conozca a su corresponsal [5].

Según Aranza y Bermeo [6], el lavado de dinero consiste en legalizar un dinero ilícito, insertándolo al sistema económico legal. Por otra parte, el mismo autor menciona que entre los tipos existen el financiamiento del terrorismo, el cual consiste en el apoyo económico a grupos subversivos o través del conocimiento que existe como clientes de la institución financiera.

De igual manera, Ansaldi [7] expresa que para prevenir el Lavado de Activos, financiamiento del terrorismo entre otros delitos dentro de las instituciones financieras, estas disponen de una Unidad de Cumplimiento y por norma se asignan dos

Oficiales de Cumplimiento, uno titular y otro suplente, los cuales son los encargados de hacer cumplir las políticas y procedimientos, además de concientizar a todo el personal de los riesgos que implican para las instituciones el involucrarse con dinero de dudosa procedencia.

Entre otro grupo de los delitos que se presenta dentro de las instituciones financieras se pueden mencionar el pitufeo, actividad mediante la cual se busca, principalmente, realizar operaciones por debajo de los límites vigilados por las autoridades y esta se realiza mediante el manejo de reducidas cantidades en efectivo en varias cuentas, en la mayoría de los casos pertenecientes a personas ajenas a la operación, quienes las prestan a cambio de una mínima remuneración pero asumiendo un enorme riesgo [8].

Existen procedimientos dentro de las instituciones que deben cumplirse al momento de identificar ciertos patrones de transacciones inusuales realizadas desde las cuentas de los clientes; éstas son analizadas por el Oficial de la cuenta en conocimiento del personal de la Unidad de Cumplimiento a través de la implementación de formatos o de la elaboración de informes ejecutivos con los soportes del caso [2]. De igual manera existe el ROII, el cual es un reporte de operaciones inusuales e injustificadas que por su naturaleza deben ser informadas a la Unidad de Análisis Financiero y Económico. Otro de los delitos que involucran al lavado de activos es el PEP, se denomina así a la persona expuesta políticamente porque desempeña funciones públicas reconocidas en el país o en el exterior y que por su perfil puede exponer en mayor grado al riesgo de lavado de activos.

El lavado de activos es uno de los mayores flagelos contra la sociedad, ya que provoca nefastos efectos en la economía y en la administración de la justicia dado que la conversión o transferencia de capitales de origen ilícito producen graves problemas y favorecen la perpetración de una cadena indeterminada de actos ilícitos, los cuales deben ser combatidos en resguardo de los intereses del país y su población. Organismos internacionales como la ONU, la OEA y el GAFISUD, de los cuales el Ecuador forma parte, recomiendan la adopción de medidas efectivas para la prevención de este tipo de delitos [9].

En este sentido, la norma ISO 27005 es aplicable dentro de las instituciones financieras, pues permite gestionar el lavado de activos, ya que se basa en la Gestión de Seguridad de la Información y la tecnología de las comunicaciones, considerando recomendaciones para la gestión de riesgo en Sistemas de Gestión de Seguridad de la Información en la cual incluye orientaciones tales como la identificación de activos y riesgos [10].

La construcción de esta guía metodológica de prevención de fraude requirió el estudio, la explicación y la determinación de las estrategias operativas y normativas fundamentales que contribuyen a prevenir el lavado de activos, así como de fraudes electrónicos enfocados a la gestión de riesgos, calidad y seguridad de la información, sistema de gestión antisoborno y el trámite y control de las tecnologías de información (TI).

Para ello, se fundamenta la teoría que sustenta las bases de la Auditoría Forense, y las metodologías y marcos para gestión de riesgos, y se analizan 12 casos de delitos en entidades financieras y los mecanismos utilizados para prevención y detección de fraudes.

El objetivo de este trabajo es el de proponer una guía metodológica para la prevención de fraude electrónico basada en las normas ISO 31000, ISO 9001:2015, ISO 27005, ISO 37001 en el marco de gobierno COBIT 5, en base al estudio de casos financieros y procedimientos utilizados por las entidades financieras para la prevención de delitos y fraudes.

Este trabajo está dividido en 8 secciones: i) introducción; ii) el estado del arte, donde se identifican trabajos relacionados realizados por otros autores; iii) la metodología aplicada en este proceso de investigación; iv) los resultados obtenidos; v) propuesta de una guía metodológica para la prevención de lavado de activos y fraude electrónico; vi) la discusión de los resultados y su relación con el estado del arte; vii) las conclusiones obtenidas como producto de esta investigación y viii trabajos futuros.

II. Marco teórico

A. La Auditoría Forense

La auditoría forense es un conjunto de técnicas dedicadas a la recolección de evidencias para transformarlas en pruebas, las cuales se presentan principalmente en las cortes de justicia, con la finalidad de demostrar delitos o resolver disputas legales. En la actualidad se vienen desarrollando importantes esfuerzos a través de auditorías de cumplimiento y auditorías integrales que deben ser fortalecidos con procedimientos legales de investigación, para así minimizar la impunidad que se expone ante delitos económicos y financieros, como lo son la corrupción administrativa, el fraude corporativo y el lavado de dinero y activos [8].

B. Diferencia entre la Auditoría Forense con otros enfoques de Auditoría

La Auditoría Forense se diferencia con otros enfoques en su característica preventiva, ya que mantiene un programa de aseguramiento constante del riesgo de fraude y sugiere medidas de control; detecta fraudes que deberán ser investigados a profundidad y ser llevados a instancias legales en su caso; considerando al fraude como la representación equivocada e intencional de hechos financieros o malversación de activos de naturaleza material [11].

C. Normas ISO

ISO 31000

La ISO 31000 es una normativa internacional que propone las directrices y principios para administrar el riesgo de las organizaciones. Esta norma fue publicada en noviembre del 2009 por la Organización Internacional de Normalización (ISO) en contribución con la Comisión Electrotécnica Internacional (IEC), y tiene por objetivo gestionar los riesgos de forma efectiva, en organizaciones de todos los tipos y tamaños por lo cual se recomienda que las empresas se dediquen a establecer, fomentar y mejorar permanentemente un marco de trabajo cuyo fin es constituir el proceso de gestión de riesgos en cada una de sus actividades. La guía ISO 31000 además de estar orientada en la gestión de riesgos, es utilizada como una herramienta destinada a facilitar a las empresas los criterios y estándares, que proporcionen más eficiencia en los eventos de riesgo y procesos, efectuados en las diversas fases organizacionales, tales como estratégicas y operativas [12].

ISO 9001

La ISO 9001 es una de las normas reconocida a nivel internacional aplicadas a sistemas de gestión de calidad (SGC). Esta norma de gestión de calidad es la más utilizada a nivel mundial, con más de 1 millón de certificados emitidos en más de 178 países. La ISO 9001 ofrece un marco de trabajo y un conjunto de principios para garantizar un enfoque lógico a la gestión de su empresa, con el fin de satisfacer a sus

clientes y partes interesadas. Por otra parte, la certificación ISO 9001 ofrece las bases para desarrollar procesos y personal efectivo que suministre como resultado productos y servicios garantizados y duraderos en el tiempo. Esta Norma Internacional precisa requisitos orientados principalmente a otorgar confianza en los productos y servicios facilitados por una organización y por lo tanto aumentar la satisfacción del cliente. Igualmente, su adecuada implementación aportará otros beneficios a la organización tales como la mejora de la comunicación interna, mejor comprensión y con organización [13].

ISO 27005

ISO 27005 es una norma internacional que se ocupa de la gestión de riesgos de seguridad de información. Dicha norma suministra las directrices para la gestión de riesgos de seguridad de la información en las organizaciones, apoyando específicamente los requisitos del sistema de gestión de seguridad de la información definidos en ISO 27001. ISO-27005, además es aplicable a todo tipo de organizaciones que consideren el propósito de gestionar los riesgos que puedan dificultar la seguridad de la información de su organización. Su metodología dependerá de una serie de factores, como el alcance real del Sistema de Gestión de Seguridad de la Información (SGSI), o el sector comercial de la propia industria [14].

ISO 37001

La norma ISO 37001 es una certificación internacional, publicada en 2016, por la Organización Internacional de Normalización, y se encarga de implementar los requisitos para la implementación de un sistema que combata la corrupción. El objetivo de la norma ISO 37001 es promover en las organizaciones una cultura empresarial ética, a través de controles que logren prevenir y detectar los riesgos de soborno en una organización. A su vez, que esta norma suministre principios y guías exhaustivas, beneficiará a las empresas en sus análisis y evaluaciones de riesgos. Esta norma internacional se puede aplicar, de igual manera, en una empresa pública, privada o comunitaria, ya que se aplica a la mayoría de las actividades empresariales, incluyendo la planificación, operaciones de gestión y procesos de comunicación [15].

COBIT 5

COBIT 5 es un marco de trabajo que permite entender la dirección y la gestión de las tecnologías de información (TI) en una organización, así como valorar el estado en que se encuentran las tecnologías de la información en la empresa. Representa un conjunto de herramientas de apoyo que permite a la gerencia de las organizaciones cumplir con los requerimientos de control, problemas técnicos y los riesgos del negocio. De igual manera, con la utilización de COBIT 5 se puede desarrollar una política clara que logre el control de las TI en la organización. La aplicación de este marco insiste principalmente en el cumplimiento regulatorio y ayuda a aumentar el valor asociado al área de TI de la organización. Desde su inicio, COBIT 5 ha progresado desde su uso en la auditoría de TI, para convertirse en una herramienta de control en la gestión de TI, el gobierno de TI, llegando a su versión actual que es un enfoque de gobierno corporativo de TI [15].

D. ANTECEDENTES INTERNACIONALES

El autor Ferreyros [8], en Lima, Perú, realizó la investigación que lleva por nombre “La auditoría forense como herramienta preventiva y de investigación para combatir el fraude y la corrupción financiera en Perú”. El objetivo general de la investigación fue determinar si la auditoría forense es una herramienta preventiva y de investigación para combatir el fraude y la corrupción financiera pública en el Perú.

El autor ratifica la necesidad de detectar por qué ocurren estos actos ilícitos, qué lleva a las personas a cometer estos delitos, por qué es difícil detectarlos, y por qué la legislación actual no ayuda a mitigar la corrupción y el fraude.

El aporte que brinda esta investigación radica en la importancia de la actualización y optimización de los procesos, específicamente los administrativos y aún más idóneo en el departamento de cuentas por pagar, dejando ver que es necesario el cumplir parámetros y normas que permitan el buen funcionamiento, estableciendo parámetros y utilización de nuevas políticas nacidas de cambios realizados en el área investigada, concluyendo que con el aseguramiento e implementación de cambios en la dirección correcta, es posible lograr el éxito dentro de la organización, agregando que la auditoría forense es una herramienta de gestión antifraude y anticorrupción y que su desarrollo y expansión solo es cuestión de tiempo.

El autor Ansaldi [7], en Argentina, realizó la investigación que lleva por nombre “Análisis de la Auditoría Forense en la investigación de delitos económicos y financieros”, cuyo objetivo general se resume en identificar y analizar las herramientas que provee la auditoría forense al contador público, como auxiliar de justicia, para contribuir al esclarecimiento de delitos económicos en Argentina, en particular el lavado de dinero durante el periodo 2016. El autor reafirma, que el lavado de dinero es un tema de relevante importancia a nivel mundial, y es por esta razón que cada año se crean nuevos convenios y estrategias para combatirlo, considerándose un desafío global.

En este estudio se evidenció que los peritos contables se encuentran tentados a incurrir en impericias y negligencias con el fin de cumplir con las exigencias de diversos sectores de poder, y, de la mano de la corrupción, propiciar su libertad. El aporte que brinda esta investigación radica en la importancia del papel del contador público, en su actuación como auxiliar de justicia, ya que este se encuentra sujeto a diversas responsabilidades que perfilan su ejercicio y que aquellos incumplimientos a su deber, acarrean consecuencias conducentes a la inhabilitación especial hasta la pena de prisión. El autor de dicha investigación concluyó que, a través del análisis de diversas causas judiciales, que la pericia contable tiene la potestad de influir y muchas veces, se logra definir el curso de un proceso judicial.

El autor Zambrano [16], en Colombia, realizó la investigación titulada “La auditoría forense: Un mecanismo para detectar el fraude de estados financieros en Colombia”. El objetivo general de la investigación fue determinar la importancia de la auditoría forense como mecanismo efectivo en la detección de los fraudes financieros en Colombia. El autor ratifica la necesidad de revisar la normatividad aplicada para sancionar los delitos por fraude en estados financieros, con el fin de sentar un precedente en la responsabilidad del contador público con la sociedad.

El aporte que brinda esta investigación, radica en la importancia de las herramientas proporcionadas por la

Auditoría Forense, y que, a través de la aplicación de un conjunto de procedimientos y técnicas aplicados de forma integrada y secuencial, permiten hallar pruebas y evidencias relevantes y útiles que evidencian resultados significativos para el trabajo de investigación. El autor concluyó que el compromiso de las empresas para erradicar los fraudes financieros reside en aumentar los controles y realizar un seguimiento constante a todos aquellos riesgos que se puedan presentar dentro de la empresa con el objetivo de disminuir su probabilidad de ocurrencia.

E. ANTECEDENTES NACIONALES

Rojas [17] realizó la investigación que lleva por nombre "Propuesta Metodológica para la Detección y Prevención de Fraudes de Lavado de Activos en empresas del Sector Inmobiliario Empleando Herramientas de Análisis de Datos Lógicos". El objetivo general de esta investigación fue diseñar una propuesta metodológica para la detección y prevención de fraudes de lavado de activos en empresas del sector inmobiliario, empleando herramientas de análisis de datos lógicos.

El aporte que brinda esta investigación radica en la importancia de normar, sancionar y hacer cumplir las leyes, ya que el lavado de activos representa una actividad ilícita por medio de la cual se oculta el origen del dinero con el objetivo de hacerlos circular libremente y de manera legal en el sistema financiero de un país. El autor concluyó que el trabajo integrado con entidades dedicadas al control de programas antifraude y con las fiscalías de cada país, permitirá determinar los orígenes y tipologías empleadas por los delincuentes en la ejecución de estos delitos y de esta manera desarrollar nuevas medidas y requerimientos para las entidades sujetas a su control, con el fin de evitar el ingreso de dinero de origen ilícito en economías legales.

En Ecuador, las estadísticas indican que, en el año 2018, las transacciones fraudulentas se clasificaron en un 37% como corrupción, un 40%, encubrimiento con un 40%, con un 10% Testaferro, por otra parte, un 4% mal uso de negocios legítimos y con un 3% pitufeo, defraudación tributaria y uso de empresas fantasmas. Además, el SRI reportó que las empresas fantasmas en el Ecuador, tuvieron un aumento de un 47% con respecto al año 2017 [18].

Por otra parte, Quevedo [19], realizó la investigación que lleva por nombre "Estrategia de auditoría forense para la prevención de fraudes empresariales" El objetivo general de la investigación fue diseñar una estrategia de auditoría forense para la prevención de fraudes empresariales, que permitiera abarcar las metodologías adecuadas, a fin de contribuir con el buen manejo del dictamen sobre la incidencia de los estados contables como una contribución para los sistemas administrativos.

El aporte que brinda esta investigación reside en la importancia del diseño de estrategias dirigidas a la prevención de fraudes empresariales, de manera que se caractericen los aspectos fundamentales de los controles internos que afectan a los procesos contables y entregar información útil para la gerencia. Concluyó que cualquier tipo de empresa es susceptible a fraudes financieros y su vulnerabilidad persiste en todos los niveles y no se pueden evitar definitivamente, pero si se pueden crear mecanismos que logren llevar un mejor, riguroso y estricto control con políticas antifraudes que se implanten las empresas.

Los autores Camposano y Moyano [20] trabajaron en la investigación denominada "Auditoría Forense aplicada al Sistema de Créditos de la cooperativa de ahorro y crédito Jardín Azuayo, Oficina Cuenca". El objetivo general de la investigación fue el análisis Forense al Sistema de Créditos de la Cooperativa de Ahorro y Crédito "Jardín Azuayo", Oficina Cuenca, con el fin de determinar los riesgos de fraude, posibles irregularidades, que permitan mejorar los controles internos. El aporte que brinda esta investigación radica en la importancia del levantamiento de información a través de informes de auditoría en los procesos administrativos, ya que son necesarios para la detección de fraude, lavado de dinero, así como el incumplimiento de normas que permitan establecer políticas y normativas para lograr el éxito dentro de la organización.

El autor concluyó que es indispensable crear conciencia al personal en las empresas, a través de una visión integral de capacitación para que evidencien, delitos, tales como: corrupción administrativa, fraude contable y el lavado de dinero, a través de los informes sobre los riesgos de fraude.

Carvallo, Crespo, Carvajal y Vintimilla [21], en su investigación, "Systematic Literature Review: Success, Failure, Risks, Benefits and Barriers Factors in the Adoption of Open Source Software" estudian el punto de partida del desarrollo del Software Libre, a través de estudios primarios más relevantes y de la definición y la posterior aplicación de cadenas de búsqueda, en bases de datos seleccionadas y así como la evaluación de la calidad de los artículos a través del protocolo de revisión diseñado para este estudio, de esta manera se examinaron los factores de éxito, fracaso, riesgos, beneficios y barreras en la adopción de software de código abierto (OSS) y su importancia estratégica, en los últimos años, donde se limita la explotación de los beneficios de adoptar OSS en la industria pública, privada y en la sociedad ecuatoriana en general, debido a las deficiencias en la identificación, evaluación y gestión de riesgos.

Crespo [22], realizó un trabajo investigativo denominado "Metodología de Seguridad de la Información para la gestión del Riesgo Informático aplicable a MPYMES" con el objetivo de proponer una guía metodológica para la identificación de riesgos y mitigación de estos dentro de los sistemas informáticos de una MPYMES, cuyo resultado se denomina ECU@Risk.

El mismo autor, en [23], realizó el trabajo "Ecu@Risk, Una metodología para la gestión de Riesgos aplicada a las MPYMEs", que examina diversas metodologías para la gestión de riesgos de seguridad de la información aplicables al entorno empresarial y organizacional del sector ecuatoriano de MIPYME, entre las cuales se mencionan, CRAMM (CCTA Risk Analysis and Management Method), OCTAVE-S, Microsoft Risk Guide, COBIT 5 COSO III. Estas metodologías se utilizan internacionalmente en la gestión de riesgos de la información, a la luz de los marcos de la industria: ISO 27001, 27002, 27005 y 31000.

Por otra parte, los autores Torres y Crespo [10], realizaron la siguiente investigación "Propuesta de modelo de gestión de calidad de servicio de Tecnologías de Información en el sector PYME basado en COBIT, COSO, ITIL y las prácticas de la industria" donde se consideran aspectos bibliográficos fundamentales y de investigación de las diferentes normativas tanto de gobierno corporativos como de gestión,

lo que permite enfocar estratégicamente a las TI utilizadas en las PYMES ecuatorianas.

Los resultados obtenidos, reflejan que algunas entidades encuestadas no cuentan con sistemas tecnológicos. Además, el análisis realizado propone un modelo que permitirá planificar, ordenar y mejorar cada uno de sus procesos. Del mismo modo este se enfocará a la calidad de servicio de TI que puede ser adoptado por el sector PYME, a los que se agregan indicadores que permitirán evaluar el nivel de este servicio.

TABLA 1 TRABAJOS RELACIONADOS A PROCEDIMIENTOS UTILIZADOS POR LA AUDITORÍA FORENSE

Nombre del Artículo	Nombre del Autor	Objetivo
La auditoría forense como herramienta preventiva y de investigación para combatir el fraude y la corrupción financiera en Perú	Ferreyros, Jorge	El objetivo general de la investigación fue determinar si la auditoría forense es una herramienta preventiva y de investigación para combatir el fraude y la corrupción financiera pública en el Perú.
Análisis de la Auditoría Forense en la investigación de delitos económicos y financieros	Ansaldi, Agustina	El objetivo general se resume en identificar y analizar las herramientas que provee la auditoría forense al contador público, como auxiliar de justicia, para contribuir al esclarecimiento de delitos económicos en Argentina, en particular el lavado de dinero durante el periodo 2016.
La auditoría forense: Un mecanismo para detectar el fraude de estados financieros en Colombia	Zambrano, Yaneth	El objetivo general de la investigación fue determinar la importancia de la auditoría forense como mecanismo efectivo en la detección de los fraudes financieros en Colombia.
Propuesta Metodológica para la Detección y Prevención de Fraudes de Lavado de Activos en empresas del Sector Inmobiliario Empleando Herramientas de Análisis de Datos Lógicos	Rojas, Rosangela	El objetivo general de esta investigación fue diseñar una propuesta metodológica para la detección y prevención de fraudes de lavado de activos en empresas del sector inmobiliario, empleando herramientas de análisis de datos lógicos.
Estrategia de auditoria forense para la prevención de fraudes empresariales	Quevedo Manuel; Ramón Glenda; Barahona Pablo; Cabrera Glenda; Quevedo Jorge	El objetivo general de la investigación fue diseñar una estrategia de auditoría forense para la prevención de fraudes empresariales, que permitiera abarcar las metodologías adecuadas, a fin de contribuir con el buen manejo del dictamen sobre la incidencia de los estados contables como una contribución para los sistemas administrativos.
Auditoría Forense aplicada al Sistema de Créditos de la cooperativa de ahorro y crédito Jardín Azuayo, Oficina Cuenca	Camposano Susana; Moyano Jessica	El objetivo general de la investigación fue el análisis Forense al Sistema de Créditos de la Cooperativa de Ahorro y Crédito "Jardín Azuayo", Oficina Cuenca
Systematic Literature Review: Success, Failure, Risks, Benefits and Barriers Factors in the Adoption of Open Source Software	Carvallo Juan; Crespo Esteban; Carvajal Fabian; Vintimilla Rosalva	El objetivo se basó en la identificación del punto de partida del desarrollo del Software Libre, a través de estudios primarios más relevantes y de la definición y la posterior aplicación de cadenas de búsqueda, en bases de datos seleccionadas y así como la evaluación de la calidad de los artículos a través del protocolo de revisión diseñado para este estudio
Metodología de Seguridad de la Información para la gestión del Riesgo Informático aplicable a MPYMES	Crespo Esteban	El objetivo general fue proponer una guía metodológica para la identificación de riesgos y mitigación de los mismos dentro de los sistemas informáticos de una MPYMES, cuyo resultado se denomina ECU@Risk.
Ecu@ Risk, Una metodología para la gestión de Riesgos aplicada a las MPYMEs	Crespo Esteban	El objetivo general fue el análisis de diversas metodologías para la gestión de riesgos de seguridad de la información aplicables al entorno empresarial y organizacional del sector ecuatoriano de MIPYME
Propuesta de modelo de gestión de calidad de servicio de Tecnologías de Información en el sector PYME basado en COBIT, COSO, ITIL y las prácticas de la industria	Crespo Esteban; Torres Adrián	El objetivo general es el análisis y revisión de aspectos bibliográficos fundamentales y de investigación de las diferentes normativas tanto de gobierno corporativos como de gestión.

Elaboración Propia

A continuación, en la tabla 2, se detallan las estimaciones del lavado de dinero en cuentas corrientes como porcentaje del PIB real nacional, por provincia y región, emitidas por la Fiscalía General del Estado. Como se menciona, en el Ecuador, para el período 2014-2017, el 4,65% del PIB real es producto del lavado de dinero en cuentas corrientes, esto en valores nominales corresponde a $4130 millones de dólares. Además, en la misma tabla se observa que en la región Costa dicha estimación presenta menor variación entre sus provincias que en la región Sierra; esta actividad en promedio entre los años 2014-2017, por región es mayor que el de la Sierra, 2,53% frente al 1,97%.

Por otro lado, la provincia en la que se lava más dinero en promedio en cuentas corrientes es Guayas, es decir, el 0,83% del PIB real nacional. Le sigue Pichincha con 0,78%, Manabí con 0,72%, Azuay con 0,55% y el Oro con 0,30%, dichas cifras representan un porcentaje del PIB, no del porcentaje total. Las provincias del Oriente tienen el más bajo porcentaje de lavado de dinero en cuentas corrientes, en promedio este, es igual que la región Insular [18].

Por último, los resultados también muestran que el lavado de dinero ha disminuido; siendo en el año 2014 de 5,58% y llegando a ser en el 2017 de 3,73%, esta tendencia también se aprecia en el monto de lavado en términos nominales; posible consecuencia de los controles con mayor intensidad implementados por el gobierno en años anteriores.

TABLA 2 ESTIMACIÓN DEL LAVADO DE DINERO, POR PROVINCIAS Y REGIONES, PERÍODO 2014-2017

REGIÓN	PROVINCIAS	2014	2015	2016	2017	Promedio
COSTA	Guayas	1.0020%	0.8696%	0.7957%	0.6435%	0.8277%
	Manabí	0.6414%	0.8287%	0.7413%	0.6768%	0.7220%
	El Oro	0.3853%	0.3110%	0.2564%	0.2413%	0.2985%
	Santo Domingo	0.3132%	0.2442%	0.2156%	0.1913%	0.2410%
	Santa Elena	0.2009%	0.1380%	0.1188%	0.1066%	0.1411%
	Los Ríos	0.1999%	0.1507%	0.1387%	0.1228%	0.1530%
	Esmeraldas	0.1930%	0.1467%	0.1355%	0.1147%	0.1475%
	Total	*2.9356%*	*2.6889%*	*2.4020%*	*2.0970%*	*2.5309%*
SIERRA	Pichincha	0.9220%	0.8237%	0.7725%	0.6142%	0.7831%
	Azuay	0.6833%	0.5865%	0.5031%	0.4109%	0.5460%
	Tungurahua	0.3278%	0.2357%	0.1989%	0.1575%	0.2300%
	Imbabura	0.2225%	0.2010%	0.1569%	0.1336%	0.1785%
	Chimborazo	0.1136%	0.0817%	0.0732%	0.0742%	0.0857%
	Loja	0.0952%	0.0899%	0.0784%	0.0637%	0.0818%
	Cotopaxi	0.0655%	0.0494%	0.0383%	0.0382%	0.0478%
	Cañar	0.0165%	0.0058%	0.0108%	0.0099%	0.0108%
	Carchi	0.0073%	0.0068%	0.0077%	0.0071%	0.0072%
	Bolívar	0.0033%	0.0029%	0.0034%	0.0042%	0.0034%
	Total	*2.4569%*	*2.0834%*	*1.8433%*	*1.5134%*	*1.9742%*
ORIENTE	Orellana	0.0589%	0.0359%	0.0225%	0.0199%	0.0343%
	Sucumbíos	0.0319%	0.0238%	0.0218%	0.0204%	0.0245%
	Pastaza	0.0059%	0.0103%	0.0049%	0.0046%	0.0064%
	Napo	0.0039%	0.0041%	0.0022%	0.0019%	0.0030%
	Morona Santiago	0.0030%	0.0022%	0.0015%	0.0010%	0.0020%
	Zamora Chinchipe	0.0023%	0.0022%	0.0025%	0.0027%	0.0024%
	Total	*0.1060%*	*0.0785%*	*0.0554%*	*0.0505%*	*0.0726%*
INSULAR	*Galápagos*	0.0781%	0.0685%	0.0795%	0.0660%	0.0730%
	TOTAL	5.5766%	4.9193%	4.3801%	3.7270%	4.6508%

Fuente: Fiscalía General del Estado [18]

En este sentido, las estadísticas en Ecuador demuestran un incremento de estos delitos, los cuales mayormente son causados por ejecutivos que laboran internamente en el banco, que componen a mafias o delincuentes organizados, revelando una grave falta de ética por parte de los empleados, siendo capaces de traicionar la confianza otorgadas a dichos cargos.

De esta manera, la Fiscalía General del Estado reporta altos índices relacionados con el fraude bancario, incremento que se visualiza desde el año 2009, siendo el fraude en cajeros automáticos de mayor incidencia en el Ecuador, generando un gran impacto para la institución financiera, obligándose a invertir en avanzados y costosos programas, así como en contratar personal que supervise, controle y monitoree.

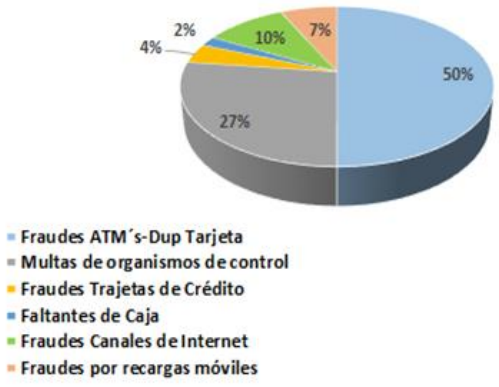

Figura 1: Distribución de los mecanismos de fraude en Ecuador 2018.
Fuente: Fiscalía General del Estado [18]

Cabe destacar que, los beneficios que se adquieren de diversas actividades delictivas ha sido una práctica desarrollada dentro del sistema bancario y financiero, sin embargo, se ha utilizado el mismo para la transformación de capitales de origen ilícito, derivados de la comisión de delitos graves, en dinero libre de sospecha.

III. METODOLOGÍA

Para esta investigación se aplicó un enfoque cualitativo, ya que se describieron ciertas características observadas en el campo de estudio, por medio de un grupo elegido como objeto de estudio. En este sentido, se recopilaron y analizaron 12 casos de fraude, sucedidos en diversas entidades financieras, identificadas mediante el muestreo por conveniencia en base al reporte de la Fiscalía General del Estado, aplicando entrevistas directas a funcionarios y auditores de bancos ubicados en las ciudades descritas en el reporte.

Por lo tanto, el tipo de investigación es descriptiva, ya que se procedió a analizar, describir la información obtenida en el campo objeto de estudio. Cabe destacar que, el diseño de este estudio se define como no experimental, ya que los datos se recopilaran directamente de la muestra seleccionada.

Igualmente, la investigación será no experimental, ya que no se procederá a manipular las variables en estudio, se analizarán los fenómenos en el lugar de estudio. Por otra parte, se precisa para este estudio un corte transversal, ya que el estudio se está aplicando para un solo período, en este sentido los datos que se recolectarán serán válidos para el período en que fue recopilada, es decir 2018.

De igual manera, la metodología presenta las bases legales que fundamentan la investigación, en el caso de Ecuador, se mencionan la Ley Orgánica de Transparencia y Acceso a la Información Pública [24], la cual establece el derecho a acceder a las fuentes de información, como mecanismo para ejercer la participación democrática en cuanto al manejo de lo público y por ende la rendición de cuentas a la que están sujetos todos los funcionarios y entidades del Estado, incluidos los actos, contratos y gestiones de las instituciones del Estado y aquellas financiadas con recursos públicos.

Así mismo, esta investigación se enmarca en la Ley General de Instituciones del Sistema Financiero [25], la cual establece que, la auditoría basada en riesgos depende del nivel de desarrollo que la propia institución del sistema financiero ha alcanzado en la gestión de riesgos en el área objeto de examen, y el grado en que han sido definidos objetivos determinados por la gerencia contra los cuales pueden medirse los riesgos asociados.

IV. RESULTADOS

1) Casos de Fraude y Lavado de Activos

Caso 1: En una entidad financiera de la provincia del Pichincha, con calificación de riesgo AAA-, para el año 2018, se entregaban tarjetas de coordenadas en fundas transparentes, donde una persona de servicio al cliente sacaba una copia de las tarjetas a escondidas mismas que contenían códigos clave de seguridad bancaria requeridas para realizar operaciones que impliquen movimiento de fondos.

Se evidenció que la empleada empezó a hacer fraude, ya que tomaba el usuario, contraseña y la fotocopia de las tarjetas de coordenadas, la cual se entregaba en un sobre de plástico transparente.

Medida de Mitigación: Como prevención en el área de Servicios bancarios de esta entidad, se estableció como política que el personal del área no puede crear contraseñas y generar usuarios a los clientes, y que la entrega de tarjetas se la debe realizar en sobres resistentes a la alteración (en inglés tamper resistant evident security envelopes).

Análisis: Los resultados evidencian la necesidad de un control interno más riguroso en la entidad financiera, además de una incorrecta manipulación de los instrumentos bancarios, por parte del personal del área, lo que significa una vulnerabilidad en la seguridad de los datos de los clientes y según las fuentes consultadas de la superintendencia de bancos, es obligación de las entidades financieras adoptar medidas de control, orientadas a prevenir y mitigar los riesgos en la realización de transacciones, las cuales pueden ser utilizadas como instrumento para lavar activos, u otros delitos.

Caso 2: En una entidad financiera de la ciudad de Guayaquil, con calificación de riesgo AA+, para el año 2018, se presentó que un empleado que se desempeñaba como técnico de sistemas se hizo amigo de las cajeras de una institución bancaria, éste tenía acceso a las cámaras, contraseñas y sistemas de asistencia remota.

El técnico visualizaba por las cámaras al momento que la cajera se iba al almuerzo, aprovechándose de este momento se conectaba vía remota y efectuaba una transferencia ficticia a otro banco, donde otra persona realizaba el cobro, producto de esta estafa, el valor transferido superaba los $200.000. Se determinó que la persona implicada tenía incompatibilidad de funciones.

Medida de Mitigación: La entidad ejecutó como plan de acción que se efectúen controles y cuadres intermedios para determinar de forma oportuna alguna anomalía, así como la segregación de funciones, según lo recomienda ECU@Risk y COBIT 5.

Análisis: Como se puede observar, el personal involucrado en este tipo de fraude cumplía funciones relacionadas directamente con el control interno en la institución, en este caso el área de cumplimiento de los bancos es la responsable de monitorear todos los movimientos y transacciones, con el objeto de identificar aquellos que puedan estar incidiendo en el blanqueo de capitales, por medio de procedimientos que

informen aquellas transferencias infundadas, o movimientos sospechosos que emitan señales de alerta temprana y según referencias consultadas con la utilización de la herramienta COBIT 5 se puede desarrollar una política clara que permita el control de las tecnologías en la organización, el cumplimiento regulatorio y aumentar así el valor asociado al área involucrada en la organización.

Caso 3: En una institución bancaria de la provincia del Guayas, con calificación de riesgo AA+, para el año 2018, un técnico se involucró sentimentalmente con la Gerente de Talento Humano Zonal.

Entre las funciones del técnico estaban las de realizar el cuadre de los cajeros ubicados en un casino. Cierto día el técnico comunica al Gerente de Sistemas, por correo electrónico, que ha decido renunciar de forma irrevocable, aduciendo que se va de viaje.

Se dieron indicios de cambio de comportamiento en cuanto a condiciones de vida social por parte del técnico, lo que daba sospechas del fraude. El valor de la estafa fue de $80.000. En el rastreo del origen del correo, el técnico enviaba el mensaje desde una cabina en Chile.

Medida de Mitigación: Luego de lo sucedido se procedió a desvincular a la Gerente de Talento Humano zonal y a realizar el rastreo de los correos electrónicos, con la finalidad de encontrar indicios de estafa. Además, se hace un monitoreo de relaciones sentimentales entre departamentos incompatibles, así como la aplicación de la ley de nepotismo.

Análisis: Con respecto a este caso, se evidencia la persuasión del personal directivo por parte de un integrante del personal subordinado, en el cual es necesario aplicar procedimientos que permitan reforzar las políticas internas en relación a la contratación del personal en dicha institución, posterior a este proceso deben tomarse diversas acciones para prevenir este tipo de riesgo y analizar posibles inconsistencias internas, a través del uso de sistemas basados en normas internacionales para mejorar la gestión de riesgos de la información, enmarcados en ISO 31000, 9001, 27005 y 37001.

Caso 4: En una institución financiera, de la provincia del Azuay, con calificación de riesgo AA+, para el año 2018, se detectó que se podían realizar transacciones en ventanillas con libreta de ahorro falsa.

Se comprobó que el personal de ventanilla de ciertas agencias efectuaba el pago a transacciones generadas por usuarios que podrían retirar dinero utilizando fotocopias de la libreta y cédula, comprobando la omisión a las políticas de seguridad exigidas para el personal de Cajas. En la auditoría, se detectó que las cajeras no utilizaban el lector ultravioleta para verificar las características de marca de agua que presentan las cartolas de las libretas como medida de seguridad.

Medida de Mitigación: Como control en la entidad financiera, se dispuso como obligatorio el uso de las lámparas ultravioletas así como el uso de lectores de huella digital para la aprobación de transacciones que superan los $5.000 USD, además del establecimiento de una política que notifique cuando una transacción realizada en ventanilla utilice medios de verificación alterados o suplantados, y sanciones ante el incumplimiento de las disposiciones que van desde una amonestación hasta el despido en caso de ser recurrente.

Análisis: Con relación a este caso, se puede observar que el perfil de los clientes fue vulnerado, ya que cada cliente de dicha entidad financiera tiene asignado un perfil, que describe lo que se espera que sea su transaccionalidad, empleando variables como lo son, el tipo de transacción, monto, frecuencia, ubicación, canal, volatilidad y crecimiento. Por otra parte, es necesario la obligación por parte de las entidades financieras, a establecer criterios en sus políticas y respectivos manuales que les permitan fortalecer, con un enfoque basado en riesgos, su régimen de prevención de fraude y de lavado de dinero.

Caso 5: En una institución financiera de la provincia del Azuay, para finales de los 90s, en este caso, se vinculó un nuevo gerente de sistemas, quien llegó por primera vez a su cargo en un vehículo estándar y una vida sin lujos ni pretensiones. Sin embargo, luego de unos 7 u 8 meses, el gerente tuvo un cambio de actitud y de estilo de vida. No dejaba que nadie toque la plataforma de sistemas de ahorro y cuentas corrientes, y había cambiado su viejo auto por un flamante Mercedes Benz; además tenía ya una casa más lujosa y un departamento en la playa. La actitud de la persona se volvió sospechosa, y cuando se realizó la auditoría, en el código fuente se identificó una modificación al algoritmo de cálculo de intereses. Todos los sobrantes que correspondían a las fracciones de mil (por ejemplo, de un valor 25,7899 USD los 00,0099 centavos) pasaban a otra cuenta, registrada a nombre de esta persona. Así, con un considerable número de clientes y operaciones de cálculo diarias, esas fracciones de centavos se convirtieron en una cantidad significativa.

Medida de Mitigación: La medida que aplicó la entidad financiera fue la certificación de código fuente, la compilación del programa y el almacenamiento de este en un sitio seguro a manera de mantener monitoreos continuos por parte del área de ciberseguridad y de auditoría informática.

Análisis: Con respecto a este caso, se evidencia complicidad por parte de un gerente y del personal del área de tecnología, encargado de modificar los algoritmos en el cálculo de intereses, de esta manera es necesario aplicar el procedimiento para evaluar una operación inusual, lo cual debe estar claramente señalado en el manual de prevención de la institución. De esta manera, el personal encargado de dicha función adquirirá seguridad respecto de sus deberes y acerca de la forma de cumplirlos al momento de evaluar las transacciones inusuales detectadas, como también ante el eventual requerimiento posterior de una autoridad administrativa encargado de la sanción respectiva.

Caso 6: En una institución financiera, en la provincia de Azuay, con calificación de riesgo AA+, para el año 2018, se suscitó en años anteriores que cuando una cuenta de ahorros o corriente era declarada como cancelada o cerrada y presentaban saldos, según el catálogo de cuentas de saldos del banco se tenía que reclasificar a una cuenta contable, pero al parecer existió una mala disposición de la entidad financiera, porque cuando hablaban de una cuenta contable hacían referencia a que todas esas cuentas de ahorros y corrientes estén dentro de una cuenta del grupo 21 de depósitos a la vista y la entidad lo que hacía era debitar de estas cuentas de ahorros o corrientes y acreditar a una cuenta 25 de saldos por devolver y como este proceso no tenía mayor control, el personal que realizaba los cuadres o ajustes de las cuentas 21 de depósitos a la vista, han estado tomando el dinero aprovechándose que se trataba de cuentas de clientes fallecidos, o que simplemente no reclamaban sus valores y en lugar de enviar al Tesoro Nacional se acreditaban a las cuentas personales.

Medida de Mitigación: Como plan de acción para mitigar el riesgo, la Institución dejó de procesar los débitos de las cuentas de los clientes de cuentas cerradas y canceladas para reclasificar contablemente los saldos, además se centralizó el control de esas cuentas en la Agencia Matriz, de manera que se cumpla con lo estipulado en el Código Orgánico Monetario y Financiero, sección Disposiciones Generales "Sexta: Pasivos y saldos inmovilizados. Los pasivos que hubieren permanecido inmovilizados en cualquier entidad del sistema financiero nacional por más de cinco años con un saldo de hasta el equivalente al 25% de un salario básico unificado, o por más de diez (10) años con un saldo mayor, por no haber sido reclamados por su beneficiario desde la fecha en que fueren exigibles, serán transferidos a la Cuenta Única del Tesoro Nacional, con excepción de los pasivos inmovilizados por disposición legal o judicial debidamente notificadas a la entidad financiera."

Análisis: El caso anteriormente expuesto, detalla la importancia de tener una cultura de riesgo dentro de las empresas, ya que, dependiendo del plan y una política para gestionar el riesgo, se logrará implementar los controles, basados en unos razonamientos y reglas claras y específicas que se comuniquen en toda la compañía. Así mismo, la entidad debe contar con un manual sobre buenas prácticas para prevenir el lavado de activos, el cual, pueda ser consultado por los empleados cuando necesiten saber qué herramientas usar, cómo actuar y de qué manera prevenir.

Caso 7: En una institución financiera, ubicada en Ambato, con calificación de riesgo AA-, en el año 2016, se detectaron acciones ilícitas por parte de la supervisora de cajas quien era encargada del custodio, manejo y arqueo del dinero de las bóvedas y recarga de los cajeros automáticos, quien, abusando de sus funciones, presuntamente realizó las recargas de los ATMs adulterando las planillas con valores distintos a los que fueron físicamente ingresados.

Los auditores procedieron a verificar los cuadres efectuados conjuntamente con la implicada, donde se revisaron los arqueos de cajas y la documentación física de respaldo. Se detectó un faltante de $124.000,00 en dos recargas efectuadas a los cajeros. La exfuncionaria fugó luego del inicio de la investigación y tras la formulación de cargos.

Medida de mitigación: Con la obtención de estas pruebas se dictó sentencia condenatoria por delito de peculado previsto y sancionado en el artículo 278 del Código Orgánico Integral Penal. La entidad financiera como plan de acción para mitigación del riesgo dispuso un mayor control en los cuadres efectuados en Cajas y ATMs.

Análisis: Con respecto a este caso expuesto, se evidencia que el hecho de revelar la participación de empleados en situaciones de fraude, corrupción y lavado de dinero representa uno de los mayores retos que afrontan las entidades financieras, sin embargo, este reto es mayor cuando el criminal ocupa cargos claves para enfrentar estos delitos. En este caso, se deben establecer controles y programas dentro de la institución, que permitan detectar los reportes de cuadres de caja, en cada cajero automático y disponer de un sistema basado en tecnología para seguimiento y análisis de operaciones inusuales.

Caso 8: En al año 2015, en la Provincia de Azuay, en una entidad financiera con calificación de riesgo AA-, se presentó un caso en el que no se habían dado cuenta de la infiltración de hackers, donde se valieron de mensajes fraudulentos en el sistema SWIFT (sistema de mensajería global interbancario) para mover 12 millones de dólares a diferentes bancos del mundo, entre estos 9 millones fueron al banco de Hong Kong y los 3 millones se enviaron a Dubái y a otros lugares.

La entidad ecuatoriana presentó una demanda contra el banco estadounidense Wells Fargo, que ordenó la mayor parte de transferencias por los 9 millones de dólares. Los ladrones cibernéticos utilizaron las credenciales de los empleados de Wells Fargo en el sistema SWIFT para transferir los valores a sus cuentas en el extranjero.

Medida de mitigación: La entidad financiera realizó evaluaciones de seguridad para asegurarse que sus redes sean seguras y evitar futuros ataques, así como la actualización de software de la interfaz de Alliance Access de SWIFT, con la finalidad de identificar situaciones en la que los hackers intenten ocultar sus rastros.

Además de nuevos monitoreos a través del aplicativo monitor plus (control y monitoreo en línea de transacciones fraudulentas), donde intervienen el departamento de cumplimiento y monitoreo transaccional.

Análisis: En este caso, se observa la vulnerabilidad del sistema y el riesgo que representa la falta de actualización de este, por esta razón se considera necesaria en la institución financiera la implementación de las buenas prácticas concentradas en el marco de referencia COBIT, lo cual permitirá la integración con la tecnología de la información para así alcanzar los mejores resultados con relación a la Gestión del Riesgo Operativo de las Tecnologías de Información.

Caso 9: En una institución financiera, en la Provincia de Azuay, con calificación de riesgo AA+, en el año 2018, se detectó un caso de fraude donde grupos de ciudadanos venezolanos habían clonado tarjetas de un banco de Venezuela para realizar transacciones en hoteles de Ecuador, utilizando pagos a través de Western Union, suplantando diferentes identidades y clonando tarjetas, entonces los ciudadanos venezolanos pagaban las reservas que iban a tener en hoteles a través de compras a domicilio (llamar y proporcionar los datos de la tarjeta), donde los hoteles establecían una tarifa por noche de acuerdo al número de huéspedes donde se adicionaba la comisión del hotel, el fraude radica en la clonación de las tarjetas y el principal perjudicado era el comercio es decir el hotel, porque estaba realizando las reservaciones con tarjetas adulteradas, entonces una vez que era autorizada la transacción con estas tarjetas, después de un mes los tarjetahabientes que eran los titulares de las tarjetas recibían valores extraños cargados a sus cuentas, los cuales ellos no habían consumido, entonces ellos procedían a efectuar los reclamos en la institución y resultando estos reclamos como pérdida para la institución financiera por los pagos realizados.

Medida de Mitigación: La entidad financiera levantó políticas de control al momento de la afiliación de locales comerciales, además en el contrato de afiliación se incluyó un numeral donde consta una garantía para cubrir eventos de fraude.

Análisis: En el caso anteriormente expuesto, se observa la vulnerabilidad de la seguridad en las tarjetas de los clientes, lo cual genera reclamos por parte de los clientes afectados, ocasionando altos costos para la entidad financiera. De esta manera se deben implementar políticas de control que

permitan garantizar a los clientes respuestas inmediatas ante posibles fraudes.

Caso 10: En una institución financiera, en la provincia de Azuay, con calificación de riesgo AA+, en el 2018, se presentó un caso donde existían negocios que necesitaban transaccionar con la máquina POS (pagos a través de tarjetas de débito y de crédito), los mismos que se afiliaban a la institución financiera indicando en el RUC la actividad comercial como (bares y discotecas), donde en los primeros 3 meses empezaban a tener una facturación entre $2.000 a $3.000 mensual, pero después empezaba a incrementar la facturación de forma inusual en valores de $50.000 a $60.000 en adelante siendo cantidades bastante altas. Cuando empezaron a existir reclamos en tarjetas provenientes de estos comercios y además los volúmenes de facturación eran demasiado altos al provenir de un bar discoteca, se realizó una investigación por parte de los asesores comerciales y el Departamento de prevención de fraudes, quienes realizaron visitas a estos negocios y descubrieron que no eran discotecas sino funcionaban como night club. Cuando se solicitaron los sustentos del incremento en las transacciones se percataron que las facturas no contaban con todos los requisitos que exigía el SRI, no tenían realizadas las declaraciones, la información se encontraba desactualizada, además el representante legal poseía algunas demandas por estafa en algunas ciudades y en otros países.

Medida de Mitigación: Se procedió a retirarles la máquina POS al negocio y se inmovilizaron los fondos en la cuenta, para al momento de recibir reclamos por parte de los tarjetahabientes efectuar parte de la devolución, de manera que no exista una alta pérdida financiera.

La entidad financiera levantó políticas de control al momento de la afiliación de locales comerciales, además en el contrato de afiliación se incluyó un numeral donde consta una garantía para cubrir eventos de fraude.

Análisis: En el caso anterior, se expone que la institución financiera no posee el control de los equipos de punto de venta, ni de las transacciones que se realizan en dichos establecimientos, lo que incrementa el riesgo de cometer fraudes, de igual manera los establecimientos incumplían con sus obligaciones a nivel tributario, lo que evidencia la importancia de la disposición de políticas y normativas internas en dicha institución que permita evitar este tipo de riesgo.

Caso 11: En una institución financiera, en la provincia de Manabí, con calificación de riesgo AA+, para el 2018, se presentó un caso relacionado a comercios con facturación no acorde al giro del negocio, donde en la ciudad de Manta, provincia de Manabí, un señor era propietario de un hotel con capacidad para 20 personas y de forma inusual el comercio empezó a facturar valores por $60.000 a $70.000, entonces el análisis consistió en determinar cuál era la verdadera actividad que desempeñaba el señor para obtener esos volúmenes tan altos de dinero. En el análisis de facturación de los últimos 3 meses el propietario del hotel como máximo mensualmente facturaba entre $900 a $1200, cuando de forma inusual en un mes empezó a facturar montos de $20.000 en delante de forma semanal, después de realizada la investigación se determinó que el propietario se encontraba clonando tarjetas del exterior y utilizando la máquina POS para estos fines ilícitos, lo que generó pérdidas para la institución financiera, después de atravesar procesos de contra cargo de tarjetas la institución financiera no pudo recuperar un valor que ya fue pagado al comercio.

Medida de Mitigación: La entidad financiera levantó políticas de control al momento de la afiliación de locales comerciales, además en el contrato de afiliación se incluyó un numeral donde consta una garantía para cubrir eventos de fraude.

Análisis: En el caso anteriormente expuesto, se observa que la institución bancaria no aplica controles preventivos que eviten estos tipos de fraudes vinculados con el establecimiento comercial, lo cual demuestra que es necesario establecer adecuadas políticas de control que permitan evitar este tipo de fraude que genera pérdidas económicas a la institución.

Caso 12: En una institución financiera, en la provincia de Esmeraldas, con calificación de riesgo BBB-, para el año 2009, el gerente de Sucursal identificó una vulnerabilidad en el sistema informático bancario, el cual funcionaba en ambiente web. La debilidad fue identificada a través de la técnica de Cross-Site Scripting, la cual se utiliza para alterar el mensaje que circula por la barra de navegación de un sitio web. Con esta técnica, esta persona tenía la capacidad de modificar la línea de código (www.entidadbancaria.com/?trans=1000&and&dest=cta) donde cta era el número de la cuenta de acreditación del saldo. El número de cuenta era visible en la trama del navegador, la cual se cambió durante el envío de mensaje y se produjo el fraude.

Medida de mitigación: La entidad, tomando contramedidas, realizó modificaciones al código informático para que los datos sensibles no sean visualizados en la trama del navegador.

Análisis: Se observa una vulnerabilidad informática en el sistema bancario que era susceptible a la técnica de ataque XSS, técnica utilizada para la modificación de tramas en el envío y recepción de datos. Al hacer esta práctica, se podía variar los valores (en el ejemplo trans=1000 podía variarse a trans=10) y hacer una repetición de transacciones. Además, se podía cambiar el valor (en el ejemplo trans=1000 podía variar a trans=100000) lo que permitió identificar una transacción anómala y fue la forma en la que se detectó este fraude.

V. Propuesta de una Guía metodológica para la prevención de Lavado de activos y fraude electrónico basada en las normas ISO 31000, ISO 9001:2015, ISO 27005, ISO 37001 y en el marco de gobierno COBIT 5

La guía metodológica que se propone incluye una introducción, el objetivo o propósito de esta y los procedimientos y procesos que la conforman, basada en las normas ISO 31000, ISO 9001:2015, ISO 27005, ISO 37001 en el marco de gobierno COBIT 5, en base al estudio de casos financieros y procedimientos utilizados por las entidades financieras para la prevención de delitos y fraudes, así como lavado de activos.

Adicionalmente, se propone como complemento a la guía metodológica, proporcionar al auditor forense una herramienta de procedimientos enfocados a detectar, identificar y prevenir fraudes de lavado de activos, el cual se detalla en los párrafos siguientes. Es importante mencionar que, los procedimientos de auditoría forense deben

desarrollarse en dos etapas, en una primera fase se evalúa a la entidad y en la segunda etapa se desarrollan los procedimientos [26].

Fase 1: Evaluación del cliente: en esta etapa el auditor debe enfocarse a realizar el proceso de planeación de la auditoría, del cual forma parte el conocimiento del cliente, para lo cual el auditor deberá solicitar: los estados financieros de los últimos 3 o 5 años, firmados por los funcionarios responsables, con los cuales se realizará la revisión analítica de las variaciones significativas e inusuales. Además, se debe recopilar los antecedentes bancarios de los miembros del Directorio y Accionistas de la Compañía, así mismo, se procederá a analizará el entorno del sector con el fin de verificar, a través de la revisión analítica, aquellas posibles variaciones detectadas relacionadas con la evolución del mercado.

Fase 2: Procedimientos de auditoría: en dicha fase se desarrollarán los principales procedimientos: a través de entrevistas realizadas a la Gerencia que posee la entidad, en relación a las políticas y procedimientos antifraude. Seguidamente, se requiere de un seguimiento sobre comunicados de no cumplimiento de la normativa sobre procedimientos de prevención de fraude de lavado de dinero, en el caso de existir dichas políticas. Adicionalmente, se debe conocer la estructura organizacional actual de la entidad, así como las capacitaciones realizadas al personal en relación a temas sobre riesgo inherente de la actividad, valores éticos, y el conocimiento del cliente.

Es importante mencionar que, dichos procedimientos expuestos anteriormente, fueron extraídos de las entrevistas realizadas a los expertos de contabilidad y auditoría; los mismos se categorizan y desarrollan con amplitud. Adicionalmente, se detallan las tipologías de lavado de activos con sus pertinentes señales de alerta, a continuación, se desarrollan dichos procedimientos de auditoría enfocados a cada tipología y al comprender el funcionamiento de cada tipología, previamente identificadas y basadas en las señales de alerta, permitirán al auditor identificar oportunamente la ocurrencia de estas tipologías. Para el desarrollo de esta propuesta metodológica se seleccionaron las señales de alerta aplicables a cada tipología y se desarrollaron los procedimientos de auditoría acordes a cada señal de alerta [27].

Por otra parte, el primer procedimiento de la guía en relación al proceso de Gestión de Riesgo, consiste en determinar los roles y responsabilidades del personal que debe soportar y participar en los procedimientos utilizados, así como la metodología considerando el ciclo de un sistema para la gestión de riesgos informáticos, el cual se desarrolla en cuatro etapas: Planificar, Ejecutar, Verificar y Actuar; conformando así procesos de gestión, un proceso de monitoreo y control, y un proceso comunicacional, utilizando estándares internacionales como la Norma ISO 31000, 9001, 27005, 37001 en el marco de gobierno COBIT 5.

Con respecto al ciclo de Demming o ciclo PEVA (por sus siglas en inglés, PDCA), en la primera fase, planificar, se establecen los objetivos y los lineamientos para gestionar el riesgo, con la finalidad de obtener resultados que cumplan las expectativas de las políticas de la empresa, así como de su misión y visión. Así mismo, en esta etapa, se elaboran diversos planes en el que se pueden abarcar todos los tipos de riesgos [12].

En la segunda fase, ejecutar, se relacionan todas las operaciones que deben ponerse en práctica para cumplir con los objetivos establecidos, a través de controles y procedimientos. Además, en esta etapa se realiza la valoración y reconocimiento de los riesgos de acuerdo con la recopilación de datos para determinar las estrategias para corregir y disminuir los riesgos.

Seguidamente, se procede a ejecutar la fase de verificación, que según Estupiñan [2] lo define como "*la revisión de los resultados obtenidos de las evaluaciones realizadas, para así describir si fueron satisfactorios, según la política y los objetivos planteados por la empresa, durante la planificación*". Esta etapa se desarrolla gracias a la medición de los riesgos y los impactos generados.

Finalmente, se desarrolla la fase actuar, la cual consiste en implementar los cambios requeridos en base a los resultados obtenidos, con el objetivo de establecer una política de gestión de riesgos a futuro. Así mismo, se procede con la mejora continua y el monitoreo constante de los riesgos.

Con respecto al COBIT 5, representa el óptimo enfoque para el gobierno y gestión de la TI empresarial, ya que permitirá adaptar el COBIT de modo efectivo en la integración de cada una de las normas internacionales en estudio para el fortalecimiento de la gestión de riesgo en las entidades financieras [28], así mismo permitirá ajustarse a los requisitos específicos de la empresa. El éxito de esta metodología dependerá de factores importantes como el compromiso y apoyo de la alta dirección, que permitan la orientación y directrices para la iniciativa de este tipo de herramientas, así como una comunicación efectiva garantizada y la habilitación de los cambios necesarios, de igual manera dependerá del enfoque en resultados inmediatos y priorizar las mejoras más favorables para la organización.

Para el estudio se aplicaría la metodología basada en la gestión de riesgo, la cual se detalla en una serie de etapas, según se describe a continuación en la Figura 1:

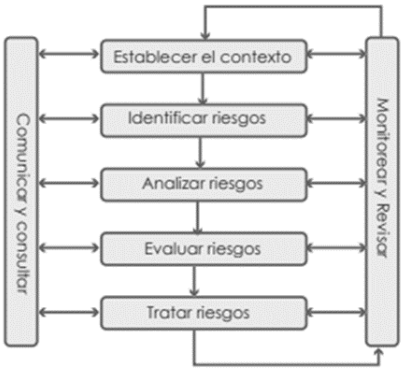

Figura 2 Proceso de Gestión de Riesgo *[28]*

Dicho proceso presentado en el Figura 1, se resumen en pasos descritos a continuación:

Etapa 1: Establecer un contexto: En esta etapa, se plantea efectuar un diagnóstico inicial, tanto del contexto interno como externo, con relación al riesgo de prevención de lavado de activos, específicamente en el sector de la banca privada.

Para el diagnóstico del contexto externo, se hará necesario un análisis PESTEL, el cual considera factores Políticos, Económicos, Socio-culturales, Tecnológicos, Ecológicos o

ambientales, y Legales [6]; los cuales afectan de una u otra manera a la organización y consecuente a su desarrollo.

Fundamentado en lo mencionado por los autores Azanza y Bermeo [6], recomiendan que, para realizar el análisis PESTEL, se debe seguir los siguientes pasos:

Paso 1. Definir y seleccionar el método apropiado para el tipo de organización, para lo cual se puede utilizar una de las siguientes opciones:

- Elaborar un análisis descriptivo por medio de investigaciones de mercado.
- Elaborar un foro, en el que se reúna a todos los involucrados del comité de Riesgo de Tecnologías de Información, y de forma consensuada, efectuar el análisis por medio de una lluvia de ideas, siendo imprescindible definir un moderador y un grupo focal.

Una vez elegido el método adecuado para su organización, se procede con el siguiente paso.

Paso 2. Delimitar la cobertura de la empresa en el país, siendo este: local, regional, nacional, internacional.

Paso 3. Investigar los componentes de cada uno de los factores del análisis PESTEL:

- **Factor Político:** se recomienda considerar los estudios de riesgo político que cada año son realizados por "AON" y por "MARSH", compañías internacionales dedicadas al análisis mundial de riesgos [6].

-**Factor Económico:** para la gestión de riesgo, se deben evaluar los "Indicadores Económicos del Banco Central del Ecuador", en el cual se encontrará información relacionada con tasas de interés, el producto interno bruto (PIB), el nivel de inflación, entre otros [6]. De igual manera se pueden examinar los datos económicos que publica el Instituto Nacional de Estadísticas y Censos (INEC) con la finalidad de conocer el estado económico del país y determinar su influencia en la organización.

En el caso del lavado de activos, se procederá a realizar el análisis financiero y económico, dentro de la institución financiera, a través de la Unidad de Análisis Financiero y Económico y como organismo legalmente facultado para solicitar y receptar con carácter de reservado la información sobre transacciones cuyos montos superen los indicios legales establecidos, incluyendo aquellas que se consideren inusuales e injustificadas, con la finalidad de realizar el respectivo análisis y determinar su esquema y origen.

En relación a lo anteriormente expuesto, se precisa detectar a través de los sujetos obligados alguna operación inusual, la cual puede convertirse en sospechosa basada en la información con la cual se dispone o solicitan de su cliente y en el caso de que exista carencia de fundamento económico o legal aparente, se puede sospechar que los fondos utilizados en esa operación proceden de alguna actividad ilícita [26].

-**Factor Socio–cultural.:** se analizan los datos que presenta el INEC, relacionados con el "Censo de población y vivienda", lo cual permitirá conocer los cambios del nivel poblacional, para así predecir comportamientos de consumo local, nacional e internacional, en base a la "Encuesta de Estratificación del Nivel Socioeconómico" [6].

-**Factor Tecnológico:** se evalúan, ya que hay que considerar los cambios tecnológicos y su evolución, motivado a que estos afectan a la industria donde compite la organización. En este sentido, Azanza y Bermeo [6], sugieren analizarlo en base a la información ofrecida por el INEC en su documento de estudio "Principales indicadores de Actividades de Ciencia, Tecnología e Innovación".

-**Factor Ecológico:** Otro aspecto significativo lo representan las regulaciones ambientales, que inciden en la imagen de la organización. Para lograrlo será significativo identificar las leyes relacionadas con la protección del medio ambiente, así como las que rigen el consumo de energía y agua, a elementos no renovables, al reciclaje de residuos, y la mitigación del impacto ambiental. Se sugiere establecer el contexto empresarial con base a los datos suministrados por el Ministerio del Ambiente del Ecuador [6].

-**Ámbito Legal:** representa a aquellas normativas que afectan a la empresa y en el que se considera el "Código del trabajo", las licencias y permisos requeridos por el área local y la Superintendencia de Bancos reguladora de las entidades financieras [6].

Paso 4. Se debe analizar los componentes de los factores PESTEL, diferenciándolos de acuerdo con cada una de las perspectivas que mantiene, permitiendo identificar de una manera más objetiva, los que inciden directamente a la organización.

Paso 5: Se procede a evaluar los componentes de los factores PESTEL, diferenciándolos de acuerdo con cada uno de los aspectos que la conforman, esto permitirá detectar los que inciden de forma directa en la compañía.

Paso 6: Se basa en priorizar cada una de las amenazas identificadas, independientemente del componente al cual corresponda. Este procedimiento debe repetirse considerando las oportunidades.

Por otra parte, para el diagnóstico del contexto interno es necesario aplicar ciertas herramientas:

1. **Matriz FODA:** Con ella se busca identificar los roles y responsabilidades de los empleados, el compromiso de estos para con la empresa, los componentes salariales, el nivel de madurez profesional. Su ejecución será a través de la revisión de manuales, la estructura organizacional y los procedimientos de la empresa. Para realizar el análisis interno, será necesario recabar las Fortalezas y Debilidades institucionales, así como las Oportunidades y Amenazas identificadas.

2. **7S de McKinsey:** Adicionalmente, se propone la aplicación de la herramienta de análisis McKinsey para el análisis Interno, el cual consiste en identificar los perfiles, actividades y roles de los colaboradores de la compañía; así como el de identificar su nivel de conocimiento sobre políticas y procedimientos organizacionales. Dicha propuesta de McKinsey facilita una herramienta basada en las 7S institucionales, que significa: Staff (personal), Structure (Estructura), Skills (Habilidades), System (políticas y procedimientos internos), Shared Values (Valores compartidos, como misión, visión, ética, valores), Strategy (Estrategias) y Style (Estilo de dirección). Dicha teoría argumenta que, si una de las S falla, el resto falla; y por lo tanto no se logra la continuidad del negocio.

Etapa 2. Identificar los riesgos: Desde el punto de vista de la administración de riesgos se persigue identificar el qué, por qué y cómo pueden producirse los eventos de riesgos, cuáles son sus causas y cómo se generaron los mismos. De esta manera se debe presentar las siguientes interrogantes [23]:

Qué puede pasar: ¿Qué podría ir mal, evitar el logro de los objetivos pertinentes? ¿Qué acontecimientos o sucesos podría poner en peligro los resultados esperados? ¿Cómo

puede pasar: ¿Qué pasó? ¿Es probable que pueda volver a ocurrir? ¿Qué factores podrían accionar su reincidencia? • Dónde puede suceder: ¿Dónde podría suceder? ¿Es probable que el riesgo ocurra en cualquier lugar o en cualquier contexto? ¿O es un riesgo que depende de la ubicación, área física o actividad? ¿Por qué podría suceder? ¿qué factores deben estar presentes para que el riesgo se materialice o vuelva a ocurrir? El comprender por qué un riesgo puede ocurrir o repetirse, es importante si se gestionará el mismo.

El proceso para identificar el riesgo se detalla seguidamente:

Paso 1: Identificar los controles existentes: consiste en conocer los controles que ya están implementados para mitigar el impacto del riesgo, los cuales pueden ser estrictos o permisivos; también pueden ser medible y repetible y pueden incluir legislación, políticas o procedimientos, formación del personal, la separación de funciones, medidas personales, equipos de protección, barreras físicas y estructurales.

Paso 2: En base a los resultados obtenidos, se deben identificar y clasificar las amenazas:

- Según el nivel de datos: está conformada por los archivos, ya sean resultados del manejo de una hoja de cálculo, de un documento de texto, de un gráfico o fotografía; o también puede ser considerado como un registro de una base de datos [23].
- Según el nivel de software: Hace referencia a las aplicaciones, programas o sistemas informáticos, en los cuales se incluye el sistema operativo, las hojas de cálculo, un procesador de texto, el sistema contable, el navegador de internet, etc. [23].
- Según el nivel de políticas, enfocados en la información o acceso no autorizado, además de evidenciar amenazas enfocadas en la desactualización de software del sistema y deficiencias de normas y manuales las cuales ocasionan grandes riesgos en el sistema [23].

Figura 3 Clasificación de los riesgos de información organizacionales, [23]

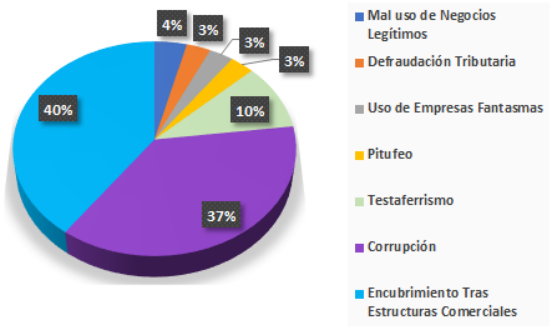

Figura 4 Clasificación de técnicas de lavado de activos 2018
Fuente: UAFE [29]

Etapa 3: Analizar los Riesgos, de lavado de activos y riesgos de información: una vez identificados los riesgos se plantea determinar los controles existentes para así analizar los riesgos y la posibilidad de ocurrencia del riesgo y su impacto en caso de materializarse los riesgos asociados, teniendo en cuenta los riesgos inherentes. A continuación, se describen los pasos:

Paso 1 Evaluar la probabilidad: Se recomienda que la probabilidad de que ocurra el riesgo sea clasificada en 5 niveles, es decir, descrita como muy bajo, bajo, medio, alto, muy alto de que ocurra.

Paso 2 Evaluar la consecuencia: se describen las consecuencias o potencial impacto de la materialización del evento serán descritas [23].

Paso 3 Valorar el nivel de riesgo: Para la valoración del nivel de riesgo se deberá utilizar la Matriz de Riesgo proporcionada a continuación; esto permitirá evaluar los niveles de probabilidad y consecuencia [23].

Matriz de Riesgos						
		Consecuencia				
		1. Leve	2. Menor	3. Moderado	4. Alto	5. Extremo
Probabilidad	E - Casi certero (frecuente)	M	M	A	E	E
	A - Probable	B	M	A	A	E
	M - Posible	B	M	M	A	A
	B - No muy común	B	B	M	M	A
	L - Raro	L	L	B	B	M

Figura 5 Clasificación de los riesgos de información organizacionales ECU@Risk, *[23]*

CAUSAS	CONSECUENCIAS	CONTROLES
1. Registros contables inadecuados	1. Afectación de la imagen y reputación. 2. Impacto negativo en la calificación de la empresa. 3. Sanción por las autoridades de control.	1. Correo de emisión de los estados financieros por parte del Director de Contabilidad al equipo de la Vicepresidencia Financiera.
2. No verificación de la información por parte de los responsables.		2. Revisión y aprobación del cierre contable por parte del Director de Contabilidad al equipo de la Vicepresidencia Financiera y VFO.
		3. Correo de remisión del informe financiero por parte de la Vicepresidencia Financiera a la Dirección de Asuntos Corporativos.

Figura 6 Proceso de Análisis de Riesgo en estados financieros *[6]*.

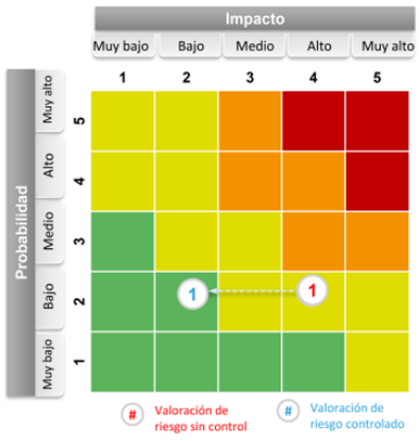

Figura 7 Proceso de análisis de probabilidad e impacto en estados financieros, *[6]*.

Etapa 4: Evaluar Riesgos: consiste en priorizar aquellos eventos de riesgos con una mayor calificación y con medidas más firmes y así repetidamente hasta llegar a niveles más bajos en la calificación. En esta fase se propone, utilizar la herramienta denominada mapa de riesgos, en la cual se realiza una medición semicuantitativa de los riesgos considerando los controles existentes, por lo tanto, los datos obtenidos son objeto de la información recolectada por el personal directivo asignado, que permitirá tomar decisiones respecto al tratamiento de riesgos obteniendo datos que son producto de estimaciones. Esta herramienta de medición, permitirá identificar cómo un evento determinado afecta a la empresa en términos monetarios (pérdidas económicas).

Esta fase se ejecutará por pasos para así determinar la manera en que se efectúa un mapa de riesgos, empleando una matriz de doble entrada:

Paso 1. Determinar los departamentos, unidades de negocio o procesos a evaluar. Se debe segmentar la empresa en Departamentos, Procesos o Líneas de negocio, en relación al tipo de empresa. Así mismo se debe clasificar los potenciales riesgos de fraude. Ejemplo. Aplicaciones fraudulentas de Crédito, Obtención fraudulenta de financiamiento, alteración contable, Transacciones no autorizadas, Apropiación indebida de activos, Soborno y corrupción, Lavado de activos, Sustracción de información y violación de IP, abuso de información privilegiada, Fraude fiscal, Espionaje a favor de los competidores.

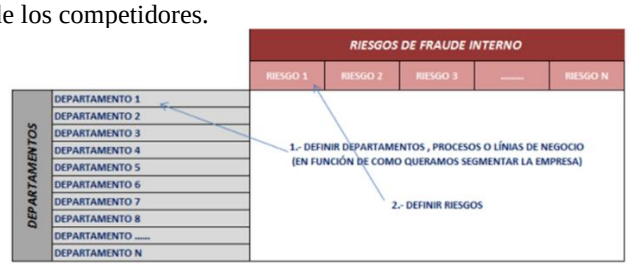

Figura 8 Mapa de Riesgos *[6]*.

Paso 2. En esta fase, para cada departamento, especificar los riesgos anteriormente identificados, para saber si aplican o no. De igual manera, se evaluarán los riesgos inherentes y los controles de riesgo históricos.

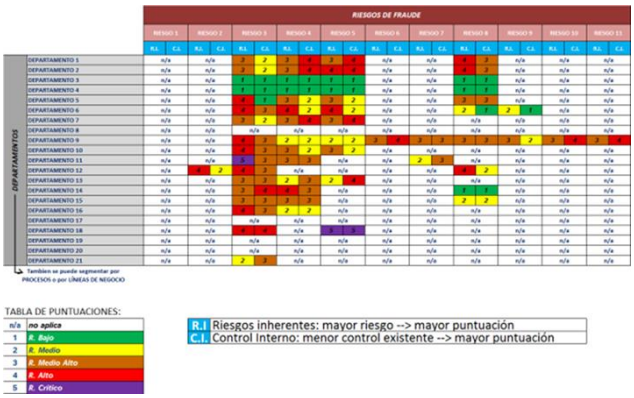

Figura 9 Cálculo del Mapa de Riesgos *[6]*.

Paso 3. En esta se obtiene el resultado de multiplicar los riesgos esenciales y las Investigaciones de riesgo, generando así el mapeo definitivo de los peligros de fraude de la empresa.

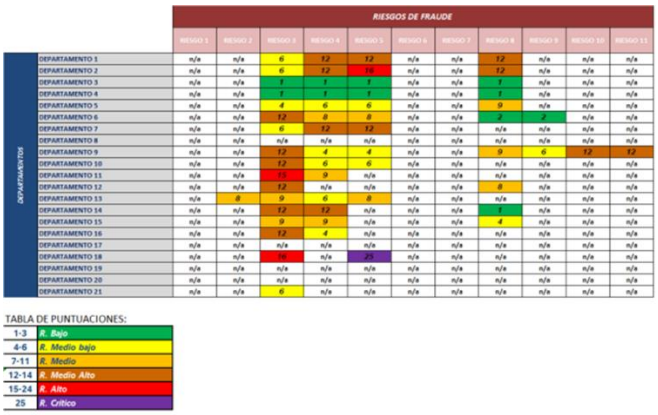

Figura 10 Resultados del Mapa de Riesgos *[6]*.

Etapa 5. Tratar o controlar los riesgos: consiste en diseñar e implementar las medidas que permitan controlar los riesgos inherentes identificados y así mismo, detectar operaciones inusuales y llevar a cabo el reporte de operaciones sospechosas, de ser el caso. Teniendo en cuenta la naturaleza del riesgo, con el objetivo de poder hacer el seguimiento a las operaciones de los clientes con el fin de determinar operaciones inusuales en unión con lo establecido en el marco normativo. De esta manera se empleará como herramienta la matriz de controles.

Figura 11 Matriz de Controles *[6]*.

Etapa 6. Monitorear y revisar: esta fase es de gran importancia, ya que es obligación de las instituciones financieras el revisar el desempeño y funcionamientos de los sistemas, periódicamente. Es importante destacar, que un sistema de administración de riesgos es un proceso basado en

mejora continua, con el fin de estabilizar los procesos y la posibilidad de mejora del sistema tomando acciones correctivas, preventivas y de eficiencia y eficacia de los controles implementados, con el objetivo de verificar su desempeño y estar precavidos para los cambios que sean necesarios.

Con esta investigación se propone, que el tratamiento del riesgo elaborado en la fase anterior se registre en un documento denominado "Plan de Acción para el Tratamiento de Riesgos", por medio del cual se deberá indicar actividades concretas (controles preventivos y mitigantes de ser el caso), fechas de implementación, responsables de las actividades, recursos necesarios y lo que se espera de dicha actividad. Con la aplicación de este plan se logrará tener un adecuado monitoreo y revisión de las actividades planteadas y será de gran utilidad al generar indicadores de gestión del plan, para medir igualmente la efectividad de la aplicación de este.

FORMATO DE PLAN DE ACCIÓN PARA EL TRATAMIENTO DE RIESGOS Directiva						
Entidad						
Número del Informe de control simultáneo						
Modalidad del servicio de control simultáneo						
Titular de la entidad						
RIESGOS COMUNICADOS						
Riesgo (Transcribir el riesgo expuesto en el informe)	Acciones adoptadas o por adoptar para el tratamiento del riesgo	Estado del riesgo (Mitigado / Aceptado / Sin acciones) *	Plazo para adoptar acciones cuando el estado del riesgo es "Sin acciones" (Establecer la fecha fin en día/mes/año)	Nombres y apellidos del funcionario responsable de adoptar acciones para el tratamiento del riesgo	Cargo en la entidad	Documento Nacional de Identidad (DNI)

Figura 12 Formato de Plan de acción para el tratamiento de riesgos *[6]*.

Es importante destacar que, en la prevención de lavado de activos, es necesario examinar todas aquellas transacciones o movimientos inusuales con las actividades regulares de un cliente, a través de procedimientos que permiten detectar dichas transacciones.

Primeramente, se define el área de cumplimiento de las instituciones financieras, la cual es la responsable de monitorear todos los movimientos de los clientes con el fin de identificar aquellos que revelen un posible lavado de dinero. Los procedimientos que se realicen deben reflejar los movimientos sospechosos que emitan señales de alerta temprana.

En este sentido, el proceso para detectar las operaciones sospechosas con base en el registro de clientes, requiere de un adecuado sistema de prevención de lavado de dinero, el cual indique si el cliente es una persona políticamente expuesta, si posee una cuenta en locales de frontera o si existe un cambio atípico en el nombre del titular de la cuenta bancaria.

Previamente generada la alerta, se debe proceder al análisis exhaustivo del cliente para confirmar la sospecha de blanqueo de capitales por parte del oficial de cumplimiento. Dicho análisis consiste en verificar movimientos, documentos, y datos contrastados con la información suministrada del sistema, en el cual es útil emplear los datos recolectados en el proceso de conozca a su cliente. Una vez realizado dicho análisis y confirmada la sospecha, el oficial de cumplimiento debe registrar el resultado en el histórico del usuario y enviar un reporte formal a la autoridad competente [30].

7. **Comunicar, consultar y documentar:** Finalmente, esta etapa se establece con el fin de garantizar que las áreas operativas y estratégicas necesarias para el adecuado funcionamiento del ISO 31000. Además, se busca que las partes interesadas en el desarrollo del proceso de gestión de riesgos sean analizadas en cada etapa del proceso y formen parte del proceso de planeación, diseño, implementación y ejecución del sistema, con el fin de evitar que la gestión del riesgo pueda afectar a la organización como un todo.

Por tanto, a través de este estudio, se propone aplicar los controles generales que propone el COBIT 5, partiendo de la identificación de los procesos y controles críticos, para luego ser evaluados, seguidamente se procede a auditar los recursos que componen la tecnología de la información para luego presentar a la gerencia los requerimientos de control, temas técnicos y riesgos de negocio y finalmente comunicar ese nivel de control a los partícipes.

Cabe destacar que, con la aplicación de esta metodología se logra visualizar de forma ejecutiva, cada uno de los aspectos más relevantes del Gobierno de TI y su estado de riesgo, desde el punto de vista del logro de los objetivos, con el fin de orientar los esfuerzos hacia una mejora continua, basándose en las mejores prácticas sugeridas por el marco de trabajo de COBIT 5, de TI.

Se sugiere utilizar en esta fase la matriz RACI, representada por los cuatro tipos de responsabilidades que podemos asignar a cada persona:

- R (responsable): es la persona que ejecuta la tarea.
- A (aprobador): es la persona que debe aprobar el trabajo realizado y dar por concluida la tarea.
- C (consultor): es la persona que presta ayuda al responsable.
- I (informado): es la persona que debe estar informada de la ejecución de la tarea, pero sin participar de ella.

De esta manera, la matriz de responsabilidad detalla no solo quien participa en cada tarea, sino también de qué forma participa.

Actividad / Recurso	Julio	Javier	Félix	Daniel
Elaborar el plan de gestión	C,I	A	C,I	I
Realizar el estudio de uso de las TIC	A	I	C,I	I
Planificación	C	A	R	I
Capacitar a los usuarios	A	C	R	I
Desarrollo del proyecto			A	R
Verificación de errores	I	R		A
Cerrar el proyecto	A	I	I	I

Figura 13 Matriz RACI *[6]*.

VI. DISCUSIÓN

La guía obtenida puede ser una herramienta práctica, útil y de fácil comprensión para cualquier organización que adopte medidas de control, orientadas a prevenir y mitigar los riesgos que, en la realización de sus transacciones, puedan ser utilizadas como instrumento para lavar activos, de esta manera la empresa puede incluir la Gestión del Riesgo como parte de su estrategia.

Esta guía permite desarrollar pautas básicas, basada en el análisis de los procedimientos utilizados por la auditoría forense, aplicada a la prevención de lavado de activos, así como el estudio de una metodología de seguridad de la información para la gestión del riesgo informático, aplicable al entorno empresarial y organizacional en el sector de la banca privada en la ciudad de Cuenca.

La adopción de las Normas ISO 31000 en este trabajo permitió presentar un esquema que nos ayuda a conocer los riesgos de manera eficiente para un buen análisis y gestión.

De esta manera, al implementarlos en las instituciones bancarias, la gestión de riesgos permitirá alcanzar los objetivos creando así conciencia de las amenazas causadas por dichos riesgos, además de manejar adecuadamente los riesgos dentro de la institución, así como obtener la capacidad de asignar y hacer uso efectivo de los recursos para tratar el riesgo. De la misma manera, se logrará tener una mejor gestión de incidentes y prevención, mejorando la eficacia y eficacia operativas y finalmente reducir las pérdidas.

Considerar la aplicación de la norma ISO 9001 en esta investigación contribuyó de manera práctica, ya que, al implementar un sistema de gestión basado en calidad dentro de las instituciones financieras, se garantiza la satisfacción de sus clientes facilitando la comprensión del funcionamiento del sistema no solamente por parte de todos los miembros de la institución, sino de los clientes, garantizándoles el resguardo de su información y la prevención del lavado de activos y financiamiento de delitos,

De igual manera, considerar el riesgo de las tecnologías de la información mediante las recomendaciones de la ISO 27005 fue relevante, puesto que enmarca aspectos requeridos por la ISO 27001 en la seguridad informática, pero con un mayor enfoque en la gestión de riesgos, al igual que los procedimientos sugeridos por la guía metodológica para la gestión de riesgos de información ECU@Risk; además de que proporciona diversas ventajas a cualquier tipo de organización, permitiendo el aumento de la seguridad efectiva de los sistemas de información, basada en una correcta planificación y gestión de la seguridad en las alianzas comerciales, logrando un comercio electrónico más seguro así como la mejora de la imagen de la organización y auditorías de seguridad más precisas y confiables.

Por otra parte, aplicación de la norma ISO 37001 permitió establecer que, como sistema basado en la lucha contra la corrupción, promueve en las instituciones financieras una cultura empresarial ética y con la implementación de esta norma integrado con un sistema de gestión antisoborno, no pueden ser corrompidas, ya que existe un cuidado en sus procesos, generando de esta manera que no sean vulnerables y corruptibles. A sí mismo, la falta de implementación de la norma ISO 37001 impacta de manera negativa en el logro de los objetivos estratégicos trazados en la empresa, ya que, la organización posee un plan estratégico que pretende llevar a cabo en un determinado tiempo y que dará como resultado la mejora en diferentes aspectos, sin embargo, si existe algún evento fortuito que no se presentara dentro del plan estratégico, se generaría el cumplimiento de los objetivos y también cambiaría el resultado esperado.

La metodología obtenida permitirá hacer frente de los escenarios de fraude especificados en este trabajo, de esta manera se facilita a las empresas a evaluar y mejorar sus sistemas de control interno, esta metodología se incorporó en las políticas, reglas y regulaciones y ha sido utilizada por muchas compañías para mejorar sus actividades de control hacia el logro de sus objetivos. Este nuevo enfoque no reemplaza el marco de control interno, sino que lo incorpora, permitiendo a las empresas mejorar sus prácticas de control interno o al decidir hacia un proceso más completo de gestión de riesgo.

El desarrollo de la metodología para mejorar la gestión se centra en subsanar las debilidades, vulnerabilidades y necesidades por medio de una gestión eficiente de las actividades y procesos basada en las directrices de la metodología COBIT 5, soportada por estándares, normas y metodologías de calidad para los servicios de gestión TI en las instituciones financieras.

Basado en la metodología ECU@Risk, el aporte de este trabajo consistió en proponer amenazas que son consideradas como lavado de activos, y que se incorporaron a las actuales identificadas en el dominio de riesgos provocados o riesgos deliberados. Con este aporte se espera que la metodología ECU@Risk pueda fortalecerse en cuanto al ámbito de instituciones bancarias y financieras.

En la actualidad, el uso de la inteligencia artificial y las técnicas de minería de datos, representan elementos importantes dentro del proceso de identificación de transacciones inusuales en las instituciones financieras, ya que, a través del análisis y conocimiento, se busca prevenir y detectar muchas de las actividades ilícitas además permite contener sus impactos en detección temprana de incidentes relacionados con el lavado de activos.

En este sentido, existen herramientas como la minería de datos, la cual presenta el proceso de Knowledge Discovery in Data Bases (KDD), que consiste en el análisis de grandes volúmenes de datos para generar conocimiento útil a favor de la toma de decisiones, además, facilitan la identificación de patrones y tendencias, así como transacciones atípicas, probablemente relacionadas con los delitos mencionados.

Es importante mencionar que, la aplicación de estas técnicas permite optimizar tiempo y recursos en el desarrollo de la inteligencia financiera, para así robustecer la información y análisis.

VII. CONCLUSIONES

Con el desarrollo del presente estudio se hace evidente la importancia de la auditoría forense, no sólo en la detección de los fraudes sino en la prevención de estos. El fraude en instituciones financieras es cometido, en la mayoría de los casos, por los funcionarios de altos cargos en el que están involucrados personal del área técnica, así como contadores.

Así mismo, en los resultados obtenidos a través de las medidas de mitigación, se observó que las sanciones impuestas al personal involucrado en los casos de fraudes no guardan proporcionalidad con los ilícitos cometidos, además de acuerdo con lo revisado no se evidencia sanciones ejemplarizantes a estos profesionales.

Con relación con lo antes expuesto, se evidencia que, al aplicar el procedimiento de auditoría forense en un caso de delito financiero, se facilita el detectar y divulgar este tipo de fraude, motivado a que este proceso implica cumplir con el valor de integridad para recoger evidencia y así mismo generar los informes correspondientes respecto al delito.

De igual manera, se expone que la ejecución de delitos de lavado de dinero genera un impacto financiero, económico y social lo cual perjudica la imagen de la institución financiera, su prestigio, la inversión, el financiamiento y las nuevas oportunidades en futuros negocios y proyectos.

Así mismo, se evidencia que a través de la implementación de diferentes técnicas de aprendizaje automático aplicadas para la detección de fraude y de lavado de activos, se obtiene datos relevantes por medio del uso de la inteligencia artificial y las técnicas de minería de datos, como elementos fundamentales dentro del proceso de

identificación de transacciones inusuales en las instituciones financieras

A través de este estudio se ha logrado presentar las señales de alerta y la forma de abordar estos riesgos en integración con los procedimientos de auditoría. Además, se destacó la importancia del uso de diversas normativas basadas en ISO 31000, ISO 9001:2015, ISO 27005, ISO 37001, enmarcados en el gobierno de COBIT 5, las cuales permitirán identificar los controles aplicables a los esquemas de fraude, controlar la ocurrencia del delito, y la importancia del compromiso por parte del personal en el cumplimiento de las políticas y normativas internas en integración con la implementación de sistemas dentro de las instituciones.

Con respecto a la discusión sobre el tema de lavado de activos, se destaca la importancia de la aplicación de herramientas computacionales robustas, a través del uso de la inteligencia artificial y las técnicas de minería de datos, que permiten facilitar la identificación de señales de alerta y construcción y seguimiento de perfiles por sector, respecto a casos atípicos, así mismo, contribuyen al proceso de toma de decisiones en entidades especializadas en prevención, detección y/o administración del riesgo.

El aporte de este trabajo fue el de identificar técnicas de lavado de activos en 12 casos identificados en instituciones financieras nacionales para proponer nuevas amenazas a las que mantiene la metodología ECU@Risk y personalizar la misma para su uso en el análisis de este tipo de técnicas.

VIII. Trabajos futuros

Una consecuencia de este trabajo resulta la investigación de la incidencia del lavado de activos que se han presentado en las instituciones bancarias antes y luego de la aplicación de esta metodología en las operaciones, contrastándola con el fraude electrónico y así determinar el porcentaje de mitigación de riesgo obtenido.

IX. Referencias

[1] FMI, «Fondo Monetario Internacional,» 10 Septiembre 2019. [En línea]. Available: https://www.imf.org/external/spanish/index.htm.

[2] G. Estupiñan, Control interno y fraudes, lima: Ecoe ediciones, 2015.

[3] E. A. Saritama Torres, C. Jaramillo Pedrera y M. J. Cuenca Jiménez, «La Auditoría Forense, una herramienta de control en el sector plúblico y privado del Ecuador,» 2017.

[4] Superintendencia de bancos, NORMAS PARA LAS ENTIDADES DE LOS SECTORES publicos y privados sobre prevencion de lavado de activos, quito: superintendencia de bancos ecuador, 2018.

[5] UAFE, manual de prevencion de lavado der activos, quito: UAFE, 2018.

[6] M. Azanza y I. Bermeo, «Manual de procedimientos para la gestión del proceso de Sevucción dentro de la industria ecuatoriana de restauración,» Cuenca, Ecuador, 2016.

[7] A. Ansaldi, «Análisis de la Auditoría Forense en la investigación de delitos económicos y financieros,» Argentina, 2016.

[8] J. Ferreyros, «La Auditoría Forense como Herramienta Preventiva y de Investigación para combatir el Fraude y la Corrupción Financiera Pública en el Perú,» Lima, 2019.

[9] Asamblea Nacional, «LEY PREVENCION DE LAVADO DE ACTIVOS Y DEL FINACIAMIENTO DE DELITOS,» Quito, 2017.

[10] A. Torres y E. Crespo, «Propuesta de modelo de gestión de calidad de servicio de Tecnologías de Información en el sector PYME basado en COBIT, COSO, ITIL y las prácticas de la industria,» 2018. [En línea]. Available: http://dspace.uazuay.edu.ec/handle/datos/8590.

[11] R. H. Marquez, Auditoría Forense, Ciudad de México , 2018.

[12] E. Lizarzaburu, G. Barriga, L. Noriega y L. Lopez, «Gestión de Riesgos Empresariales ISO 31000,» *Espacios*, p. 8, 2017.

[13] H. Mejia, Gestión Integral de Riesgos y Seguros, ECOE, 2014.

[14] E. Kowask y F. Alcantara, Gestión del Riesgo de las TI NTC 27005, REDCEDIA, 2016.

[15] E. Martinez y J. Garcia, «Sistemas Informáticos de Innovación Empresarial,» *ECORFAN*, 2011.

[16] Y. Zambrano, «La Auditoría Forense: Un mecanismo para detectar el fraude de estados financieros en Colombia,» *Inquietud Empesarial*, p. 36, 2015.

[17] R. Rojas, «Propuesta Metodológica para la Detección y Prevención de Fraudes de Lavado de Activos en Empresas del Sector Inmobiliario,» 2018.

[18] FGE, «Fiscalía General del Estado,» 2019. [En línea]. Available: https://www.fiscalia.gob.ec/. [Último acceso: 10 Septiembre 2020].

[19] M. Quevedo, G. Ramón, P. Barahona, G. Cabrera y J. Quevedo, «Estrategia de auditoría forense para la prevención de fraudes empresariales,» *Revista Científica Dominio de las Ciencias*, p. 415, 2019.

[20] S. Camposano y J. Moyano, «Auditoría Forense aplicada al Sistema de Créditos de la cooperativa de ahorro y crédito Jardín Azuayo, Oficina Cuenca,» Cuenca, 2014.

[21] J. Carvallo, F. Carvajal, R. Vintimilla y E. Crespo, «Success, Failure, Risks, Benefits and Barriers Factors in the Adoption of Open Source Software,» 2018.

[22] E. Crespo, «Metodología de Seguridad de la Información para la gestión del Riesgo Informático aplicable a MPYMES,» Cuenca, 2017.

[23] E. Crespo, «Ecu@ Risk, Una metodología para la gestión de Riesgos aplicada a las MPYMEs,» *Enfoque UTE*, p. 121, 2017.

[24] LOTAIP, «Ley Orgánica de Transparencia y Acceso a La Información,» *Registro Oficial Suplemento 337*, nº 24, 18 Mayo 2004.

[25] LGISF, «Ley General de Instituciones del Sistema Financiero,» *Registro Oficial 250*, 2012.

[26] A. Ponce y R. Villagómez, «Revisión de las herramientas estadísticas empleadas en la detección del lavado de activos,» *Publicando*, vol. 3, nº 8, pp. 420-431, 2016.

[27] F. Pérez, «Valoración del Delito Previo como Prueba Determinante en el Delito de Lavado de Activos,» *Revista Jurídica Científica SSIAS*, vol. 10, nº 2, pp. 25-40, 2017.

[28] ISACA, «ISACA,» 2012. [En línea]. Available: http://cotana.informatica.edu.bo/downloads/COBIT5-Framework-Spanish.pdf.

[29] UAFE, «Unidad de Análisis Financiero y Económico,» 10 Septiembre 2018. [En línea]. Available: https://www.uafe.gob.ec/#.

[30] Á. Toso, «La regulación de prevención del lavado de activos relativa al momento en que se debe conocer a los clientes. Reflexiones derivadas de su aplicación por el banco emisor de un crédito documentario*,» *Lus et Praxis*, vol. 22, nº 2, pp. 19-52, 2016.

[31] V. Pons, «Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad,» *Revista Latinoamericana de Estudios de Seguridad*, nº 20, pp. 80-93, 2017.

[32] A. Ponce, P. Piedrahita y R. Villagómez, «Toma de decisiones y responsabilidad penal frente al lavado de activos en Ecuador,» *Política Criminalística*, vol. 14, nº 28, pp. 365-384, 2019.

[33] J. Giboney, J. Gainer, S. Goel y J. Valacich, «The Security Expertise Assessment Measure (SEAM): Developing a scale for hacker expertise[La medida de evaluación de la experiencia en seguridad (SEAM): desarrollo de una escala para la experiencia de los piratas informáticos],» *Computers & Security*, vol. 60, nº 2, pp. 37-51, 2016.

[34] D. Bradbury, «A hole in the security wall: ATM hacking,» *Network Security*, vol. 2010, nº 6, pp. 12-15, 2010.

[35] F. Königstorfer y S. Thalmann, «Applications of Artificial Intelligence in commercial banks – A research agenda for behavioral finance[Aplicaciones de la inteligencia artificial en los bancos

comerciales: una agenda de investigación para las finanzas conductuales],» *Journal of Behavioral and Experimental Finance*, vol. 27, nº N/A, pp. 205-220, 2020.

[36] N. Kupka, R. Tolosana, E. Schach, K. Bachmann, T. Heining y M. Rudolph, «an environment for data mining of process mineralogy data: A case study of an industrial rougher flotation bank[un entorno para la minería de datos de datos de mineralogía de procesos: un estudio de caso de un banco de flotación industrial],» *Minerals Engineering*, vol. 14, nº 6, pp. 106-111, 2020.