

Universidad Andina Simón Bolívar

Sede Ecuador

Área de Gestión

Maestría en Gestión Financiera y Administración de Riesgos Financieros

**Administración del Riesgo de Lavado de Activos y Financiamiento del
Terrorismo en la Banca Electrónica de una Institución Financiera
Ecuatoriana: apertura de cuentas online y uso de ATM's**

Verónica Alexandra Pineda Ribera

Tutora: Silvana Raquel Salazar Torres

Quito, 2019



Cláusula de cesión de derechos de publicación de tesis

Yo, Verónica Alexandra Pineda Ribera, autor de la tesis intitulada *Administración del Riesgo de Lavado de Activos y Financiamiento del Terrorismo en la Banca Electrónica de una Institución Financiera ecuatoriana: apertura de cuentas online y uso de ATM's* mediante el presente documento dejo constancia de que la obra es de mi exclusiva autoría y producción, que la he elaborado para cumplir con uno de los requisitos previos para la obtención del título de Máster en Gestión Financiera y Administración de Riesgos en la Universidad Andina Simón Bolívar, Sede Ecuador.

1. Cedo a la Universidad Andina Simón Bolívar, Sede Ecuador, los derechos exclusivos de reproducción, comunicación pública, distribución y divulgación, durante 36 meses a partir de mi graduación, pudiendo por lo tanto la Universidad, utilizar y usar esta obra por cualquier medio conocido o por conocer, siempre y cuando no se lo haga para obtener beneficio económico. Esta autorización incluye la reproducción total o parcial en los formatos virtual, electrónico, digital, óptico, como usos en red local y en internet.
2. Declaro que en caso de presentarse cualquier reclamo de parte de terceros respecto de los derechos de autor/a de la obra antes referida, yo asumiré toda responsabilidad frente a terceros y a la Universidad.
3. En esta fecha entrego a la Secretaria General, el ejemplar respectivo y sus anexos en formato impreso y digital o electrónico.

.....

Firma:.....

Resumen

Este trabajo fue elaborado para identificar y analizar los riesgos de lavado de activos y financiamiento del terrorismo a los que se encuentra expuesta una institución financiera ecuatoriana en la apertura de cuentas online y uso de cajeros automáticos (por sus siglas en inglés, ATM), con la finalidad de proponer acciones de gestión que permitan mitigar estos riesgos. Para ello, partimos por entender conceptualmente qué es el lavado de activos y el financiamiento del terrorismo, así como, el proceso de administración de riesgos, la banca electrónica y las tipologías de lavado de activos y financiamiento del terrorismo asociadas a la banca electrónica. También analizamos las mejores prácticas internacionales y la normativa nacional, pues este conocimiento previo permite formar un criterio para poder analizar y evaluar los procesos existentes.

El proceso continúa con entrevistas a los responsables de los procesos para conocer como es el desarrollo de cada uno de estos, una vez que se diagraman los procesos se procede a levantar los eventos de riesgo. Mediante la elaboración de una matriz de riesgos, se establecen los criterios para la medición de dichos riesgos, se identifican los controles para mitigar cada uno de ellos, posteriormente se analizan y califican los controles existentes. Así, se determina el riesgo residual de la entidad financiera y se plantea las posibles recomendaciones para mitigar los riesgos.

Finalmente este trabajo concluye con la presentación de las propuestas de mejora en los procesos de la institución y ajustes en los controles establecidos, de tal manera que, los riesgos residuales altos sean mitigados para evitar que la institución financiera sea vulnerable al lavado de activos y financiamiento del terrorismo, mediante la apertura de cuentas online y transacciones efectuadas por los clientes a través de los ATM.

Tabla de Contenidos

Abreviaturas.....	11
Glosario	13
Introducción.....	19
Capítulo primero Planteamiento del problema.....	21
1. Descripción.....	21
2. Objetivo general y específico	23
3. Justificación.....	24
4. Delimitación del problema	25
5. Características de la institución financiera	26
Capítulo segundo Aspectos generales de la administración del riesgo de LA/FT	27
1. Lavado de activos y financiamiento del terrorismo	27
1.1. Definiciones	27
1.2. Etapas del LA/FT	28
2. Administración del riesgo de LA/FT.....	30
2.1. Definiciones	30
2.2. Proceso de administración del riesgo de LA/FT	31
3. Banca Electrónica.....	40
3.1. Definiciones	40
3.2. Principales productos de la banca electrónica.....	42
3.3. Tipologías de LA/FT asociados a la banca electrónica.....	43
Capítulo tercero Mejores prácticas internacionales y normativa nacional	47
1. Mejores prácticas internacionales	47
1.1. Los orígenes	47
1.2. Instrumentos internacionales.....	48
1.3. Opinión de los organismos internacionales respecto a los canales electrónicos... 54	54
2. Normativa nacional	57
3. Análisis comparativo ventajas y limitaciones de la normativa nacional.....	62

Capítulo cuarto Estructura del sistema de administración del riesgo de lavado de activos y financiamiento del terrorismo para la banca electrónica de una institución financiera ecuatoriana.....	69
1. El sistema financiero privado ecuatoriano y la banca electrónica.....	69
2. Identificación de eventos de riesgo de LA/FT	73
2.1. Apertura cuenta online	73
2.2. Uso de ATM.....	78
3. Medición del riesgo de LA/FT	82
3.1. Apertura de cuentas online.....	87
3.2. Uso de ATM.....	90
4. Evaluación de controles.....	92
4.1. Apertura de cuentas online.....	92
4.2. Uso de ATM.....	97
5. Tratamiento del riesgo	100
5.1. Apertura de cuentas online.....	100
5.2. Uso de ATM.....	104
Capítulo quinto Conclusiones y recomendaciones.....	107
1. Conclusiones	107
2. Recomendaciones	109
Lista de referencias	113
Anexos.....	117
Anexo 1: Identificación de eventos de riesgo apertura de cuenta online	117
Anexo 2: Identificación de eventos de riesgo transacciones a través de ATM.....	124
Anexo 3: Cálculo de probabilidades apertura cuenta online.....	133
Anexo 4: Cálculo de probabilidades transacciones a través de ATM.....	134
Anexo 5: Cálculo del impacto del evento de riesgo de LA/FT apertura cuentas online.....	135
Anexo 6: Cálculo del impacto del evento de riesgo de LA/FT uso de ATM.....	136
Anexo 7: Cálculo de la efectividad de los controles apertura cuenta online.....	137
Anexo 8: Cálculo de la efectividad de los controles en el uso de ATM	139

Tabla de Ilustraciones

Ilustración 1	Proceso administración de riesgos	30
Ilustración 2	Cálculo de probabilidad, impacto y riesgo inherente	33
Ilustración 3	Mapa de calor	36
Ilustración 4	Ejemplo ubicación de evento de riesgo LA/FT en mapa de calor.....	39
Ilustración 5	Estructura Institucional.....	59
Ilustración 6	Flujograma apertura cuenta online	76
Ilustración 7	Flujograma transacciones a través de ATM	80
Ilustración 8	Ejemplo de cálculo de probabilidad	84
Ilustración 9	Ejemplo de cálculo del impacto	86
Ilustración 10	Ejemplo ubicación de evento de riesgo LA/FT en mapa de calor.....	87
Ilustración 11	Flujograma del proceso propuesto para apertura de cuenta online	103
Ilustración 12	Flujograma del proceso propuesto para uso de ATM	106
Gráfico 1	Riesgo Inherente en la apertura de cuentas online	89
Gráfico 2	Riesgo Inherente uso de ATM	92
Gráfico 3	Riesgo residual en la apertura de cuentas online.....	96
Gráfico 4	Comparativo riesgo inherente y residual apertura de cuentas online.....	96
Gráfico 5	Riesgo residual en el uso de ATM	99
Gráfico 6	Comparativo riesgo inherente y residual uso de ATM	100
Tabla 1	Naturaleza del control.....	37
Tabla 2	Frecuencia de aplicación de los controles	37
Tabla 3	Nivel de automatización del control.....	37
Tabla 4	Modelo de valoración de efectividad del control	38
Tabla 5	Comparación de los estándares internacionales con la norma ecuatoriana.....	65
Tabla 6	Principales productos y servicios que instituciones financieras ecuatorianas ofrecen a través de internet.....	71
Tabla 7	Escala para probabilidades apertura cuentas online	83
Tabla 8	Escala para probabilidades transacciones a través de ATM.....	83
Tabla 9	Escala de medición de impacto por riesgos asociados	85
Tabla 10	Escala de riesgo de LA/FT	86
Tabla 11	Cálculo del riesgo inherente apertura de cuentas online	88
Tabla 12	Cálculo del riesgo inherente uso de ATM.....	90

Tabla 13 Detalle de controles para la apertura de cuentas online	93
Tabla 14 Cálculo del riesgo residual	94
Tabla 15 Detalle de controles para uso de ATM	97
Tabla 16 Cálculo del riesgo residual	98

Abreviaturas

AML: Anti Laundering Money

ASC: Asesor al cliente

ASOBANCA: Asociación de Bancos Privados

ATM: Automated Teller Machine o cajero automático

CNT: Corporación Nacional de Telecomunicaciones

COSO: Committee of Sponsoring Organizations of the Treadway

COBIT: Objetivos de Control para Tecnología de Información y Tecnologías relacionadas

CPS: Coordinador de Punto de Servicio

EBT: Especialista de Banca Telefónica

E-business: Electronic business

FINTECH: Finance Technology

GAFI: Grupo de Acción Financiera Internacional

GG: Gerente General

JPC: Jefe de Procesos Centralizados

KYC: Know your customer - Conozca su cliente

LA/FT: Lavado de Activos y Financiamiento del Terrorismo

OFAC: Office of Foreign Assets Control

PEP: Personas Expuestas Políticamente

PLA/FT: Prevención de Lavado de Activos y Financiamiento del Terrorismo

SARLAFT: Sistema de Administración de Riesgos de Lavado de Activos y Financiamiento del Terrorismo.

SB: Superintendencia de Bancos

SRI: Servicio de Rentas Internas

TI: Tecnologías de la información

UAFE: Unidad de Análisis Financiero y Económico

Glosario

Para una mejor comprensión del lector los términos utilizados en el presente trabajo, deben ser interpretados de acuerdo con las siguientes definiciones:

- **Actividades de alto riesgo.-** Son todas las actividades que por sus características son vulnerables a ser usadas en actividades ilícitas como es el lavado de activos y financiamiento del terrorismo.
- **Asesor al cliente.-** Empleado de la institución financiera que asesora al cliente en el uso adecuado de los diferentes productos y servicios que ofrece la institución financiera y que mejor se acoplan a las necesidades financieras del cliente.
- **Asociación de Bancos.-** Entidad gremial sin fines de lucro, constituida para representar los intereses legítimos de los Bancos Privados del Ecuador y promover un ambiente idóneo para su desarrollo.
- **ATM.-** Es un equipo automatizado enlazado a una entidad bancaria el cual permite la realización de distintas actividades como entrega y admisión de dinero mediante una clave de usuario y una tarjeta que comúnmente cuenta con un chip o una banda magnética.
- **ATM full.-** Cajero automático que permite al cliente depositar y retirar efectivo. Dispensa el efectivo que le ha sido asignado.
- **ATM reciclador.-** Cajero automático que permite al cliente depositar y retirar efectivo, a diferencia del ATM full el dinero depositado por los clientes es dispensado en el caso de retiros, por ende es más eficiente.
- **Beneficiario final.-** Es toda persona natural propietaria o destinataria que se encuentra autorizada o facultada para disponer de recursos o bienes; así como también hace referencia a toda persona que influye sobre personas jurídicas o entidades.
- **COBIT:** Marco internacionalmente aceptado, para auditar la gestión y control de los sistemas de información y tecnología en todos los sectores de una organización, se utiliza para implementar el gobierno de IT y mejorar los controles de IT. Contiene objetivos de control, directivas de aseguramiento, medidas de desempeño y resultados, factores críticos de éxito y modelos de madurez.

- **Código de depósito.**- Número que permite efectuar depósitos en ATM a clientes y no clientes sin la necesidad de contar con la tarjeta de débito. No tiene plazo máximo de vigencia.
- **Código de retiro.**- Número que permite efectuar retiros en ATM solo a clientes y por un monto específico sin la necesidad de contar con la tarjeta de débito y tiene un plazo máximo de vigencia de 24 horas.
- **Cajero multifuncional.**- Permite el depósito de efectivo y cheques.
- **COSO.**- Estándar de referencia que contiene directrices para la implementación, gestión y control de un sistema de administración de riesgos, involucra a toda la entidad, proporciona seguridad razonable a la junta directiva de la organización y está orientada al logro de objetivos del negocio.
- **Debida diligencia mejorada, reforzada o ampliada.**- Grupo de políticas, procesos y procedimientos exhaustivos, diseñados en función del nivel de riesgo de la institución para prevenir el LA/FT en la entidad.
- **Debida diligencia.**- Es el conjunto de procesos, políticas y procedimientos que una entidad emplea como medida de prevención para evitar que la misma sea usada para el lavado de activos y financiamiento de delitos por parte de sus accionistas, clientes, empleados, corresponsales y mercado.
- **Delitos precedentes de LA/FT.**- Son todos aquellos delitos previos al lavado de activos o financiamiento del terrorismo, como por ejemplo: corrupción; peculado; secuestro; narcotráfico de personas, animales, armas, sustancias sicotrópicas, etc.
- **E-business.**- Surgió en 1990. Es el empleo de recursos tecnológicos de comunicación especialmente de internet en un negocio o empresa para desarrollarse y facilitar así las tareas de los mismos, permite la integración de la información y está orientado a distintas actividades. Al permitir la interacción vendedor-cliente virtualmente, en ciertas ocasiones se admite el anonimato de cualquiera de los actores abriendo así la puerta a distintas actividades ilícitas como estafas, lavado de activos entre otras.
- **Empresa de papel.**- También denominadas empresas fantasmas son aquellas que carecen de activos propios u operacionales, las mismas no son ilegales y son creadas con la finalidad de permitir realizar distintas actividades a nivel

empresarial; sin embargo, pueden ser usadas para encubrir beneficios en paraísos fiscales.

- **Empresa pantalla.**- Son empresas que en ningún país ni en el país en el cual fueron legalmente constituidas y autorizadas poseen presencia física.
- **Ficha de depósito.**- Formulario con el cual el cliente firma y detalla su nombre, número de documento de identidad, número de cuenta en la cual se depositará y el detalle del monto a depositar en efectivo y cheque.
- **FINTECH.**- Son empresas intermediarias las cuales permiten realizar distintas operaciones financieras mediante dispositivos móviles. Este tipo de empresas presentan vulnerabilidades ante el LA/FT debido a que, en ciertos casos facilitan el anonimato de sus usuarios lo que impide un correcto seguimiento de las transacciones; poseen alcance transnacional para efectuar operaciones en distintas jurisdicciones y admiten el uso de monedas electrónicas.
- **Firma electrónica.**- Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.
- **Formularios de licitud de fondos.**- Documento en el cual el depositante declara el origen y destino de los fondos a depositar, su nombre, actividad económica, número de documento de identidad, número de cuenta en la cual se depositará, datos del beneficiario del depósito y monto depositado. Se llena y firma por el depositante para depósitos en efectivo iguales o superiores a los 5,000.00USD.
- **Funda de seguridad.**- Instrumento en el cual el cliente usuario del ATM para depósitos iguales o mayores a 5,000.00USD usa para guardar el formulario de licitud de fondos, la ficha de depósito y las monedas, billetes y cheques a depositar.
- **GAFI.**- Tiene como principal objetivo erradicar el lavado de activos y financiamiento del terrorismo. En sus inicios, fue creado por el G7 en 1989 como una entidad que permita combatir los ingresos del narcotráfico, pero luego de los acontecimientos terroristas del 11 de septiembre se incluyó

también como uno de sus objetivos controlar y eliminar el financiamiento de esta actividad ilícita.

- **Grupo Egmont.**- Organismo Internacional que agrupa a las Unidades de Inteligencia Financiera del mundo, para facilitar el intercambio de información en la lucha contra el lavado de activos y financiamiento del terrorismo.
- **Intervalos de clase.**- Rango utilizado para dividir un conjunto de valores numéricos entre un valor mínimo y un valor máximo que delimitan el intervalo para facilitar la interpretación de grandes cantidades de datos mediante tablas o gráficos.
- **ISO 31000.**- Norma para la gestión del riesgo, que proporciona principios y directrices genéricas sobre la gestión de riesgos, busca armonizar la gran cantidad de estándares, metodologías y paradigmas existentes que difieren entre industrias, temas y regiones.
- **Listas de restricción.**- Listado de personas que han sido sentenciadas por lavado de activos, delitos precedentes de lavado de activos y financiamiento del terrorismo. Es elaborado por distintos organismos internacionales como: OFAC, ONU, etc; así como, entidades nacionales como la UAFE en Ecuador.
- **Mensaje de datos.**- Es toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio como: documentos electrónicos, registros electrónicos, correo electrónico, servicios web, telegrama, télex, fax e intercambio electrónico de datos.
- **OFAC.**- Administra y aplica sanciones económicas y comerciales contra países y regímenes extranjeros, terroristas, narcotraficantes internacionales y quienes participan en actividades relacionadas a la proliferación de armas de destrucción masiva y otras amenazas a la seguridad nacional, la política exterior o la economía de los Estados Unidos.
- **País de alto riesgo de lavado de activos.**- Son países con bajos o nulos controles de prevención de LA/FT que los vuelve vulnerables tanto del delito de lavado de activos como de sus delitos precedentes.
- **Paraíso Fiscal.**- Son estados que tienen laxas legislaciones tributarias y de control; siendo vulnerables a la evasión fiscal y a distintas actividades ilícitas.

- **Perfil del riesgo de comportamiento del cliente.**- Permite determinar y asignar el nivel de tolerancia transaccional del cliente en base a característica inherentes del mismo con relación a la modalidad de uso de servicios y productos ofertados por la institución.
- **Perfil transaccional del cliente.**- Es un parámetro máximo contra el cual se compara las transacciones del cliente. Se calcula con base en los productos, la situación y actividad económica del cliente y de acuerdo con la metodología planteada por la institución financiera.
- **Persona Expuesta Políticamente.**- Son todas las personas naturales que desempeñan o han desempeñado un cargo público destacado a nivel nacional o internacional.
- **Procesos Centralizados.**- Grupo de colaboradores de la institución financiera (back office) que efectúan los procesos de apertura de cuentas, asignación de servicios financieros, proceso de transacciones como: depósitos en efectivo, cheques, transferencias, etc.
- **Riesgo de Contagio.**- Es la probabilidad de pérdida directa o indirecta que puede presentar una entidad como consecuencia del accionar de un vinculado.
- **Riesgo inherente.**- Es el riesgo correspondiente a una determinada actividad sin considerar el efecto de los controles.
- **Riesgo legal.**- Probabilidad de que la entidad sufra pérdidas o sea objeto de multas y sanciones causadas por una mala interpretación u omisión legal.
- **Riesgo operativo.**- Es la probabilidad de pérdida generada por errores o fallos en procedimientos, sistemas, fallas humanas y acontecimientos externos que perjudican la operatividad de dicha entidad.
- **Riesgo Reputacional.**- Probabilidad de pérdidas a casusa del desprestigio de una entidad ya sea por un accionar indebido o una mala imagen infundada.
- **Riesgo residual.**- Es el riesgo remanente que está presente luego de ejercer todo tipo de controles.
- **Riesgos asociados al LA/FT.**- Son aquellos a través de los cuales se materializa el riesgo de Lavado de activos y del financiamiento de delitos.
- **Sujeto obligado.**- Son todos los sectores económicos que están obligados por ley a informar a la UAFE sobre movimientos de dinero superiores o iguales a diez mil dólares americanos mismos que sean injustificados o inusuales; las

personas naturales o jurídicas que pertenezcan a estos sectores también se encuentran obligadas a informar y generar reportes que tengan como principal objetivo evitar el lavado de activos y la financiación del terrorismo.

- **Tarjeta de débito.**- Es una tarjeta física plástica la cual contiene información del usuario y generalmente incorpora un chip o una banda magnética, la cual permite realizar ciertas operaciones bancarias ya sean estas activas, pasivas o neutrales.
- **Tarjeta de seguridad.**- Es una tarjeta física plástica la cual contiene información del usuario e incorpora una banda magnética, la cual permite abrir la caja del ATM que la institución financiera posee para depósitos superiores a los 5,000.00USD en efectivo o cheque.
- **Telemática.**- Usan tanto los sistemas informáticos como los de telecomunicación para implementar servicios y aplicaciones.
- **UAFE.**- Es la institución encargada de recopilar información, realizar reportes, ejecutar políticas y estrategias nacionales de PLA/FT.

Introducción

Los avances tecnológicos y el internet han significado el progreso y desarrollo de una parte de la humanidad. En la actualidad, es una constante que los sectores económicos para ser competitivos y no quedar relegados del mercado, buscan estar al alcance de sus clientes a través de un clic. Esto implica, una fuerte inversión no solo desde el punto de vista de desarrollo tecnológico, si no, desde la perspectiva de administración de riesgos, pues son herramientas que están al alcance de todo el mundo incluyendo grupos delictivos.

La intermediación financiera, actividad realizada por las instituciones financieras autorizadas para captar recursos de quienes tienen excedentes y destinarlos a quienes tienen necesidades de liquidez obteniendo por ello una comisión, también ha visto en los dispositivos móviles e internet una forma de seguir haciendo negocio. Sin embargo, la poca regulación sobre estas herramientas tecnológicas ha sido la razón principal para que se conviertan en el medio preferido por los delincuentes para lavar dinero y financiar al terrorismo.

El presente trabajo centra su atención en la banca y su incursión en la implementación de canales electrónicos para efectuar transacciones e incluso vincular a nuevos clientes. El objetivo, identificar los principales riesgos de lavado de activos y financiamiento del terrorismo que presenta la banca electrónica en una institución financiera ecuatoriana, tanto en la apertura de cuentas online como en el uso de los ATM, con la finalidad de proponer medidas a tomar para mitigar estos riesgos.

En el capítulo primero, denominado Planteamiento del problema, se describe brevemente el reto que implica la migración de la banca tradicional hacia la banca electrónica, no solo para las instituciones financieras si no para los gobiernos, organizaciones internacionales y sujetos obligados desde el punto de vista de evitar que la evolución tecnológica permita que el sistema financiero sea vulnerable para el lavado de activos y financiamiento del terrorismo; delitos que traen grandes afectaciones a la economía en general.

En el capítulo segundo, denominado Aspectos generales de la administración del riesgo de lavado de activos y financiamiento del terrorismo, se definen y ejemplifican los principales términos que están relacionados con la administración del riesgo de lavado de activos y financiamiento del terrorismo. También, se define la banca electrónica, se

detallan los productos/ servicios que en ella se brindan y las principales tipologías de lavado de activos y financiamiento del terrorismo que se podrían presentar en esta nueva forma de hacer banca.

El capítulo tercero, denominado Mejores prácticas internacionales y normativa nacional empieza con una síntesis de los pasos que algunos países y organismos internacionales emprendieron para frenar los continuos intentos de los delincuentes por ocultar el dinero mal habido en los diferentes sectores económicos, el fortalecimiento de las regulaciones para evitar atraer operaciones financieras ilegales y la cooperación internacional como medio para eliminar las brechas regulatorias entre países con el objetivo de prevenir eficientemente el lavado de activos y financiamiento del terrorismo. Se detallada cada uno de los instrumentos internacionales que han ido surgiendo con el paso del tiempo a nivel internacional y que se han implementado en Ecuador. Se describe brevemente el marco regulatorio ecuatoriano y se realiza un análisis comparativo de las ventajas y limitaciones de la normativa nacional. También, se expone la opinión de los organismos internacionales respecto a las nuevas tecnologías y se analiza la normativa ecuatoriana con referencia a esta nueva tendencia.

En el cuarto capítulo, titulado Estructura del sistema de administración del riesgo de lavado de activos y financiamiento del terrorismo para la banca electrónica de una institución financiera ecuatoriana, presenta una breve perspectiva del sistema financiero privado ecuatoriano y su incursión en la banca electrónica, tendencia mundial para responder a las necesidades de los clientes, conquistar a nuevos clientes especialmente a los más jóvenes y competir con las tecnologías financieras (en adelante, Fintech). Así también, muestra la aplicación del Sistema de Administración de Riesgo de Lavado de Activos y Financiamiento del Terrorismo en la apertura de cuentas online y uso de los ATM en una institución del sistema financiero ecuatoriano.

Finalmente, en el capítulo quinto se presentan las conclusiones y recomendaciones de cada capítulo y las relacionadas con los resultados obtenidos luego de la evaluación de los procesos de apertura de cuentas online y uso de los ATM en la institución financiera bajo análisis, cuyo nombre se mantiene en reserva por razones de confidencialidad de la información.

Capítulo primero

Planteamiento del problema

1. Descripción

El sistema financiero es un conjunto de instituciones, que canalizan los recursos monetarios de quienes tienen excedentes hacia quienes lo necesitan, permitiendo dinamizar la economía de un país. Este sistema, en Ecuador está regulado y conformado de la siguiente manera: la Junta de Política y Regulación Monetaria y Financiera que es la responsable de la regulación, de la supervisión monetaria y de la elaboración de políticas públicas; los organismos de supervisión y control como la Superintendencia de Bancos, la Superintendencia de Economía Popular y Solidaria y la Superintendencia de Compañías, Valores y Seguros; finalmente las instituciones reguladas como bancos, mutualistas, sociedades financieras, cooperativas de ahorro y crédito y las compañías de seguros y valores. El sistema de Bancos Privados representa el 80% del total del sistema financiero ecuatoriano y está compuesto por 24 instituciones, que de acuerdo al monto de sus activos está dividido en: bancos grandes (más de 1,000 millones USD), bancos medianos (entre 200 y 1,000 millones USD) y bancos pequeños (menos de 200 millones USD). Además se encuentra dominado por ocho organizaciones líderes en servicios financieros y a la vanguardia de la tecnología, experiencia y servicio al cliente que en conjunto al 2018 representan el 88% del total de activos, el 89% de los depósitos y 91% de las utilidades de los bancos. Su cartera de crédito de 24,077 millones USD y depósitos por 27,686 millones USD les permite reportar una utilidad conjunta de 503 millones USD (Zabala, Chávez y Calvopiña 2019, 62-70).

Las tecnologías exponenciales como la telefonía móvil, están cambiando la forma en la que funcionan muchos sectores de la economía, estas han permitido un crecimiento muy rápido de los negocios. El descontento de los usuarios con el funcionamiento de la banca tradicional a partir de la crisis financiera, ha permitido el nacimiento de un nuevo sector denominado Fintech, que apoyado en las plataformas digitales se ha enfocado en ofrecer y potencializar el financiamiento, los sistemas de pago, remesas, asesoría financiera, etc. Para poder competir con las Fintech las instituciones financieras se han visto en la obligación de buscar la manera de automatizar muchos de sus productos y

servicios sin dejar de lado los controles que les evite ser sujeto de fraude o incluso ser un medio para el lavado de dinero y financiamiento del terrorismo.

Las instituciones financieras ecuatorianas en los últimos años se han enfocado en conseguir que sus clientes puedan acceder a sus productos financieros y realizar transacciones desde cualquier parte a través de sus dispositivos móviles, servicios como: la apertura de cuentas, pagos de servicios, la obtención de certificados y referencias bancarias, revisión de estados de cuenta, transferencias de fondos, registro de solicitud de crédito, depósitos y retiros de dinero a través de ATM con o sin tarjeta de débito, entre otras operaciones financieras ya se pueden realizar en línea, solo se requiere conexión a internet y un dispositivo móvil. En promedio los canales digitales, según la Asociación de Bancos Privados del Ecuador (en adelante Asobanca) a noviembre de 2016 representaron el 60% del total de las transacciones (González 2017, 4). Según la Superintendencia de Bancos, el 73% de las transacciones en el 2017 se efectuaron a través de canales electrónicos. Mientras que el Banco Central señala que la tasa de crecimiento del uso de medios de pago digitales va en aumento pues ha pasado de 16% en el 2016 a 30% en el 2017 (Tapia 2018, 5).

Los bancos constituyen la puerta más accesible para introducir el dinero de origen delictivo en la economía legítima, ya que son rápidas y seguras para efectuar transacciones financieras y ofrecen: estructura, organización y acceso a los sistemas de pagos nacionales, internacionales y los mercados de capitales. Si no se evita que el dinero ilícito ingrese al sistema financiero las posibilidades de rastrear con éxito su procedencia ilícita es nula, por ello es importante localizar e intervenir el dinero ilícito al momento de la colocación en las agencias bancarias. Por lo que, la identificación de clientes, mantenimiento de registros, disponibilidad de registros y comunicación de transacciones sospechosas es vital (Comisión Andina de Juristas 2000, 95-6).

El lavado de dinero es un delito que está en constante evolución, busca nuevas formas de operar con sofisticadas innovaciones que aparte de dificultar su control y prevención, incrementa su impacto en la sociedad.

Tanto las instituciones financieras públicas como privadas están obligadas a adoptar medidas de control, dispuestas por la Junta de Política y Regulación Monetaria y Financiera, la Unidad de Análisis Financiero y Económico y la Superintendencia de Bancos, dirigidas a prevenir y mitigar los riesgos que por el giro de su negocio pueden implicar lavado activos o financiamiento del terrorismo. Para salvaguardar el bienestar de los depositantes y de la propia institución, las instituciones financieras están en la

obligación de analizar el nivel de riesgo que las nuevas aplicaciones, procesos, productos o modelos de negocio implican, con la finalidad de proponer acciones concretas que permitan disminuirlos.

El lavado de activos tiene efectos perjudiciales en el sistema económico, para prevenir y evitar que la entidad sea usada para legitimar fondos de proveniencia ilícita a través de sus productos debe establecer políticas, procesos y procedimientos que permitan conocer al cliente, al empleado, el mercado y al corresponsal o contraparte, para ello, una adecuada administración de riesgos le permitirá conocer los riesgos a los que está expuesta, tomar decisiones respecto a sus controles y mejorar su desarrollo. El omitir la gestión del riesgo de lavado de activos y financiamiento del terrorismo expone a la entidad al riesgo reputacional y riesgo legal que recae en una afectación del prestigio de la institución financiera por estar relacionada con negocios ilícitos, pérdidas económicas y sanciones severas impuestas por los organismos de control, como por ejemplo el cierre definitivo de la institución financiera y la revocatoria de su licencia.

2. Objetivo general y específico

Objetivo general:

Identificar los principales riesgos de lavado de activos y financiamiento del terrorismo que presenta la banca electrónica en una institución financiera ecuatoriana, tanto en la apertura de cuentas online como en el uso de ATM, a través de una matriz de riesgo, con la finalidad de proponer acciones de gestión para estos riesgos.

Objetivos específicos:

- Identificar las características de la banca electrónica y los métodos utilizados para legitimar fondos de origen ilícito a través de ella.
- Analizar lo planteado por las mejores prácticas internacionales y la normativa nacional para la administración del riesgo de LA/FT, con la finalidad de comparar y determinar ventajas y limitaciones de la normativa nacional.
- Identificar, medir, controlar y monitorear los riesgos de LA/FT de la banca electrónica de una institución financiera ecuatoriana, tanto en la apertura de cuentas online como en el uso de ATM, a través de una matriz de riesgo, para determinar las principales medidas que se deberían tomar para mitigar estos riesgos.

3. Justificación

Hoy en día vivimos en una economía globalizada que se fundamenta en la innovación, la tecnología y la expansión de los mercados. Los sistemas de pagos a través de internet permiten que las transacciones se realicen con mayor velocidad, lo que dificulta el control, la aplicación de leyes y la identificación o rastreo de transferencias de fondos. Debilidades que son aprovechadas por los lavadores de dinero porque permite su anonimato y por ende el ocultamiento del origen ilegal de sus fondos.

El enfoque basado en riesgos que recomiendan los estándares internacionales, busca que los sujetos obligados vayan más allá del simple hecho de cumplir con la normativa nacional y los estándares internacionales, a que el sujeto obligado conozca sus riesgos y establezca controles adecuados, para evitar que sea susceptible de lavado de dinero y financiamiento del terrorismo. Por esta razón, es importante que previo el lanzamiento de un nuevo producto o servicio a través de los canales tecnológicos la institución financiera conozca los riesgos de LA/FT a los que se exponen con estos y no adopte los controles que otras instituciones hayan implementado o que implemente sistemas de administración de riesgos que empresas externas hayan estandarizado, pues el resultado no será el mismo que los obtenidos al tener un propio sistema de administración de riesgos el cual se acople a la realidad de la institución.

Evidentemente este es un trabajo en conjunto entre gobiernos, organizaciones internacionales y sujetos obligados. Pues los gobiernos a través de sus unidades de inteligencia financiera, fiscalías y superintendencias deben contar con las normas adecuadas para guiar a los sujetos obligados, entender la realidad del país en cuanto a la exposición del mismo al riesgo de LA/FT y tener criterios amplios para supervisar y auditar a sus controlados. Las organizaciones internacionales de igual manera deberán identificar nuevas tipologías de LA/FT a través de las nuevas tecnologías, asesorar y orientar a sus miembros en las nuevas modalidades de prevención de LA/FT. Los sujetos obligados entre ellos las entidades financieras está en la primera línea de batalla, por ende tienen que conocer a sus clientes, aprender de las personas que llegan a abrir una cuenta y monitorear las transacciones de sus clientes de tal manera que puedan establecer parámetros de comportamiento de sus clientes que les permita establecer cuáles son las actividades económicas que representan un mayor riesgo de LA/FT para la institución, cuales son los sectores o tipos de clientes a quienes previo a su vinculación deben realizar una debida diligencia ampliada, clientes a quienes por el bajo nivel de riesgo de LA/FT

que representan se podrían exonerar de presentar el documento que certifique su nivel de ingresos y cuya vinculación no amerite una visita in situ, etc. Todo esto se puede lograr solo si el sujeto obligado pasa de cumplir con la normativa a conocer sus riesgos lo que le permitirá mitigar los mismos y mejorar su gestión porque podrá realizar un uso eficiente de sus recursos.

Una administración adecuada del riesgo de lavado de activos y financiamiento del terrorismo trae múltiples beneficios para toda una sociedad, ya que, se evita la competencia desleal, contribuyendo de esta manera a la permanencia y sostenibilidad de los negocios, se fortalece la gestión empresarial lo que facilita la toma de decisiones estratégicas que promueven prácticas de Responsabilidad Social Empresarial, así también, se previene la complicidad, la corrupción y se mejora la reputación de los negocios.

Para las instituciones financieras el identificar, evaluar y administrar el riesgo de lavado de activos y financiamiento del terrorismo en los nuevos productos y servicios que ofrecen, permite a los directivos conocer los riesgos a los cuales se encuentran expuestos como consecuencia del giro normal del negocio y tomar de esta manera acciones preventivas que minimicen las posibilidades de pérdidas para la institución a la vez que protegen a sus usuarios.

4. Delimitación del problema

Varios son los productos y servicios financieros, cuyo acceso hoy en día se puede realizar a través de los dispositivos tecnológicos. La inteligencia artificial, la minería de datos, la ciberseguridad y una buena base de datos han contribuido en gran medida a que una página web y una app permitan el primer contacto con el cliente, así como, ofrecer productos personalizados, efectuar un análisis y otorgamiento de crédito acorde a las necesidades del cliente más rápido, menos complicado y a través de internet.

La digitalización de la economía apunta hacia la desintermediación lo que complica la regulación, el control y la prevención del LA/FT. Sin embargo, las regulaciones actuales sobre intermediación financiera en Ecuador aún no lo permiten por el mismo hecho de que es en este punto donde muchos de los riesgos se pueden identificar, medir, controlar y monitorear. Tanto los organismos de control como las instituciones financieras deben realizar un trabajo conjunto porque aunque los requerimientos tecnológicos y operativos estén prácticamente listos para trabajar completamente a través

de internet, hace falta la emisión de la normativa necesaria para la operación en la que se estipulen aspectos como: la firma electrónica, el reconocimiento biométrico, entre otros que permitan por ejemplo abrir una cuenta bajo la modalidad 100% electrónica.

En ese sentido, debido a que en la actualidad la apertura de cuentas a través de dispositivos móviles y el uso de ATM para efectuar depósitos y retiros de efectivo son los productos/servicios más impulsados por el sistema financiero ecuatoriano y sobre los cuales la identificación del solicitante o depositante es complejo, el presente trabajo centra su análisis en la gestión del riesgo de lavado de activos y financiamiento del terrorismo inherente en la apertura de cuentas online y uso de ATM.

5. Características de la institución financiera

La institución financiera bajo análisis, obtuvo en el 2005 su licencia para funcionar como banco, es una entidad ecuatoriana del sector privado y por el nivel de sus activos que al cierre del 2018 fueron de 318,530,842 USD está catalogado como un banco mediano.

Es un banco comercial, pues entre los productos que ofrece están: cuenta de ahorro, cuenta corriente, garantías bancarias, depósito a plazo fijo y créditos. Su enfoque son las pequeñas y medianas empresas así como clientes privados interesados en ahorrar. Considerada en el medio como una institución fuerte con sobresaliente trayectoria de rentabilidad y claras perspectivas de estabilidad que se refleja en su calificación AAA-.

Es la primera institución en el Ecuador en ofrecer créditos eco para el desarrollo de energías renovables, eficiencia energética y medidas ambientales. Desde el 2016 se ha enfocado no sólo en proporcionar acceso directo a sus clientes a todos sus servicios bancarios para gestionar sus fondos las 24 horas, sino en ser un medio que facilite el control total de sus finanzas a través de los diferentes dispositivos electrónicos.

Capítulo segundo

Aspectos generales de la administración del riesgo de LA/FT

1. Lavado de activos y financiamiento del terrorismo

1.1. Definiciones

El lavado de activos conocido también como lavado de capitales, blanqueo de capitales o legitimación de capitales, ha sido contextualizado por varios autores a lo largo de los tiempos, pero todos concluyen que es el proceso para dar apariencia de legalidad a fondos provenientes de actividades ilegales. El financiamiento del terrorismo, a diferencia del lavado de activos sus recursos pueden provenir de actividades lícitas e ilícitas, para financiar el cometimiento de actos violentos, degradantes e intimidantes que presionen a gobiernos y sociedades a tomar decisiones a favor de los grupos terroristas. Ambos delitos nacen con el único objetivo de continuar con la cadena de operaciones delictivas.

Victor Nando (2014, 16) señala que:

El lavado de dinero es el fenómeno que representa un delito característico de la época moderna. La especialización en los sistemas financieros, la integración en grandes empresas y las operaciones realizadas en diversos continentes son notas concomitantes del lavado de dinero. La idea que se ha dado aparece relacionada con el ocultamiento del dinero a las autoridades fiscales, con el fin de evitar el seguimiento de los responsables de evasión de pagos de impuestos. Posteriormente, la idea de lavado de dinero se ha relacionado con toda clase de delitos que generan grandes cantidades de dinero.

Ulises Torres Soto (2010, 10), manifiesta que: “se deberá entender como lavado de activos a aquella actividad por la cual se procure dar la apariencia de legalidad a recursos económicos provenientes de actividades ilícitas, con el objeto de que se confundan con los recursos lícitos de una persona, sociedad o Estado”.

La Unidad de Análisis Financiero de República Dominicana (2018, párr.3) define el financiamiento del terrorismo como:

Cualquier forma de acción económica, ayuda o mediación que proporcione apoyo financiero a las actividades de elementos o grupos terroristas. Aunque el objetivo principal de los grupos terroristas no es financiero, requieren de fondos para llevar a cabo sus actividades, cuyo origen puede provenir de fuentes legítimas, actividades delictivas o ambas.

José María Peláez (2014, 301) en su libro cita la ley 10/2010 de España donde se define al financiamiento del terrorismo como: “el suministro, el depósito, la distribución

o la recogida de fondos o bienes, por cualquier medio, de forma directa o indirecta, con la intención de utilizarlos o con el conocimiento de que serán utilizados, íntegramente o en parte, para la comisión de cualquiera de los delitos de terrorismo tipificados en el Código Penal”.

1.2. Etapas del LA/FT

Todo proceso implica un conjunto de fases sucesivas que permiten lograr un fin, es así que, para poder lavar dinero se necesita llevar a cabo las siguientes etapas:

1. **Colocación:** Es introducir el dinero, bienes o ganancias procedentes de actividades ilícitas dentro del sistema financiero o económico.

Para entender mejor este concepto, tomamos como ejemplo el caso de un secuestrador, que una vez realizado su trabajo recibe una cuantiosa cantidad de dinero. Dinero que si es llevado directamente a una institución financiera levantará sospechas de su origen ilegal y por ende el secuestrador será detenido por las autoridades con facilidad. Para ocultar su procedencia ilegal sin levantar sospechas, el secuestrador optará por comprar bienes muebles e inmuebles, negocios en quiebra y solicitará a personas con necesidades económicas abrir cuentas para depositar su dinero a cambio de una comisión, de esta manera ha ingresado su dinero ilegal sin ser identificado por las autoridades al sistema financiero y económico.

2. **Estratificación:** Son las transacciones, negociaciones que buscan alejar de su origen ilegal al dinero, bienes o ganancias procedentes de actividades ilícitas.

Una vez que el secuestrador ha ingresado el dinero de procedencia ilegal al sistema financiero y económico sin ser identificado, venderá los bienes muebles e inmuebles antes adquiridos y solicitará que el pago se los efectúen en una entidad financiera, fondos que ya pueden ser justificados como de origen lícito; depositará el resto del dinero ilegal señalando que provienen del giro del negocio de la empresa en quiebra que adquirió; a través de las terceras personas a quien paga comisiones por transacción abrirá pólizas, solicitará créditos que cancelará puntualmente o en su defecto los pre-cancelará con el dinero ilegal; de esta manera ha

diversificado sus fondos de tal forma que es difícil de determinar su origen ilegal.

3. **Integración:** Retorno del dinero, bienes o ganancias ya con apariencia de legalidad al lavador de dinero, quien lo inserta para el financiamiento de actividades delictivas.

Finalmente el secuestrador, desea integrar nuevamente el dinero que ahora se encuentra en la economía y lo hace transfiriendo esos fondos por concepto de ayuda familiar, compra de materia prima, compra de bienes en el exterior, etc., a una cuenta común en un paraíso fiscal, los fondos salen e ingresan a las instituciones financieras sin levantar sospechas, pues su origen y supuesto destino ahora son legales. Así, el secuestrador puede financiar sus actividades ilícitas sin ser identificado por las autoridades.

Por otro lado, el financiamiento del terrorismo implica las siguientes etapas que las ejemplificaremos en una fundación:

1. **Recaudación:** constituye el suministro de fondos que pueden ser de origen legal o ilegal.

La fundación a través de campañas, solicita a sus adeptos aportar fondos para apoyar el desarrollo de proyectos para el tratamiento de la esquizofrenia apelando a la sensibilidad de las personas. Estos adeptos, personas sin antecedentes penales y de intachable reputación deciden donar fondos de proveniencia lícita a la fundación. A esta fundación también acuden aquellos políticos que conocen de la ilegalidad de la fundación y hacen ver como donaciones al dinero proveniente de sus actos de corrupción, así como, los delincuentes e incluso miembros de grupos terroristas que hacen ver como donación el dinero proveniente de sus estafas, fraude, narcotráfico, secuestro y demás actividades ilegales.

2. **Disposición:** se refiere a la transformación, movimiento u ocultamiento de los fondos que serán destinados a actos delictivos.

La fundación posee una cuenta en una institución financiera en donde recauda las “donaciones” de sus adeptos y destina sus fondos al desarrollo de sus proyectos, para ello deberá adquirir medicamentos en el extranjero o equipos médicos para apoyar a sus beneficiarios, en ese sentido efectúa transferencias a distintas partes del mundo por estos conceptos, lo cual no levanta sospechas de la institución financiera ni las autoridades, pues las

transacciones efectuadas en su cuenta están acorde al giro de su actividad sin fines de lucro. Sin embargo, “el proveedor” de equipos médicos y medicamentos son vendedores de armas, material explosivo etc.

3. **Utilización:** es la financiación de costos logísticos y operativos de la organización terrorista.

Una vez que el dinero ha llegado a los grupos terroristas ya sea en efectivo, armamento o material explosivo pueden continuar y llevar a cabo sus atentados.

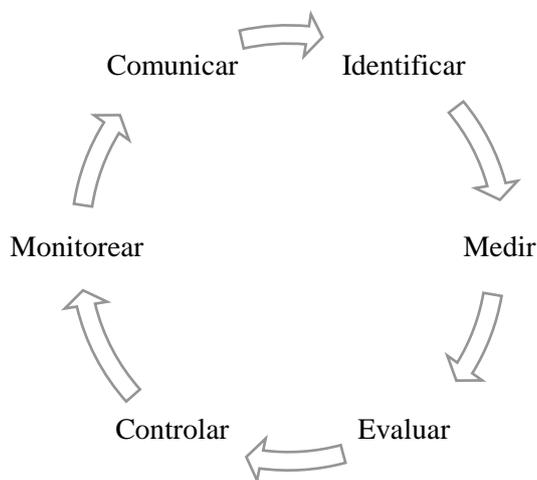
2. Administración del riesgo de lavado de activos y financiamiento del terrorismo

2.1. Definiciones

La administración del riesgo de LA/FT es el proceso de mejora continua mediante el cual la entidad identifica, mide, evalúa controles, controla, monitorea y comunica los posibles eventos de riesgo de LA/FT a los que se expone la entidad financiera en cada uno de los productos o servicios que ofrece.

Ilustración 1

Proceso administración de riesgos



Fuente y elaboración propia

Antes de revisar el proceso de administración de riesgos definiremos que es riesgo. El riesgo es una desviación de lo esperado que puede ser positivo o negativo, está expresado en términos de una combinación de las consecuencias de un evento y la probabilidad de ocurrencia asociada. Por lo tanto, los componentes para cuantificar el riesgo son: probabilidad (oportunidad de que algo suceda) e impacto (resultado de un

evento que afecta a los objetivos) y puede ser medido de manera cuantitativa (expresado en términos de números, unidades, regularmente en términos financieros) o cualitativa (expresado en una escala gradual de niveles relativos como alto, bajo y medio), no existe un método que sea puro en cuanto a los dos, porque no siempre vamos a tener toda la información para el método cuantitativo y por otro lado el método cualitativo puede ser muy subjetivo, por lo que será necesario un análisis híbrido.

2.2. Proceso de administración del riesgo de LA/FT

A continuación definiremos cada una de las etapas de la administración del riesgo de LA/FT, para una mejor comprensión y entendimiento:

Identificación de eventos de riesgo de LA/FT.- Siempre que haya una amenaza debe haber una vulnerabilidad para que el riesgo se materialice. Por lo tanto, en esta etapa se debe identificar los riesgos y un conjunto de eventos que puedan dar origen a hechos de LA/FT dentro de la institución. Es un proceso continuo que implica todos los procesos para el desarrollo del negocio y los diversos factores de riesgo como: cliente, producto/servicio, canal de distribución, jurisdicción y empleado, a los cuales puede estar expuesta la organización. Es decir, consiste en generar una lista amplia de eventos que podrían afectar a la organización, la cual debe incluir todos los riesgos ya sea que, tengan o no controles establecidos. Para poder identificar los eventos de riesgo de LA/FT se debe entender la unidad de negocio bajo análisis, en este caso el proceso de apertura de cuenta online y uso de ATM, para ello es importante diagramar cada proceso. Una vez entendido el proceso, la manera de hallar estos eventos de riesgo es con el método de solución causa - efecto que implica: identificar el problema, examinar los efectos y posibles causas del problema (Sintura, Martinez y Quintana 2011, 290).

Para una mejor comprensión de la etapa de identificación procedemos a definir cada uno de los términos citados anteriormente:

- *Amenaza.-* tiene el potencial de causar efectos adversos en las personas, los sistemas, los bienes y medio ambiente. Matemáticamente es la probabilidad de exceder un nivel de ocurrencia de un evento con una cierta intensidad en un cierto sitio y en un cierto periodo.
- *Vulnerabilidad.-* factor de riesgo interno que matemáticamente está expresado como la factibilidad de que el sujeto o sistema expuesto sea afectado por el fenómeno que caracteriza la amenaza. Grado de resistencia

ante un fenómeno amenazante o capacidad para responder después que éste ha ocurrido. Está ligada a aspectos culturales y al nivel de desarrollo de las organizaciones. Depende de diferentes factores como: tipo de banco o características de los productos que ofrece en su portafolio, solidez de los canales de distribución, solidez de los procesos de control, capacitación de los colaboradores de la entidad, enfoque efectivo sobre la prevención, idoneidad de las herramientas de tecnología de información y comunicación.

- *Factores de riesgo.*- Condicionan el origen o la existencia del riesgo. Algunos factores son de origen externo o asociados a la amenaza, mientras que otros son de origen interno o asociados con la vulnerabilidad. Así tenemos: cliente, producto/servicio, canal de distribución, jurisdicción, empleado y proveedor.
 1. Cliente: personas naturales o jurídicas que poseen un producto/servicio en la institución financiera.
 2. Producto/ servicio: Instrumentos que permiten el ahorro, crédito y efectuar transacciones a los clientes. Entre ellos tenemos: cuenta de ahorro y corriente, planes de ahorro, inversiones a plazo fijo, crédito, sobregiro, transferencias, etc.
 3. Canal de distribución: Medio a través del cual una institución financiera pone a disposición el producto o servicio que oferta. Entre ellos tenemos: ATM, app móvil, página web, tarjeta de débito y crédito, códigos de depósito y retiro.
 4. Empleado: Son las personas que laboran en la entidad financiera y dependiendo del cargo que ocupen en la misma, representan una vulnerabilidad para que la entidad sea usada para LA/FT. Por ejemplo: un especialista de cumplimiento conoce las debilidades del sistema de monitoreo y podría aprovecharlas para que un tercero realice transacciones que no detecta el sistema pero que permitan LA/FT.
 5. Jurisdicción: Territorio que dependiendo de su ubicación geográfica representa una mayor o menor vulnerabilidad para lavar activos o financiar al terrorismo. Por ejemplo ciudades fronterizas

o portuarias porque facilitan el narcotráfico de sustancias estupefacientes o psicotrópicas.

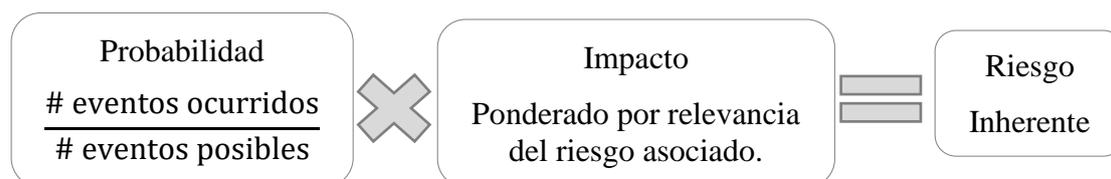
6. Proveedores: Son las personas naturales o jurídicas que prestan servicios o productos a la institución financiera y que pueden representar un riesgo reputacional para la entidad si se encuentran involucradas en actividades ilícitas.

- *Evento*.- puede ser una fuente riesgo, algo que se espera que suceda o no suceda, se percibe mediante señales de alerta observadas en los factores de riesgo que integran una unidad estratégica de negocio, responde a ciertas causas que permiten predecir la posibilidad de impactos negativos en la empresa.

Medición del riesgo.- Concluida la etapa de identificación, para medir los eventos de riesgo de LA/FT debemos medir el riesgo inherente, mediante la obtención de valores de probabilidad de ocurrencia de los eventos de riesgo de LA/FT e impacto a la institución financiera medido en términos de una pérdida de: imagen, dinero por sanciones o multas y bloqueo financiero.

Como se observa en la ilustración 2, la multiplicación de la probabilidad de ocurrencia por magnitud del impacto permite obtener el riesgo inherente para cada uno de los riesgos identificados:

Ilustración 2
Cálculo de probabilidad, impacto y riesgo inherente



Fuente: (Sintura, Martínez y Quintana 2011, 302)

Elaboración propia

En la construcción por cuadrantes, debido a que, una escala mayor permite amplitud en los cuadrantes de riesgo y clasificarlos como: aceptable, significativo, moderado, crítico y catastrófico, se utilizará una matriz de riesgo 5x5.

La probabilidad.- Es la posibilidad de que ocurra un evento, se describe matemáticamente como la frecuencia de ocurrencia de un evento en un periodo de tiempo determinado que resulta de dividir el número de eventos ocurridos para el número de eventos posibles, para ello se debe (Sintura, Martínez y Quintana 2011, 304-305):

1. Definir qué tipo de medición cuantitativa (elaborada con valores numéricos o porcentuales de datos estadísticos) y cualitativa (elaborada con escalas descriptivas) se debe utilizar.
2. Definir el tipo de fuente de información para la frecuencia
3. Definir el horizonte de tiempo para establecer la probabilidad de ocurrencia
4. Determinar la cantidad de eventos ocurridos y posibles
5. Definir frecuencia absoluta y relativa
6. Clasificar la probabilidad de ocurrencia en términos de la escala de probabilidades
7. Documentar la medición de la frecuencia

Para determinar la probabilidad de ocurrencia de un evento de riesgo de LA/FT el horizonte de tiempo puede ser de un año y la unidad de medida con base en una matriz de riesgo 5x5 podría ser:

- **Improbable:** Evento de riesgo de LA/FT cuya posibilidad de que ocurra es improbable.
- **Raro:** Evento de riesgo de LA/FT que rara vez puede ocurrir.
- **Posible:** Evento de riesgo de LA/FT que posiblemente ocurra.
- **Probable:** Evento de riesgo de LA/FT cuya ocurrencia es probable.
- **Casi seguro:** Evento de riesgo de LA/FT que casi seguro ocurre.

El Impacto.- Es el nivel de daño que un evento de riesgo de LA/FT puede causar a la entidad, se materializa en los diferentes riesgos asociados a los que se expone la entidad y que definimos a continuación:

1. Operativo: Corresponde al riesgo de que la institución financiera sea usada para LA/FT por fallas en los sistemas de monitoreo; por no contar con las políticas, procesos y procedimientos para la PLA/FT; porque los funcionarios no cuenten con la adecuada capacitación o estén vinculados con delincuentes; y porque sus clientes se asocien con delincuentes.
2. Legal: Corresponde al riesgo que por error, negligencia, impericia, imprudencia o dolo, que deriven de la inobservancia, incorrecta o inoportuna aplicación de disposiciones legales, normativas, resoluciones o instrucciones emanadas de los organismos de control referentes a PLA/FT,

pueden significar multas o sanciones administrativas y penales para la entidad.

3. **Reputacional:** Pérdida de confianza por parte del público como consecuencia de que se publiquen noticias en la que se involucre a la entidad con actividades de LA/FT y que implique la intervención de las autoridades competentes.
4. **Contagio:** Probabilidad de efectos legales y de reputación para la entidad como consecuencia de que sus proveedores, clientes, funcionarios, directivos y accionistas estén implicados en actividades de LA/FT.

Los riesgos asociados deben ser medidos en escalas diferentes de acuerdo con su relevancia. Por ejemplo, el riesgo legal que en el peor de los casos implicaría la remoción de autoridades y revocatoria de la licencia es el más relevante por lo que podría ser ponderado con un 40%, seguido por el riesgo reputacional con un 30%, riesgo operacional 20% y riesgo de contagio 10% cuya sumatoria implicaría un riesgo de LA/FT del 100%, que con base en una matriz de riesgo 5x5 estará catalogado de la siguiente manera:

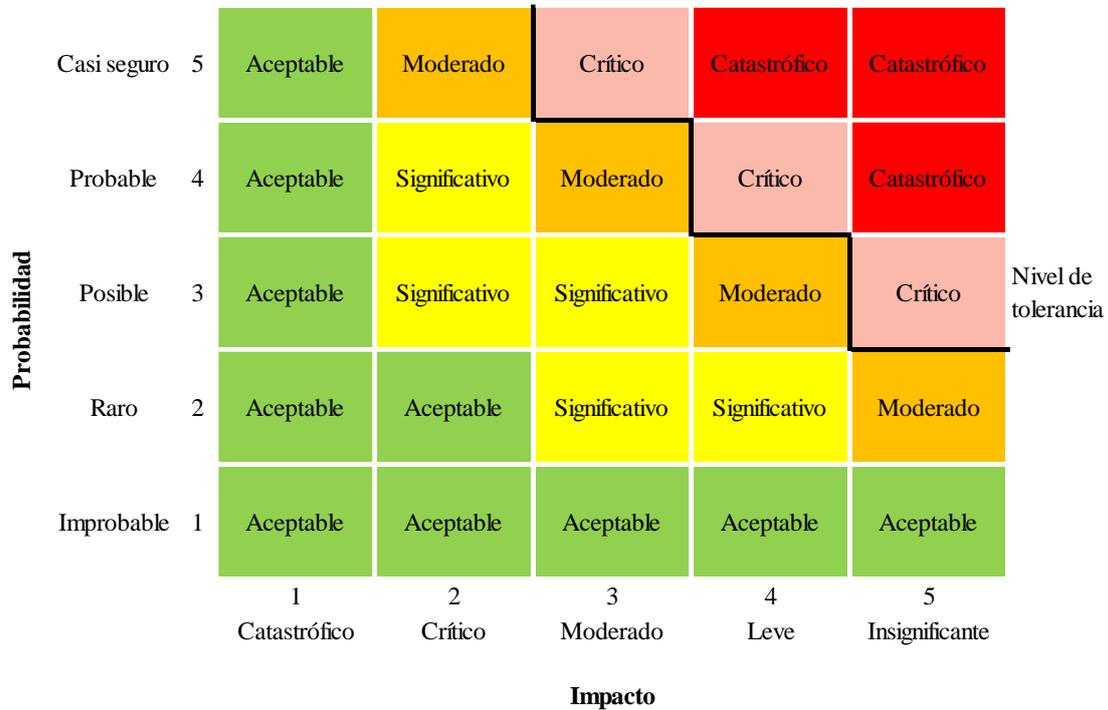
- **Insignificante:** Sin perjuicios, baja pérdida financiera o daño reputacional.
- **Leve:** Leve pérdida o daño. Puede ser susceptible de sanción moderada de índole económico. No genera pérdida de clientes, ni genera pérdida de ingresos o incremento de gastos por pérdida de reputación. Puede implicar el involucramiento de clientes en actividades de LA/FT.
- **Moderado:** Pérdida o daño moderado. Susceptible de una amonestación de índole económico. Puede haber pérdida de clientes, disminución de ingresos por desprestigio, mala imagen o publicidad negativa. El riesgo de contagio se presenta por los funcionarios.
- **Crítico:** Pérdida o daño crítico. Susceptible de una amonestación de índole económica a la mayor cuantía posible. Pérdida de clientes, disminución de los ingresos por mala imagen o publicidad. Puede implicar el involucramiento de directivos en actividades de LA/FT.
- **Catastrófico:** Pérdida o daño catastrófico, susceptible de cuantiosas amonestaciones económicas y estrictas sanciones de suspensión, inhabilitación o remoción de administradores, oficial de cumplimiento y otros funcionarios, cancelación de operaciones, suspensión de actividades,

intervención de la organización. Pérdida de clientes, disminución de ingresos por desprestigio que puede colocar en peligro la solvencia de la entidad. Puede implicar el involucramiento de accionistas en actividades de LA/FT.

En la siguiente ilustración a partir de un plano cartesiano, donde el eje horizontal (eje “X”) representa el impacto y el eje vertical (eje “Y”) la probabilidad del evento de riesgo de LA/FT, se ejemplifica el riesgo inherente o punto indicativo del cruce de los valores de probabilidad e impacto. Las cinco áreas en distintas tonalidades representan los sitios donde se puede ubicar cada evento de riesgo de LA/FT cuya tonalidad varía según el nivel de riesgo de LA/FT que en este caso va del 1 al 25, donde 1 es el más bajo nivel de riesgo inherente y 25 el más alto.

Todos los riesgos ubicados por encima del nivel de tolerancia serán considerados como riesgos críticos y catastróficos, esto significa que la entidad debe realizar seguimiento y tratamiento estricto para minimizar el impacto de los mismos en caso de su ocurrencia.

Ilustración 3
Mapa de calor



Fuente y elaboración propia

Todo lo antes detallado se plasmará en una matriz de riesgo, en la que se determina tanto de manera cuantitativa como cualitativa cuales son los niveles y valores de probabilidad y de impacto que la organización determina son aceptables para ellos.

Evaluación de controles.- Si bien en la etapa anterior llegamos a conocer nuestro nivel de riesgo, éste no ha considerado los controles que la entidad puede tener, por ello es necesario calcular la exposición real al riesgo o riesgo residual, para ello es necesario determinar la eficiencia de los controles que implica conocer su naturaleza, nivel de automatización y frecuencia, que explicamos a continuación:

Tabla 1
Naturaleza del control

Clasificación	Descripción
Preventivo	Controles aplicados durante todo el proceso, antes que se realice la operación u ocurra el evento, intentan prevenir los problemas propuestos, para evitar la ocurrencia de la causa del riesgo.
Correctivo	Controles que actúan durante el proceso y que permiten corregir los errores y las deficiencias.
Detectivo	Controles que se aplican durante todo el proceso para detectar errores o desviaciones, controles que solo actúan una vez que el proceso ha terminado.

Fuente y elaboración: (Reyes Hiedra 2012, 36)

Tabla 2
Frecuencia de aplicación de los controles

Clasificación	Descripción
Permanente	Controles aplicados durante todo el proceso, es decir en cada operación
Periódico	Controles aplicados solo cuando ha transcurrido un periodo específico de tiempo
Ocasional	Controles que se aplican solo en forma ocasional en un proceso

Fuente y elaboración: (Reyes Hiedra 2012, 36)

Tabla 3
Nivel de automatización del control

Clasificación	Descripción
Automático	Sistema de seguimiento y control informatizado y automáticamente para tomar las medidas necesarias de seguimiento
Semiautomático	Sistema de seguimiento y control informatizado y manual para tomar las medidas necesarias de seguimiento
Manual	Sistema de seguimiento y control manual para tomar las medidas necesarias de seguimiento

Fuente y elaboración: (Reyes Hiedra 2012, 36)

La efectividad de los controles se medirá bajo los siguientes criterios:

Tabla 4
Modelo de valoración de efectividad del control

Características del diseño de control			Clasificación	Valor del control
Naturaleza	Automatización	Frecuencia		
Preventivo	Automático Semiautomático	Permanente	Óptimo	5
Correctivo	Automático Semiautomático	Permanente	Muy Bueno	4
Preventivo Correctivo	Manual	Permanente Periódico Ocasional	Bueno	3
Detectivo	Automático Semiautomático Manual	Permanente Periódico	Regular	2
Detectivo	Manual	Ocasional	Deficiente	1
No determinado	No determinado	No determinado	Inexistente	0

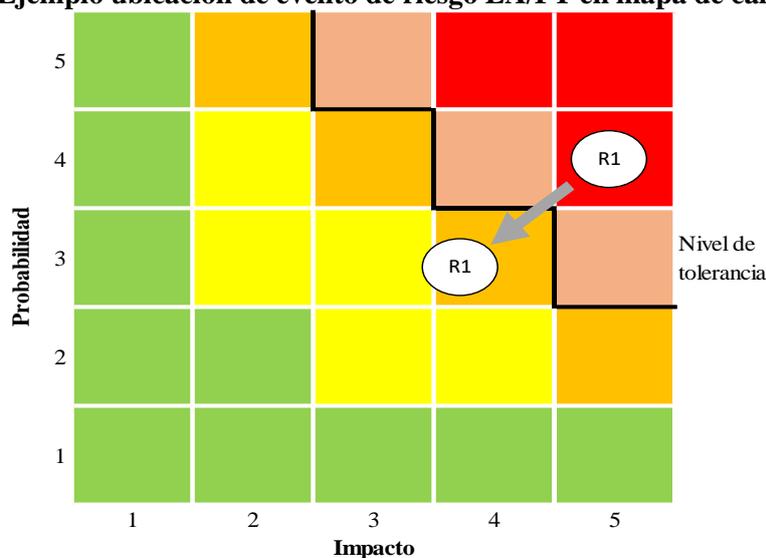
Fuente y elaboración: (Reyes Hiedra 2012, 37)

Una vez que se ha obtenido la efectividad de los controles se procede a calcular el riesgo residual, que es el nivel resultante del riesgo después de aplicar controles. La fórmula para calcular el riesgo residual la hemos obtenido del libro Administración de Riesgos Medición, Seguimiento, Análisis y Control (Reyes Hiedra 2012, 38):

$$\text{Riesgo residual} = \frac{\text{Nivel de riesgo inherente}}{\text{Efectividad del control}}$$

Dentro de un plano cartesiano, cuando un evento de riesgo de LA/FT es sometido a tratamiento mediante controles, tanto su probabilidad de ocurrencia como magnitud de impacto pueden variar, los cambios presentados en el riesgo de LA/FT implican un desplazamiento dentro del mapa, como se muestra a continuación:

Ilustración 4
Ejemplo ubicación de evento de riesgo LA/FT en mapa de calor



Fuente y Elaboración propia

En este ejemplo se puede evidenciar que el control ha permitido reducir las consecuencias de presentarse este evento de riesgo en la institución financiera.

Tratamiento del riesgo.- Para llevar los riesgos a niveles aceptables se deben tomar medidas ya sea para afrontar los riesgos que ponen en peligro la consecución de los objetivos de la entidad. Existen cuatro formas de responder al riesgo que se contextualizan a continuación:

- *Aceptación.-* Si el costo de implementar un control para tratar este riesgo es muy alto en comparación a su impacto en la organización, quizá la decisión de la alta gerencia sea aceptar dicho riesgo. O en su defecto implica no hacer nada.
- *Rechazo.-* Consiste en eliminar la actividad asociada a este riesgo.
- *Transferencia.-* Se da mediante la contratación de una póliza de seguros o a través de la tercerización porque no siempre vamos a tener una organización que asuma con las consecuencias de un incidente como una póliza de seguros pero lo podemos tercerizar.
- *Mitigación.-* Si hay una situación de peligro lo mitigamos por medio de la modificación del riesgo que implica modificar la probabilidad o el impacto.

Monitorear.- Los riesgos y la efectividad de los controles necesitan ser monitoreadas, de tal manera que, los posibles cambios en los procesos como consecuencia del progreso de los mismos no alteren las prioridades de los riesgos. Revisar los sistemas

de control interno, permite evaluar la calidad de su rendimiento y determinar el momento adecuado para actualizarlo o corregirlo pues con el paso del tiempo pueden perder su eficacia o se vuelven innecesarios (Standards Australia/Standards New Zealand Committee 1999, 19).

Comunicar.- Para que el proceso de gestión del riesgo se desarrolle en armonía es necesario que estén abiertos los canales de comunicación que permitan transmitir el conocimiento a las diferentes partes de la organización y de esta forma aprovechar la retroalimentación. Esta etapa implica el diálogo entre los responsables de su implementación y el resto de la organización para asegurar que la base sobre la cual se toman las decisiones sea comprendida, por qué se requieren ciertas acciones en particular. Abarca tanto datos internos como información de eventos, actividades y condiciones externas, información que debe comunicarse en tiempo y forma de tal manera que permita la toma de decisiones y el cumplimiento a los empleados de sus responsabilidades.

3. Banca Electrónica

3.1. Definiciones

Los avances tecnológicos han permitido u obligado al sistema financiero a evolucionar también, para retener a los clientes actuales y cautivar nuevos clientes a través de un mejor servicio y productos versátiles e innovadores o en su defecto adaptar los ya existentes a las nuevas tecnologías para cubrir las necesidades del público y ser competitivos. Es así que, a continuación presentamos algunas definiciones y puntos de vista sobre la banca electrónica:

“La banca a distancia en cuya categoría se incluyen la banca telefónica y la banca online es un servicio bancario que permite al cliente realizar sus transacciones habituales de forma más fácil y rápida, evita los desplazamientos y para ello se vale de las nuevas tecnologías” (Caldas Blanco, Murias Bermejo y Gregorio Arroyo 2015, 162).

Tom Forester (1992, 261) comenta que, la banca comercial está cambiando conforme la competencia le obliga, indica que los bancos nunca volverán a ser los mismos y hace una proyección de cómo serán los bancos del mañana:

Los bancos no tendrán barreras de ningún tipo entre su personal y los clientes, contarán con sillones cómodos y una atmósfera más tranquila y amable. Los ATM, ubicados en una sección, liberarán al personal de ventanilla de las tareas más aburridas y repetitivas, permitiendo a ese personal dar asesoría financiera y un servicio más personalizado,

adaptado a las necesidades de cada cliente. Las horas hábiles de las sucursales se ampliarán, de manera que los clientes puedan tener acceso a ellas los fines de semana y fuera de las horas normales de oficina. La sección de ATM estará abierta las 24 horas al día.

David Castillo y Patricia Gabaldón (2010, 33) entienden por banca electrónica o e-banca aquella que:

Integra a la presentación de bienes y servicios financieros cualquier tecnología disponible. Forman parte de la operativa de la banca electrónica la actividad realizada a través de los cajeros automáticos (ATM), los terminales de los puntos de venta, las líneas telefónicas digitales tanto a través de voz como a través de los denominados property PC, esto es, la conexión directa del usuario con la red interna del banco, sin empleo de internet, e incluso los recientes servicios prestados a través de la banca por ordenador o la telefonía móvil.

La normativa ecuatoriana define a la Banca Electrónica como: “los servicios suministrados por las instituciones del sistema financiero a los clientes a través de internet en el sitio que corresponda a uno o más dominios de la institución, indistintamente del dispositivo tecnológico a través del cual se acceda” (EC Junta Bancaria del Ecuador 2012, art.2).

Visto desde el lado de la inclusión financiera, la banca electrónica permite acercar el sistema financiero a los lugares donde la banca tradicional no llegaba. Implica elementos como: un entorno regulatorio propicio, adecuada protección al consumidor y transparencia de información, oferta de productos adecuados, conocimientos financieros básicos, cobertura del sector financiero a canales transaccionales tradicionales y no tradicionales para recibir servicios de calidad a precios razonables que permitan realizar transacciones de forma segura y eficiente (Banco Central del Ecuador 2012, 21-2).

Desde el lado tecnológico, el incremento del conocimiento de los usuarios en el uso de computadoras y teléfonos móviles ha permitido que hoy en día la capacidad instalada de estos equipos sea muy alta y tomando en consideración que internet es un medio libre de comunicación de dos vías la banca ha podido potencializar la competitividad, optimizar la red de sucursales para reducir costos, prestar servicios 24/7, ofrecer productos financieros en línea, acceso a mercados y clientes antes imposibles de alcanzar debido a las limitaciones geográficas (Peña Valenzuela 2007, 167-8).

La banca electrónica por lo tanto, es aquella que aprovecha y hace uso de los dispositivos tecnológicos disponibles para ofertar sus productos y servicios a los clientes, permitiendo mayor accesibilidad, reducción de costos, comodidad, seguridad y confianza en sus transacciones. Implica también una infraestructura sólida y un cambio de todos los miembros que integran el sistema financiero como: entidades financieras, reguladores,

supervisores y operadores, pues se debe simplificar procesos, contar con canales accesibles, productos adecuados al mercado objetivo, sólida información por parte de los burós para un rápido análisis y un marco normativo y operativo que permita la operación y competencia.

3.2. Principales productos de la banca electrónica

Entre las ventajas del uso de los dispositivos móviles dentro de la banca están: permite el acceso oportuno a los recursos para efectuar transferencias, pagos, retiros, etc.; fomenta el ahorro en la población; reduce los costos y riesgos asociados al manejo de efectivo; pone al alcance de la población de regiones a los que no llega la banca tradicional la apertura de una cuenta bancaria lo que reduce costos y tiempo de los usuarios; genera un historial transaccional que sirve para otros productos financieros como créditos. Entre los productos financieros que por el momento se pueden otorgar a través de la banca electrónica tenemos:

1. **Apertura de cuentas:** para acceder a este producto cada banco ha establecido sus procesos y procedimientos de tal manera que la identidad del posible cliente quede clara y comprobada. En ese sentido, en América Latina por ejemplo algunas entidades financieras permiten realizar la solicitud de crédito a través de internet, pero luego el cliente para concluir con el proceso debe acercarse ya sea a la agencia más cercana, concretar una cita para que un asesor lo visite o acercarse donde un agente bancario (tiendas, farmacias, etc., que trabajan como corresponsales de la entidad financiera en lugares donde esta no tiene sucursales) (Banco Central del Ecuador 2012, 69-99). Sin embargo, en el continente Europeo en España por ejemplo, instituciones financieras como: BBVA Online, EVO banco y Selfbank abren cuentas en cinco minutos una vez que mediante una fotografía o una selfie del cliente efectúan un reconocimiento biométrico y mediante un SMS en el móvil firman el contrato (HelpMyCash 2017, párr.10).
2. **Depósitos y retiros a través de ATM:** Ofrece alternativas para realizar transacciones que antes se debían hacer por ventanilla, están disponibles las 24 horas del día todos los días del año, permiten depósitos en efectivo y cheques; realizar transferencias nacionales, internacionales y entre

cuentas; consultar movimientos de cuenta; comprar entradas; efectuar recargas telefónicas; pagar recibos e impuestos; cambiar códigos de tarjetas e incluso contratar un préstamo personal (HelpMyCash 2017, párr.6).

3. **Otorgamiento de créditos financieros:** Las solicitudes se efectúan en línea, dependerá del monto, el destino de los fondos y el tipo de cliente el tiempo que tome la aprobación del mismo y si se requiere de visita y papeles adicionales.
4. **Obtención de estados financieros o garantías bancarias:** Es un servicio que se le puede obtener en línea, a través de los cajeros automáticos o por banca telefónica solo se necesita de usuario y clave.
5. **Transacciones como pagos y transferencias bancarias:** Para efectuar pagos el cliente necesitará de una tarjeta de débito, la cual le permitirá realizar transacciones en establecimientos autorizados y compras a través de internet, incluso hay instituciones financieras que han implementado el uso del celular como un medio de pago pasando simplemente el teléfono por encima del datafono. Para las transferencias tanto nacionales como internacionales el cliente necesitará de usuario y clave para acceder a la plataforma que su institución le ofrezca para efectuar sus transacciones.

3.3. Tipologías de LA/FT asociados a la banca electrónica

En este punto se describen las técnicas y métodos utilizados por las organizaciones criminales para dar apariencia de legalidad al dinero, bienes o ganancias de procedencia ilícita y trasladarlo de un lugar a otro a efectos de su recapitalización. La tipología es el conjunto de operaciones entrelazadas para cubrir las diferentes etapas de un delito de lavado de activos. Para que sea considerado como una tipología debe cumplir con las siguientes características: continuidad una vez que tiene éxito la primera operación; flexibilidad y adaptabilidad del esquema para evitar ser detectados; cambiabilidad para evolucionar y ser más sofisticadas; y una cuarta característica la imperceptibilidad para evitar ser identificada (Páucar Chappa 2013, 84-9).

A continuación se presenta algunas tipologías que pueden presentarse a criterio del autor a través de la banca electrónica y en especial en la apertura de cuentas online y uso de ATM:

1. Un lavador con la finalidad de trasladar dineros de un país en el que se origina los recursos ilícitos a otro, podría abrir cuentas corrientes o de ahorros en un determinado país para transferir a otros los dineros de origen ilícito realizando retiros en la moneda local a través de cajeros automáticos. El volumen de recursos a movilizar no sería de grandes sumas siempre que los cajeros restrinjan la posibilidad de retiros diarios a sumas relativamente pequeñas. Para ello tendría que recurrir a la apertura de varias cuentas y a la utilización de un gran número de tarjetas de débito (Cifuentes Muñoz, Ospina Velasco y Serna Jaramillo 2002, 83-5).
2. Cuentas bancarias de terceros es una manera de colocar, insertar, depositar o canalizar el dinero ilícito en el sistema financiero sin que sea vinculado directa o indirectamente con estas operaciones el cabecilla. Bajo esta tipología hay tres supuestos: la primera cuando el dinero depositado se hace con el permiso del titular de la cuenta bancaria ya sea voluntariamente o mediante engaños. La segunda cuando no existe permiso ni conocimiento del titular de la cuenta bancaria porque se ha suplantado su identidad. Y la tercera se origina con la complicidad de un empleado de la entidad financiera quien informa al lavador de aquellas cuentas que por diversas razones pueden ser utilizadas para lavar dinero (Páucar Chappa 2013, 96-7).
3. Utilización de testaferros que no son simples prestanombres, son personas de confianza de los lavadores de activos, personas de su entorno amigos de infancia, excompañeros de colegio, universidad, familiares directos o profesionales cercanos que les prestan servicios como abogados o contadores, etc. Esta tipología comprende dos funciones: la de administrador y custodia que no son nada más que la persona que administra bienes, negocios, cuentas bancarias y demás propiedades del criminal o en el caso de custodia que son las personas que aparecen como propietarios para escudar el verdadero nombre del dueño (Páucar Chappa 2013, 97-8).
4. Uso de créditos fingidos: solicita un crédito y ofrece una garantía aparentando dar buen uso del dinero y pagando puntualmente sus cuotas. Sin embargo, adrede deja de cumplir con los pagos, incurre en mora y obliga a la entidad financiera a ejecutar la garantía, de esta manera se justifica la procedencia ilegal del dinero inicialmente ilícito (Páucar Chappa 2013, 95).

5. Transferencias electrónicas: las organizaciones criminales usan una red de comunicaciones electrónicas, bancos o compañías que se dedican a transferencias de fondos comerciales para mover el dinero ilícito desde un país hacia cualquier parte del mundo, a través de manera estratificada y sucesiva, por montos pequeños de varias cuentas a una sola cuenta en común desde varios puntos de un país o región con la finalidad de esconder la fuente criminal, la propiedad de los fondos y oscurecer rastros en el caso de alguna auditoría. Tipología que se presta para estructuras más complejas y dinámicas, ya que, permite la transferencia de fondos a países que permiten ocultar la identidad del depositante y luego los fondos se transfieren a bancos internacionales que tienen acceso a mercados de todo el mundo (Páucar Chappa 2013, 100-1).
6. Estratificación mediante pitufo: las organizaciones criminales utilizan una o varias personas para colocar pequeñas sumas de dinero en el sistema financiero a través de depósitos que serán destinados a una sola cuenta matriz o depósitos desde varias entidades bancarias para una persona en común (Páucar Chappa 2013, 99).
7. Disfrazar dinero ilegal como fondos provenientes de empresas legalmente constituidas. Para ello los criminales compran empresas en quiebra, crean empresas fantasmas o utilizan empresas existentes para engañar y colocar los fondos de origen ilícito en el sistema financiero.

Las tipologías permiten a los responsables, en el caso de tener transacciones que cumplan con estas características sospechar que están frente a un incidente de lavado de activos y financiamiento del terrorismo. Son guías, puntos de referencia para los sujetos obligados al momento de decidir si reportar o no el caso a las Unidades de Inteligencia Financiera correspondientes y una evidencia importante en las investigaciones posteriores.

En este capítulo hemos visto que, la banca electrónica es otra forma de hacer banca, porque trae consigo las mismas amenazas de lavado de activos y financiamiento del terrorismo, solo que en un escenario diferente. Esto no significa que no se deban identificar, analizar, evaluar y tratar los riesgos, por el contrario hay que determinar que los controles son acordes al nuevo escenario y objetivos de la organización sin exponer la reputación y viabilidad del negocio. Debido a que, el giro del negocio se está trasladando a un campo de acción diferente al usual, el cual implica el rediseño de

procesos y el desarrollo o adquisición de nuevas competencias, es claro que el impacto y probabilidad del riesgo también varían de manera sustancial, por lo que se requiere analizar los procesos que involucra el nuevo campo de negocio, identificar las amenazas a las que está expuesta y los riesgos originados producto de estas amenazas con la finalidad de definir el perfil de riesgo de la entidad ante el nuevo escenario de operación e incorporar políticas y procedimientos de operación y control para el negocio, que incluye la tecnología necesaria para habilitar esta operación y componentes de seguridad.

Capítulo tercero

Mejores prácticas internacionales y normativa nacional

1. Mejores prácticas internacionales

1.1. Los orígenes

El lavado de activos es una acción que permite ocultar el dinero proveniente de repudiables actividades como: el narcotráfico, trata de personas, tráfico de órganos, tráfico de especies protegidas, terrorismo, secuestro, fraude, corrupción, testaferrismo, entre otras actividades ilícitas, para que la delincuencia organizada pueda financiar nuevas acciones delictivas con esas ganancias mal habidas. Acto que daña a la sociedad tanto al inicio como al final de su proceso, porque para lograr este objetivo los lavadores corrompen a funcionarios públicos, compiten deslealmente con los negocios legítimos, atacan la moral de los pueblos y debilitan la estabilidad de las estructuras políticas y económicas.

Ante esta problemática, varios países entre ellos Estados Unidos adoptaron medidas represivas y preventivas ante el lavado de dinero con la finalidad de proteger sus economías. En 1970 Estados Unidos por ejemplo, aprueba la Ley del Secreto Bancario con la finalidad de identificar la fuente, el volumen y el movimiento de la moneda y otros instrumentos monetarios trasladados o transferidos a los Estados Unidos o fuera de los Estados Unidos. Desde inicios de los años 80, los Estados Unidos y el Consejo de Europa impulsaron la prevención de operaciones de lavado de dinero en el sistema financiero, para ello dictaron disposiciones legales y recomendaciones dirigidas a estimular en el sector bancario una actitud anti lavado. Medidas que se refieren al registro y comunicación de determinadas operaciones con dinero en efectivo con el fin de controlar los flujos de dinero de origen ilícito.

Sin embargo, ante las medidas tomadas por estos países hay una contra respuesta por parte de los delincuentes, quienes se adaptaron a las medidas, pero al enterarse que había un límite de 10 mil empezaron a depositar en menores cantidades. Ante esto, se desarrollaron reportes de actividades sospechosas, pero los criminales se movieron de las entidades financieras estrictamente reguladas y eficientes, al sector no financiero que por no estar regulado ofrecía brechas y facilidades (Comisión Andina de Juristas 2000, 154).

Por otra parte, la seguridad al secreto bancario, leyes frágiles, el anonimato, instituciones financieras poco reglamentadas, el uso de corporaciones en el extranjero en donde no se sabe quién es el dueño de la corporación y no hay restricciones en las transferencias de acciones ni de registros y la baja o nula tributación que ciertos países ofrecían, permitieron que con el paso del tiempo se dieran cuenta que cualquier esfuerzo era inútil si no existía una colaboración internacional efectiva, pues no es posible frenar el movimiento de divisas si no hay controles conjuntos entre países que actúan como plaza de depósitos o transferencias de dinero. Los delincuentes se mueven de un país a otro conforme los controles que cada uno imponga incluso dentro del mismo país buscan que tipo de sector les da mayores facilidades para legitimar capitales, existen mecanismos informales para lavar dinero como: el mercado de moneda extranjera, casinos, juegos de azar, entre otros que pueden dejar de lado los esfuerzos realizados. Medidas como: el decomiso de la droga tiene efectos muy limitados, pues la oferta es lo bastante elástica para adaptarse a grandes disminuciones de mercancía, incluso los precios han demostrado ser inmunes. En cambio, el bloqueo en el sistema financiero puede perturbar las operaciones del tráfico. El dinero es el alma y el único fin del tráfico ilícito y aquel país que no se protege contra el lavado de activos atrae operaciones financieras ilegales (Comisión Andina de Juristas 2000, 33-48).

Es así que, organismos internacionales como la Organización de Naciones Unidas (ONU), la Unión Europea (UE) y algunos países del mundo, se reúnen con el objetivo de establecer estándares internacionales a seguir en conjunto que permitan frenar los efectos negativos del lavado de activos y financiamiento del terrorismo, pues contar con normas lo suficientemente similares evita que los delincuentes encuentren brechas que puedan aprovechar para la delincuencia organizada.

1.2. Instrumentos internacionales

La Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Psicotrópicos celebrado en Viena en 1988, es el primer instrumento internacional en el que se abordó el lavado de dinero como delito, pues contempla la opción de penalizar el lavado de dinero, enfatiza en la importancia de la cooperación internacional para facilitar las investigaciones y establece que el secreto bancario no debe servir de obtáculo en las investigaciones penales dentro de la cooperación internacional. Es el instrumento de

carácter obligatorio más ratificado y difundido, pues ha servido de base para la redacción de los demás instrumentos de lucha contra el Lavado de Dinero como:

- La Declaración de Principios del Comité de Basilea acordada el 12 de diciembre de 1988, que nace en el Comité de Reglas y Prácticas de Control de las Operaciones Bancarias. Integrado por bancos centrales y órganos de vigilancia bancaria de Alemania, Bélgica, Canadá, EEUU, Francia, Italia, Japón Luxemburgo, Países Bajos, Reino Unido, Suecia y Suiza. Enfatiza en la importancia de que los bancos establezcan mecanismos de identificación de clientes, el cumplimiento de las leyes, cooperación con las autoridades judiciales y la negativa de participar en transacciones que aparentemente tengan vinculación con el lavado de dinero, con la finalidad de evitar que los bancos sean puente para el tránsito de capitales ilegales.
- Las 40 recomendaciones para prevenir el Lavado de Dinero del Grupo de Acción Financiera Internacional (GAFI) de febrero de 1990, conocidas como las 40 Recomendaciones del GAFI. Tienen cuatro bases fundamentales que son: a) sistemas jurídicos; b) medidas a adoptar por las instituciones financieras, empresas no financieras y profesionales para PLA/FT; c) institucionales y otras medidas necesarias en los sistemas de lucha contra el lavado de dinero y; d) cooperación internacional. Las 9 recomendaciones especiales adoptadas para combatir la financiación del terrorismo comprenden: a) la ratificación y aplicación de los instrumentos de las Naciones Unidas; b) tipificación de la financiación del terrorismo y blanqueo de dinero asociado; c) congelación y decomiso de activos terroristas; d) reporte de transacciones sospechosas relacionadas con el terrorismo; e) cooperación internacional; f) variante de remesas; g) transferencias electrónicas; h) organizaciones lucrativas y; i) envíos de dinero en efectivo.
- Las 19 recomendaciones del Grupo de Acción Financiera del Caribe aprobadas en la Reunión Ministerial sobre Lavado de Dinero en Kingston de noviembre de 1992 y elaboradas en la conferencia de Aruba sobre Lavado de Dinero de junio de 1990 comprenden: dependencias especializadas en la lucha contra el lavado de dinero; delito de lavado de dinero; el privilegio de la relación cliente-abogado; confiscación; registros contables; información sobre movimientos monetarios; cooperación administrativa; entrenamiento y ayuda.

- El Convenio del Consejo de Europa relativo al lavado, la investigación, la incautación y el decomiso del producto del delito, del 8 de noviembre de 1990 conocido como el Convenio de Estrasburgo.
- La Declaración y Programa de Acción de Ixtapa, México del 20 de abril de 1990 en el numeral 6 hace hincapié en la necesidad de tipificar como delito toda actividad relacionada al lavado de activos para facilitar la identificación, el rastreo, la aprehensión, el decomiso y la confiscación de tales activos.
- La Directriz del Consejo de las Comunidades Europeas del 10 de junio de 1991, centrada en que la lucha contra el lavado de dinero no debe limitarse al enfoque penal sino a la prevención de la utilización del sistema financiero en el blanqueo de capitales.
- El Reglamento Modelo de la Comisión Interamericana para el Control del Abuso de Drogas (CICAD). Entidad que es el foro político del hemisferio occidental, establecido por la Asamblea General de la Organización de Estados Americanos (OEA) en 1986, maneja programas de acción por medio de su Secretaría Ejecutiva para suscitar la cooperación y coordinación entre los países miembros, cuyo objetivo es hacer frente a las consecuencias del tráfico de drogas, que suponen una creciente amenaza para la salud, el desarrollo económico, la cohesión social y el cumplimiento de la ley. Éste manual es uno de los documentos más importantes en Latinoamérica, porque establece estándares mínimos de control de las actividades delictivas del lavado de activos, pero no es mandatorio es una guía para lograr armonizar las legislaciones.
- La Declaración Política y el Plan de Acción Mundial de Nápoles, aprobados en la conferencia ministerial mundial sobre la delincuencia transnacional organizada y celebrada en Nápoles del 21 al 23 de noviembre de 1994.
- El comunicado de la conferencia ministerial de la cumbre de las Américas concerniente al lavado de dinero e instrumentos del crimen, emitido en Buenos Aires en diciembre de 1995.
- La legislación modelo examinada y finalizada en 1995 por El Programa de las Naciones Unidas para la Fiscalización de las Drogas (PNUFID). Principal organismo multilateral encargado de controlar los problemas relacionados con las drogas, organismo que no sólo ejecuta proyectos y actúa como consejero de muchos países sobre asuntos de política de drogas, sino que también funciona

como secretaría de la Comisión de Estupefacientes de la ONU. Esta legislación modelo fue destinada a servir como modelo para completar y modernizar la legislación contra el tráfico ilícito de estupefacientes y lavado de dinero, consta de tres partes: el lavado de dinero, el decomiso y la asistencia judicial recíproca.

- La declaración política y el plan de acción adoptados en 1998 por la Asamblea General de las NNUU, que mejora y actualiza la anterior con la finalidad de perfeccionar y fortalecer la acción de la comunidad internacional. Condena el lavado de activos y otros delitos graves, así como utilizar el sistema financiero para dichos fines. Solicita poner en práctica el crear un marco legislativo, un régimen financiero y reglamentario eficaz mediante el cumplimiento del principio conozca a su cliente, denuncia de actividades sospechosas, compartir información y eliminación del secreto bancario para los casos encaminados a la investigación del delito.
- Para apoyar el cumplimiento de los estándares internacionales en la materia, la Oficina de Drogas y Crimen de las Naciones Unidas desarrolla el Programa Mundial contra el lavado de activos, producto del delito y la financiación del terrorismo (GPML), el cual apoya el establecimiento de servicios de inteligencia financiera, su objetivo es el de aumentar las medidas adoptadas a escala internacional contra el LA/FT, se lleva a cabo en colaboración con otras organizaciones internacionales, regionales y nacionales interesadas como Interpol, el grupo especial de expertos financieros sobre lavado de capitales, la secretaria del Commonwealth, el Consejo de Europa y la CICAD. Este programa consta de tres actividades principales: la promoción de la cooperación, la comprensión del fenómeno del lavado de dinero y aumentar la eficacia de los organismos encargados de hacer cumplir las leyes.
- Directiva 2005/60/CE del Parlamento Europeo y del Consejo, del 26 de octubre de 2005, relativa a la prevención de la utilización de sistema financiero para el LA/FT. Contiene normas generales y medidas para la debida diligencia al cliente, aplicación a terceros, obligaciones de información, conservación de documentos, datos estadísticos, medidas de ejecución y de aplicación. Modificada posteriormente por Directiva 2008/20/CE.

- Directiva 2009/110/CE del Parlamento Europeo y del Consejo de 16 de septiembre de 2009 sobre el acceso a la actividad de las entidades de dinero electrónico, su ejercicio y supervisión prudencial.
- Las directrices globales sobre prevención de blanqueo de capitales para la banca privada más conocida como Principios de Wolfsberg. Es el resultado de los bancos integrados por: Citigroup, Banco de Tokio Mitsubishi Ltda, Santander Central Hispano S.A, HSBC, Deutsche Bank Ag, CreditSwisseGroup, ABN AmroBank , Barclays Banck, Golman Sachs, JP Morgan Chase, Société Générale y UBS AG, quienes establecieron 11 principios que debían ser adoptados por la banca privada y estos son: aceptación de clientes (directrices generales), aceptación de cliente (situaciones que requieren diligencia/atención adicional), actualización de archivos de clientes, prácticas para identificar actividades inusuales o sospechosas, análisis, responsables de control, comunicación a la dirección, formación e información, mantenimiento de registros, excepciones y desviaciones, organización de prevención de blanqueo de capitales. También son conocidos los principios de Wolfsberg para la prevención del blanqueo de dinero en banca de correspondencia y la declaración de Wolfsberg sobre supresión de la financiación del terrorismo son instrumentos internacionales que contribuyen a que la banca privada que haya adherido los mismos disminuya el riesgo frente a operaciones mundiales de carácter delictivo (Torres Soto 2010, 114-5).

Este régimen internacional que implican numerosas convenciones, resoluciones, leyes y reglamentos, de vigencia internacional algunas enfocadas a la penalización del delito y otras a la prevención del mismo hacen especial énfasis en:

- La tipificación del lavado de dinero como delito y la ampliación de la categoría de delitos precedentes de lavado de dinero para incluir a todos los crímenes graves. Debido a que cada vez es más difícil determinar si el lavado proviene del fraude, corrupción, narcotráfico, terrorismo, etc., se trata de dar autonomía al lavado de activos e incluir los otros delitos como origen del lavado.
- La extensión de las normas que regulan el lavado de dinero a los sectores no reglamentados con el objetivo de eliminar debilidades sectoriales, evitar que existan actividades que queden al margen de la ley y que se presten para el lavado de activos. Todas las recomendaciones internacionales solicitan a los estados que las instituciones financieras y de crédito, establezcan controles internos y

procedimientos de comunicaciones adecuadas para prevenir e impedir las actividades de lavado de dinero y para asegurar que todos los empleados reciban capacitación en procedimientos para combatir el lavado de dinero. Las autoridades deben orientar, respaldar y supervisar la ejecución de las responsabilidades a cargo de las instituciones.

- El desarrollar pericia en el área, es decir lo importante del entendimiento de las leyes para hacer que estas funcionen.
- El perfeccionamiento de los aspectos institucionales del régimen para combatir el lavado de dinero. Es decir, el establecimiento de un sistema para informar sobre transacciones sospechosas lo cual conlleva la creación de estructuras para recibir y tramitar la información revelada (Unidades de Inteligencia Financiera). Entidades que serán centros de intercambio de información, punto de almacenamiento y análisis de información para suministrar indicadores de lavado de activos y otros delitos financieros a otras instituciones.
- Cooperación internacional.
- Sugieren la implementación por parte de los sujetos obligados de políticas como:
 1. Conozca a su cliente.- Que implica el conocimiento de su moralidad comercial, sus actividades económicas y su perfil financiero, información útil para saber si una transacción es sospechosa. No se pretende que el banco sustituya el trabajo de la autoridad instigadora, simplemente se busca que ninguna persona pueda llevar a cabo operaciones relevantes sin que su identidad quede debidamente registrada.
 2. Conocimiento del mercado financiero.- los productos y servicios de las instituciones financieras están diseñados para satisfacer necesidades de sus clientes, por lo que se debe conocer los perfiles financieros que incluye su comportamiento usual para efectuar comparaciones de las transacciones de clientes con perfiles similares y detectar si se trata de una transacción inusual o sospechosa.
 3. Conocimiento del personal.- las instituciones financieras deben tener conocimiento pleno de su personal gerencial y operativo, lo que implica una revisión y evaluación periódica de los antecedentes personales, laborales, patrimoniales, condición social, capacidad económica, desempeño profesional, de esta manera se podrá prevenir, detectar y

sancionar oportunamente actividades disfuncionales o corruptas que facilitan el uso de la institución en el lavado de dinero.

4. Capacitación permanente en medidas anti lavado.- para ilustrar a empleados y funcionarios sobre las operaciones de lavado de activos, sus modalidades más frecuentes, sus obligaciones y responsabilidades en la prevención de tales actos.
5. Registro de transacciones inusuales.- con la finalidad de preservar la confianza en el sistema financiero, es importante tener una actitud vigilante, al volumen y movimiento de fondos de los clientes, los cuales deben guardar relación con su perfil financiero teniendo principal cuidado con las transacciones complejas, poco usuales o que no tengan un propósito económico visible.
6. Reporte de transacciones sospechosas.- se debe reportar transacciones que tengan indicios de estar conectadas con dinero procedente de una actividad criminal.

Estos documentos son la base a partir de los cuales se configuran los programas nacionales, pues no presentan un carácter self-executing, es decir, no son suficientes por ellos mismos y los estados deben tomar las medidas internas necesarias para su ejecución, Por ello, la tarea más grande la tiene cada país porque de ellos depende la elaboración de nuevas leyes y su transformación en acciones.

1.3. Opinión de los organismos internacionales respecto a los canales electrónicos

La globalización y por ende la libre circulación de personas, bienes y servicios, los vacíos jurídicos, la falta de control fronterizo, la fluidez de datos enviados a través de internet ha facilitado el lavado de activos y el financiamiento del terrorismo. Los teléfonos móviles y demás aplicativos que hoy en día permiten la globalización de la economía, están conectados a internet, medios totalmente desregularizados que permiten el anonimato y la fluidez de transacciones a través de todo el mundo complicando el seguir la pista de estos fondos y por ende determinar su origen. Razón por la cual, hoy en día conforme avanza el comercio electrónico y por ende la banca electrónica, los organismos internacionales insisten en un sistema de administración de riesgos acorde al giro de negocio de cada entidad, que implica el conocimiento pleno del cliente, de la fuente de

sus recursos y del uso de los canales a su disposición, que permitan determinar el comportamiento esperado de los clientes y por lo tanto el nivel de riesgo al que está expuesta la institución (Cabuli y Jatib 2006, 112).

La administración de riesgo como lo sugieren los estándares y mejores prácticas internacionales se puede llevar a cabo mediante los modelos COSO, COBIT, ISO 31000, Estándar Australiano y Basilea II, que involucran controles apropiados y procedimientos adecuados de monitoreo de riesgos como la medición de los controles existentes y del riesgo residual. Si bien la administración de riesgos de lavado de activos y financiamiento del terrorismo como se ha visto hasta el momento es un tema en el que han venido insistiendo los organismos internacionales, la banca electrónica se encuentra aún en desarrollo, por ende, varios de los riesgos que en ella se presentan son aún desconocidos para aquellas instituciones que están empezando a descubrir e incursionar en este campo. A continuación se hace un breve resumen de las recomendaciones y sugerencias que hasta el momento los organismos internacionales han hecho bajo esta perspectiva de banca electrónica:

El Comité de Basilea mediante el informe denominado Gestión de Riesgo para la Banca Electrónica y Actividades con Dinero Electrónico de marzo de 1998, menciona que el desarrollo del comercio electrónico podría crear nuevas oportunidades para los bancos en cuanto a la ampliación de sus mercados, fortalecimiento de su posición competitiva y reducción de costos de operación a nivel nacional e internacional. Debido a que, la banca electrónica se encuentra en la etapa inicial de desarrollo no se pueden medir algunos aspectos de los riesgos y es importante que los supervisores eviten establecer políticas que podrían obstaculizar la innovación y la experimentación de estas nuevas tendencias, ya que, una reglamentación prematura podría paralizar la innovación. Esto no exime a las instituciones financieras a desarrollar procesos de gestión de riesgo amplios, rigurosos y flexibles que permitan administrar adecuadamente los riesgos que conllevan estas nuevas actividades, buscando siempre un equilibrio entre riesgos y beneficios. El informe sostiene que los riesgos generados por la banca electrónica no son nuevos, pero la magnitud de su efecto puede ser nuevo para los bancos y sus supervisores, ya que los sistemas de dinero electrónico pueden ser atractivos para el lavado de dinero cuando ofrecen límites flexibles de saldos y disponen una posibilidad limitada de auditoría de las transacciones. Debido a que, la banca electrónica puede ser conducida a la distancia los bancos pueden enfrentarse a mayores dificultades para aplicar métodos

tradicionales de prevención y detección de la actividad criminal. (Comité de Basilea para la Supervisión Bancaria 1998, 1-26).

El Grupo de Acción Financiera Internacional (GAFI) ente intergubernamental establecido en 1989, promueven la implementación efectiva de medidas legales, regulatorias y operativas para combatir el lavado de activos, el financiamiento del terrorismo y la proliferación de armas de destrucción masiva, también trata de identificar vulnerabilidades a nivel nacional para proteger al sistema financiero internacional de usos indebidos. Las 40 recomendaciones más las 9 recomendaciones especiales contra el terrorismo del GAFI, constituyen un esquema completo y consistente que los países deben implementar para combatir el lavado de activos, el financiamiento del terrorismo y la proliferación de armas de destrucción masiva y se convierten en un estándar internacional. La recomendación número uno: evaluación de riesgos y aplicación de un enfoque basado en riesgos, sugiere a los países tomar medidas preventivas o mitigantes proporcionales a los riesgos identificados que permitan una asignación eficaz de recursos. La recomendación número diez: debida diligencia del cliente indica que, cada país debe asegurar que las instituciones financieras realicen procesos de debida diligencia, ya sea por ley o por medios coercitivos con la finalidad de identificar antes y durante la relación comercial al beneficiario final, el propósito y el carácter que se pretende dar a la relación comercial y examinar las transacciones llevadas a cabo a lo largo de esa relación comercial, con la finalidad de identificar que el comportamiento del cliente es coherente con el conocimiento del mismo, el alcance de tales medidas será bajo un enfoque basado en riesgos. En cuanto a las nuevas tecnologías, la recomendación quince enfatiza que, las instituciones del sistema financiero deben identificar y evaluar los riesgos de lavado de activos y financiamiento del terrorismo que pudieran surgir con respecto al desarrollo de nuevos productos y nuevas prácticas comerciales antes del lanzamiento de dichos productos con la finalidad de administrar y mitigar esos riesgos (GAFI 2012, 13-20).

El Grupo Wolfsberg recomienda que para las relaciones comerciales iniciadas por medio de canales electrónicos, se requiera una mayor diligencia previa a la apertura de la cuenta, se debe adoptar medidas específicas para identificar de forma satisfactoria a los clientes que no se presenten de forma física, es importante obtener y registrar información sobre los siguientes aspectos: propósito y razones de la apertura de cuenta, actividad esperada en la cuenta, origen del patrimonio (descripción de la actividad económica que ha generado el patrimonio), patrimonio estimado, origen de los fondos aceptados para la apertura de cuenta, referencias u otras fuentes que corroboren la información

proporcionada por el posible cliente. A no ser que se cuente con otras medidas que sean adecuadas para obtener información favorable y fiable de la persona que nos permita llevar a cabo la diligencia debida sobre un cliente, se debe tener lugar una entrevista personal con el cliente antes de la apertura de la cuenta (The Wolfsberg Group 2002, 3).

2. Normativa nacional

Como en tantos otros países del mundo, el marco legal ecuatoriana se dio en cumplimiento a la Convención de Viena de 1988 y de los demás estándares internacionales. Como Estado responsable de adoptar normativas para penalizar y prevenir el lavado de dinero, Ecuador ha suscrito un sinnúmero de tratados multilaterales entre los que sobresalen:

- Declaración de Guatemala “Alianza de las Américas contra el Narcotráfico”, Guatemala 1986.
- Declaración y Programa de Acción de Ixtapa, México 1990.
- Reglamento Modelo sobre Delito de Lavado, Tráfico Ilícito de Drogas y Delitos Conexos, Bahamas 1992.
- Convención Interamericana sobre Asistencia Mutua en Materia Penal, Bahamas 1992.
- Estrategia Antidrogas en el Hemisferio, Buenos Aires, 1996.
- Convención Interamericana contra la Corrupción, Caracas Venezuela 1996.
- Convención Interamericana contra la fabricación y el Tráfico Ilícito de Armas de Fuego, Municiones, Explosivos y otros Materiales Relacionados 1997.
- Convención Interamericana contra el Terrorismo, Bridgetown Barbados 2002.
- Convención de las Naciones Unidas contra la Corrupción 2003.

También ha suscrito convenios de doble tributación con: Alemania, Argentina, Belarús, Bélgica, Brasil, Canadá, Chile, China, Corea, España, Francia, Italia, México Rumania, Singapur, Suiza, Uruguay y la Comunidad Andina (Perú, Bolivia, Colombia) (Barriga Bedoya 2011, 276-7).

Ecuador al estar en medio de dos países productores de droga, se ha convertido en un centro logístico de acopio y distribución de este producto y aún se encuentra en el camino para formar un cuerpo normativo e institucional fuerte para reprimir y prevenir el lavado de activos y financiamiento de delitos. Aunque ha progresado gracias al apoyo de organismos internacionales y países vecinos, la economía sigue evolucionando y con esta

las tipologías de lavado de activos. Es así que, brevemente se resumen los principales cambios que el país ha realizado en este ámbito:

La ley de sustancias estupefacientes y psicotrópicas anteriormente registraba en sus normas criterios para tipificar al delito de lavado de activos como un delito codependiente de los tipificados en esta ley. Por lo tanto, los tribunales penales debían en primera instancia sancionar a los responsables de los delitos graves de droga para que esta sea la carta habilitante para investigar un nuevo delito, el lavado de activos, esto impedía que Ecuador pudiera reprimir efectivamente al dinero producto de actividades ilícitas. El 18 de octubre de 2005, el presidente de la república el Dr. Alfredo Palacio y el Congreso Nacional derogan estas normas y promulgaron la ley 2005-12 denominada Ley para Reprimir el Lavado de Activos, la cual permitía: reprimir el delito de lavado de activos como un delito autónomo; crear un organismo que centraliza la información financiera del país para facilitar el análisis e investigación de recursos de origen ilícito; direccionar esfuerzos al sector financiero; crear el Consejo Nacional Contra el Lavado de Activos (CONCLA) y su órgano ejecutor la Unidad de Inteligencia Financiera dejando de lado a la Unidad de Procesamiento de Información reservada que pertenecía al CONSEP. Mientras que, el 24 de abril de 2006 se aprueba su reglamento (Torres Soto 2010, 122-6).

En febrero del 2010, el GAFI cataloga a Ecuador como país no cooperante en la lucha contra el lavado de activos y financiamiento al terrorismo por dos razones: la primera porque este organismo sostenía que la ley del 2005 era inconsistente en cuanto al lavado de activos y nula con respecto al financiamiento del terrorismo y la segunda porque el Gobierno de Rafael Correa había fomentado relaciones internacionales y de cooperación con Irán, que apuntaban a permitir el funcionamiento para la región del Banco de Desarrollo de las Importaciones de Irán (EDBI), institución sancionada por las Naciones Unidas por sus vínculos con grupos terroristas (Barriga Bedoya 2011, 273).

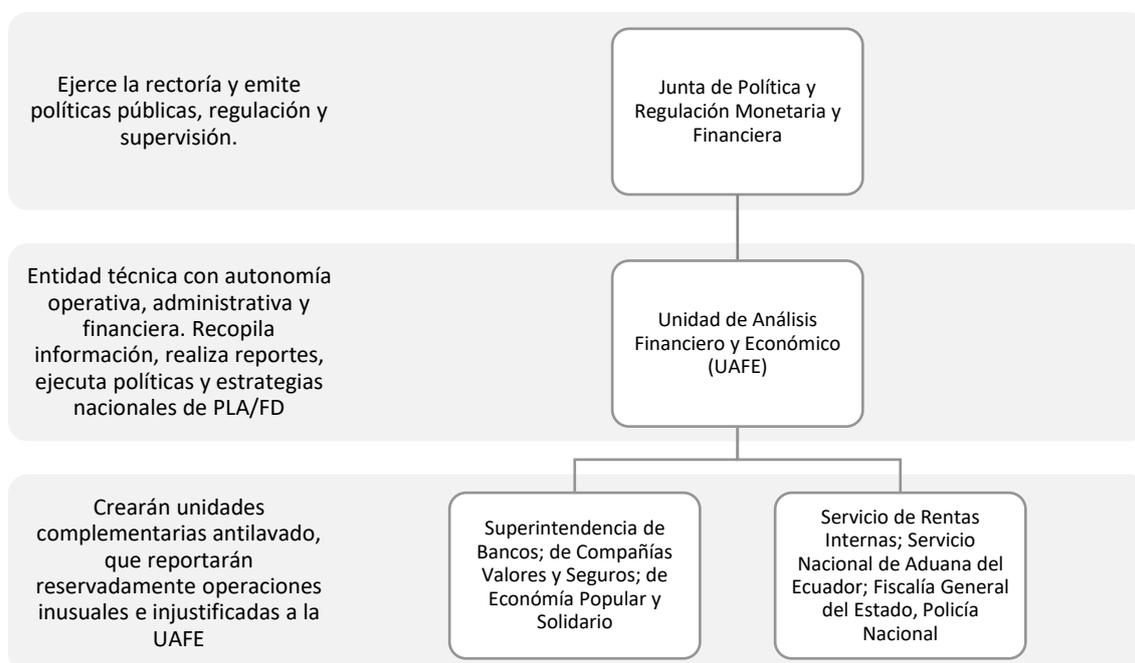
Por ello, la Procuraduría General del Estado presenta el proyecto de ley reformativa a la Asamblea Nacional, la cual incorpora los siguientes cambios: la tipificación de los delitos de terrorismo y su financiación; el fortalecimiento de la tipificación del delito de lavado de activos; la inmovilización de fondos o activos de propiedad de terroristas o vinculados a ellos y la expedición de regulaciones de supervisión que establecen controles preventivos de debida diligencia en los sectores bancario, de seguros, societario y de economía popular y solidaria. Motivo por el cual, el 22 de octubre de 2015 el GAFI resuelve eliminar definitivamente de sus listados a

Ecuador, debido a que estableció un marco legal y regulatorio que satisface los compromisos asumidos en su Plan de Acción (Barriga Bedoya 2011, 274).

Así también, su Unidad de Análisis Financiero y Económico (UAFE) cuenta con el apoyo en la lucha y prevención del lavado de activos de organismos internacionales como la ONU, la OEA y de grupos como el GAFI, GAFILAT y Grupo Egmont, al cual ingresó oficialmente el 31 de julio de 2016 auspiciado por las Unidades de Inteligencia de Perú y Argentina.

En cuanto al régimen institucional en materia de prevención de lavado de activos y financiamiento de delitos, está conformado de la siguiente manera:

Ilustración 5
Estructura Institucional



Fuente: (EC 2016, art.9-16)

Elaboración propia

Por otra parte, Ecuador cuenta con un sistema normativo que regula la prevención y sanción de actos de lavado de dinero y financiamiento de delitos, a través del sistema bancario que comprende normas penales y administrativas. El marco legal vigente en la materia es el siguiente:

- Ley Orgánica de Prevención, Detección y Erradicación del Delito de Lavado de Activos y del Financiamiento de Delitos. Publicada en el registro oficial No. 802 del 21 de julio de 2016.

- Reglamento General a la Ley Orgánica de Prevención, Detección y Erradicación del Delito de Lavado de Activos y del Financiamiento de Delitos. Publicada en el registro oficial suplemento No. 966 del 20 de marzo de 2017.
- Reglamento para la Aplicación de Sanciones por falta de envío de Información Prevista en la Ley de Prevención, Detección y Erradicación del Delito de Lavado de Activos y Financiamiento de Delitos: Publicada en el Registro Oficial No. 702 del 14-May-2012
- Libro I, Título XI, Capítulo III de la Codificación de Resoluciones de la Superintendencia de Bancos: Normas para las Entidades de los Sectores Financieros Público y Privado sobre Prevención de Lavado de Activos y del Financiamiento de Delitos como el Terrorismo.
- Código Orgánico Monetario y Financiero. Publicado en el registro oficial No.180 del 10 de febrero de 2014.
- Ley Orgánica de Prevención Integral del Fenómeno Socio Económico de las Drogas y de Regulación y Control del Uso de Sustancias Catalogadas Sujetas a Fiscalización. Publicada en el suplemento del registro oficial No. 615 de 26-Oct-2015.
- Código Orgánico Integral Penal. Publicada en el suplemento del registro oficial No. 180 de 10-Feb-2014.
- Normas de Prevención de Lavado de Activos, Financiamiento del Terrorismo y otros Delitos. Publicado en el registro oficial No.319 del 4 de septiembre de 2018.
- Manual Genérico de Prevención de Lavado de Activos de la Unidad de Análisis Financiero y Económico a través de la Dirección de Prevención de Lavado de Activos.
- Código de conducta de las entidades bancarias.

Además, la Junta Bancaria ha emitido varias resoluciones para regular de mejor manera el lavado de activos en las instituciones financieras que son el resumen de todas las obligaciones y compromisos asumidos por Ecuador al suscribir convenios y tratados internacionales.

El Libro I, Título XI, Capítulo III de la Codificación de Resoluciones de la Superintendencia de Bancos: Normas para las Entidades de los Sectores Financieros Público y Privado sobre Prevención de Lavados de Activos y del Financiamiento de

Delitos como el Terrorismo señala, la obligación de las entidades de los sectores financieros público y privados de contar con políticas y procedimientos de control orientadas a prevenir los riesgos de ser utilizados como instrumento para lavar activos y/o financiar el terrorismo y otros delitos, mismas que deben constar en el manual de prevención de lavado de activos y financiamiento de delitos como el terrorismo y en el Código de Ética para orientar a todos los miembros de la entidad. Habla también de la debida diligencia y sus procedimientos; del perfil transaccional y de comportamiento del cliente; de las políticas conozca su cliente, conozca su empleado, conozca su proveedor, conozca su corresponsal y conozca su mercado; de la estructura organizacional y de la capacitación. Así también, el artículo 6 señala que sobre la base de factores y criterios de riesgo establecidos por la entidad, las políticas y procedimientos de control deben estar descritos en una matriz de riesgo.

Desde junio de 2018 la Superintendencia de Bancos ha socializado y trabajado junto los oficiales de cumplimiento de las instituciones financieras en dos normas, la primera la Reforma a la Norma de Control Interno para las Entidades que Conforman los Sectores Financieros Público y Privado, sobre Prevención, Detección y Erradicación del Delito de Lavado de Activos y del Financiamiento de Delitos como el Terrorismo, compuesta por: las políticas y procedimientos de control interno; mecanismos para el cumplimiento de las políticas conozca su cliente, conozca su mercado, conozca su accionista, conozca su empleado y conozca su corresponsal; estructura organizacional en las que se detallan: las funciones del directorio, del comité de cumplimiento, del representante legal, del oficial de cumplimiento titular y suplente e informe del oficial de cumplimiento; las unidades de control en las que se encuentran: el auditor interno y externo; procesos y procedimientos para registrar la información, mantener sus archivos físicos y digitalizados y reportarla a la Unidad de Análisis Financiero y Económico (UAFE); finalmente la reserva y confidencialidad del reporte de transacciones inusuales e injustificadas de personas no autorizadas. La segunda, una propuesta de Norma de Control que Regula los Sistemas de Administración de Riesgos de Lavado de Activos y del Financiamiento de Delitos como el Terrorismo, en el que se solicita el diseño e implementación de un sistema de administración del riesgo de lavado de activos y de financiamiento de delitos como el terrorismo el cual deberá contener etapas como: identificación, medición y evaluación, control y monitoreo; elementos como: políticas, procesos y procedimientos; e instrumentos como: señales de alerta, aletas tempranas, identificación, análisis de operaciones inusuales, determinación y reporte de operaciones inusuales e injustificadas,

segmentación de factores y seguimiento de operaciones. Sus publicaciones se darán en los próximos días.

Por otro lado, en el 2019 Ecuador será objeto de la evaluación del GAFI, razón por la cual la Superintendencia de Bancos está participando en la evaluación nacional de riesgo que lidera la UAFE con la asistencia técnica del Banco Mundial y donde tienen lugar un número importante de sectores de la economía, entre ellos el sector real y por supuesto, el financiero a través de la Asobanca.

3. Análisis comparativo ventajas y limitaciones de la normativa nacional

Como hemos visto en el punto anterior, Ecuador ha enfocado sus esfuerzos en mejorar tanto la institucionalidad como la normativa de prevención de lavado de activos y otros delitos, para ello ha solicitado la ayuda y asesoría de países como Colombia, cuyo sistema de administración de riesgos SARLAFT ha sido reconocido internacionalmente, pues está fundamentado en las técnicas de gestión de riesgo como: COSO, COSO ERM, COBIT, ISO 31000, Estándar Australiano AS/NZS, así como, se complementa de los demás sistemas de administración de riesgos obligatorios como: Saro para riesgo operativo, Sarc riesgo crediticio, Sarm riesgo de mercado y Sarl riesgo de liquidez, pero no es un estándar, ya que cada entidad debe desarrollar y perfeccionar su propio SARLAFT (Infolaft Anticorrupción, fraude y LA/FT 2017, párr.87).

La administración del riesgo de LA/FT tiene una naturaleza diferente a la de los procesos de administración de los riesgos operativo, crédito, mercado, liquidez, etc., pues mientras que los mecanismos para la administración del primero se dirigen a prevenirlo, detectarlo y reportarlo oportuna y eficazmente, los mecanismos para la administración de los segundos se dirigen a asumirlos íntegra o parcialmente en función del apetito al riesgo de la institución y la relación riesgo rentabilidad.

Los organismos internacionales recomiendan el enfoque basado en la gestión de riesgos, pasar del conozca a su cliente al complejo y exigente conozca su riesgo, emplear métodos técnicos de gestión de riesgo que permitan identificar los factores de riesgo que generan una amenaza a la entidad.

Por ello podemos decir que, entre las ventajas de que Ecuador destine una norma a la administración de riesgos están:

1. Análisis de las vulnerabilidades de la entidad.

2. El enfoque deja de ser el cumplimiento normativo para pasar a la administración del riesgo propio de la institución.
3. Permite la participación de toda la institución por lo que deja de ser la prevención del LA/FT una obligación solo del oficial de cumplimiento para convertirse en responsabilidad de todos.
4. Permite que la parte comercial avance de la mano de los controles y en armonía con el área de cumplimiento.
5. La supervisión toma una dinámica diferente, pues pasa de ser una inspección de cumplimiento normativo a estar enfocada en el riesgo de cada institución.
6. Permite que los sistemas de administración sean una herramienta que contribuye a la prevención y control del riesgo LA/FT.
7. Permite contar con los argumentos necesarios para tomar decisiones propias del negocio, por ejemplo: para seleccionar el mercado objetivo, selección de productos o canales a promocionar, funcionarios cuyos conocimientos deben ser reforzados, inversión en software y hardware para un mejor control y monitoreo, segmentos de clientes a quienes se deben aplicar un tipo de debida diligencia en particular o con los cuales se debe terminar la relación comercial, operaciones que requieren un monitoreo especial, etc.

Sin embargo, un sistema de administración de riesgos requiere de una sólida base de datos, la cual es difícil de obtener si tomamos en consideración lo antes mencionado, el riesgo de LA/FT se previene, detecta y reporta por lo que a diferencia de los otros riesgos no tiene equivalencia económica ni se cuenta con información histórica suficiente de hechos de LA/FT que se hayan dado en la institución, es por ello que la mayor parte se basará en juicio de experto o datos del sector que no van a explicar necesariamente la realidad de la entidad. Entre las desventajas de adoptar esta nueva norma tenemos:

1. Si bien, la norma próxima a aprobarse ha sido socializada con el sector financiero, esto no ha permitido un aporte al SARLAFT, de tal manera que se apege a la realidad de los sujetos obligados del país, más bien se ha mantenido la misma esencia de la norma Colombiana.
2. No todos los sectores cuentan con una buena calidad de información, por lo que en principio será difícil contar con buenas bases de datos que alimenten al sistema de administración de riesgos.
3. Debido a la diferencia que existe entre cada entidad por el tipo de operaciones, número de clientes, volumen, etc., es complejo la utilización de los criterios

mínimos obligatorios para definir la segmentación, el cumplimiento de las condiciones de homogeneidad y heterogeneidad al universo real de clientes.

4. Con frecuencia hay señales de alerta que no la involucran dentro de los criterios mínimos, por lo que el monitoreo se convierte en precario y el sistema deja de ser un sistema para convertirse en una verificación de cumplimiento limitado por etapas que no cubren todos los factores de riesgo ni toda la realidad de la entidad.
5. Las entidades dependen de las personas que han hecho los procesos de diseño e implementación de sus sistemas, olvidando documentar. De esta manera, ante la ausencia de dichos funcionarios es difícil establecer como mínimo qué se hizo, cómo se construyó y ante todo cómo funciona. Incluso cuando hay documentación es dispersa, no es coherente y no está actualizada, lo cual limita el entendimiento que se requiere de las definiciones de la entidad vigilada por parte del supervisor y lo peor, por parte de la propia organización.
6. La supervisión deberá ser más objetiva para entender si el sistema de administración de riesgos responde a los riesgos reales de la entidad, caso contrario no servirá de nada los esfuerzos de los sujetos obligados en implementarla, si la supervisión será bajo parámetros estandarizados.

Por otra parte, también hemos querido presentar como la normativa ecuatoriana se apega a los estándares internacionales. Para ello hemos tomado los puntos relevantes de los estándares internacionales y los hemos comparado con el Capítulo III Normas para las Entidades de los Sectores Financieros Público y Privado sobre Prevención de Lavado de Activos y del Financiamiento de Delitos como el Terrorismo, Título X del Control Interno, Libro I Normas de Control para las Entidades de los Sectores Financieros Público y Privado, cuyos resultados se muestran a continuación:

Tabla 5
Comparación de los estándares internacionales con la norma ecuatoriana

Estándares Internacionales	Normativa Ecuatoriana
Deber de informar	Si, a través de los ROII, cuyo respaldo y evidencia debe ser archivada por 10 años.
Deber de confidencialidad	Sección III, en el caso de que algún empleado o funcionario lo incumpla deberá ser reportado en un ROII a la UAFE, para que este en su defecto comunique a la Fiscalía General del Estado.
Conozca a su cliente	Sección V, se especifica la debida diligencia a realizar, los procedimientos de conocimiento del cliente, la información y documentación mínima a solicitar.
Conozca su mercado	Artículo 29, señala que se debe contar con información de los sectores económicos, evolución de ingresos, zonas geográficas, principales variables macroeconómicas que influyen en los mercados y ciclos de las actividades económicas para determinar características homogéneas, segmentar clientes e identificar comportamientos inusuales.
Conozca a su empleado	Artículo 24, enfatiza la solicitud, revisión y validación previa al inicio de la relación contractual de directores, ejecutivos, funcionarios, empleados y personal temporal, para determinar si su nivel de vida está acorde a sus ingresos.
Conozca a su corresponsal	Artículo 31, se debe conocer la naturaleza de la actividad comercial del corresponsal, mantener y actualizar su información, conocer los productos y servicios que posee, así como las políticas y procedimientos que posee para prevenir el riesgo de LA/FT, gestión anual y relaciones en el mercado.
Programas de capacitación del personal.	La sección VIII, señala que se deben diseñar y coordinar programas de capacitación sobre PLA/FD para todo el personal al menos una vez al año, en el proceso de inducción, a terceros relacionados con el negocio, cuyos resultados deberán ser evaluados por escrito.
Sistema de control interno.	La sección II políticas y procedimientos de control, sección IV del manual de PLA/FT y VII de la estructura organizacional, incluyen los procedimientos y controles internos comprendiendo el nombramiento de las personas responsables al nivel de dirección.
Principios de cooperación.	Las entidades de los sectores financieros público y privado deben registrar, reportar a la UAFE y mantener sus archivos físicos o digitalizados de la información a la que se refieren las letras c), d) y e) del artículo 4 de la Ley Orgánica de Prevención, Detección y Erradicación del delito de Lavado de Activos y del Financiamiento de Delitos.

Fuente: (EC 2018)
 Elaboración propia

En cuanto al uso de la tecnología para abrir cuentas y efectuar transacciones, en Ecuador no hay normativa específica que regule su accionar. Sin embargo, como hemos visto la tecnología avanza y por ende la banca se ha visto en la obligación de avanzar también y lo ha hecho apegado a la actual normativa y basándose en las recomendaciones de los organismos internacionales para mitigar los riesgos de LA/FT existentes.

En nuestro derecho no se establece prohibición alguna que impida u obstaculice que los contratos bancarios puedan formalizarse telemáticamente. De hecho, la Ley de Comercio Electrónico, Firmas y Mensajes de Datos ha sido parte fundamental para que varias instituciones financieras puedan llevar a cabo sus proyectos de banca electrónica, pues en esta ley se contemplan varios aspectos como: la recopilación de datos personales de fuentes accesibles al público para vincular o mantener relaciones comerciales o de cumplimiento de contratos; la utilización de bases de datos con el consentimiento del titular; la validez de la firma electrónica al igual que una manuscrita como prueba en un juicio; el consentimiento para aceptar mensajes de datos siempre y cuando el consumidor sea informado clara, precisa y satisfactoriamente sobre todos los requisitos, condiciones y restricciones para adquirir y hacer uso de los bienes o servicios promocionados. Así también, esta ley señala que: “cualquier actividad, transacción mercantil, financiera o de servicios, que se realice con mensajes de datos, a través de redes electrónicas, se someterá a los requisitos y solemnidades establecidos en la ley que las rijan, en todo lo que fuere aplicable y tendrá el mismo valor y los mismos efectos jurídicos que los señalados en dicha ley” (EC 2002, art.44-51). Señala además que, los contratos podrán ser instrumentados mediante mensajes de datos y no se negará su validez por la sola razón de haberse utilizado en su formación uno o más mensajes de datos, debiendo también estar disponible la información escrita por si el consumidor lo requiere.

En Ecuador, muchas instituciones financieras han tenido que aliarse con varias Fintech para poder ofrecer sus productos y servicios a través de medios electrónicos. Así tenemos varios emprendimientos que de seguro son complementos vitales para la banca:

- Kullki es una plataforma para conectar prestamistas y solicitantes de microcréditos a tasas competitivas. Virtualiza el rol del “oficial de crédito” y brinda servicios como: apertura de cuenta mediante reconocimiento biométrico (PhoneApp), determinación de riesgo crediticio por Minería de Datos Financieros, cálculo del monto de seguro de protección al inversionista por no-pago del beneficiario y simulación de escenarios de inversión.

- Helio.geo, un producto de la firma ecuatoriana Handytec, provee de análisis y modelos predictivos basados en datos geoespaciales que permiten realizar estudios de mercado o pronosticar el comportamiento de un producto (Astudillo 2018, párr.20).
- CreditAccess Plataforma de búsqueda de créditos para que los ciudadanos comparen las condiciones de los préstamos que ofrecen las instituciones financieras del país y tomen mejores decisiones.
- Kapitalika Es un sistema blockchain que permite a la banca ofrecer a sus clientes los servicios de wallet y xChange para inversiones en bitcoin y ethereum. Reduce el riesgo de fraude en inversiones en criptomonedas de una manera formal y legal.
- Nodalblock proveedor de servicios de autenticación e identidad que utiliza blockchain y una autenticación sólida para un KYC más confiable, trazabilidad certificada y sistema seguro de compartición de datos.
- Mensajea ofrece un chatbot que es un robot que simula, por voz o por texto, una conversación humana y permite atender a clientes las 24 horas del día utilizando un motor de inteligencia artificial y un motor de lenguaje natural; este último es un programa que reconoce la estructura de una frase y que ayuda a entender lo que dice el cliente (Tapia y Maldonado 2018, párr.52).

Actualmente, en el país las Fintech funcionan en asociación con la banca, pues por una parte aún no existe una regulación específica para ellas y por otro lado, necesitan mayor comprensión de las regulaciones del país y del funcionamiento de la banca. Evidentemente, esto significa un trabajo conjunto entre Fintech, instituciones financieras y entes reguladores, pues mientras la primeras desarrollan nuevas tecnologías que permiten a las instituciones financieras llegar con más facilidad a clientes no bancarizados de áreas suburbanas, donde la gente talvez no usa los servicios de un banco pero está familiarizada con el uso de celulares e Internet; los organismos de control deben emitir una regulación específica referente a billeteras móviles y electrónicas, donde se autorice a los bancos a abrir cuentas, otorgar créditos entre otros productos y servicios a través de la telefonía móvil, donde se definan en qué casos se podrá usar este sistema, para qué, sobre qué montos, bajo qué controles y otros factores importantes para garantizar la seguridad de los involucrados y reducir la vulnerabilidad de los mismos para el lavado de activos. Hoy en día el sector financiero ha tenido que administrar los riesgos que implica

ser un banco digital, apoyado en el conocimiento del cliente y en un enfoque basado en riesgos. Sin embargo, el no contar con estándares internacionales y regulaciones claras vuelve más susceptible al sistema financiero de ser blanco de los delincuentes, no solo en lo que tiene que ver con lavado de activos y financiamiento del terrorismo o seguridad de la información, sino en todos los campos que hacer banca implica.

Capítulo cuarto

Estructura del sistema de administración del riesgo de lavado de activos y financiamiento del terrorismo para la banca electrónica de una institución financiera ecuatoriana

1. El sistema financiero privado ecuatoriano y la banca electrónica

Luego de la crisis financiera de 1999, el sistema financiero ecuatoriano se dedicó a recuperar la confianza de los cuenta ahorristas a través del fortalecimiento de la normativa y de su gestión, con el fin de alejarse de los factores que provocaron la crisis y convertirse en un sistema sólido, líquido y cubierto. El alto dinamismo de los bancos privados ha permitido presentar un desempeño eficiente y solvente en los últimos años, pues en conjunto a enero de 2019, según el último reporte de la Asobanca lograron utilidades netas de 50 millones USD, respondiendo así adecuadamente a la evolución de la economía. Debido a que, en la actualidad los bancos no son la única opción para acceder al mercado financiero, las entidades tienen que ser competitivas y usar mayor cantidad de herramientas tecnológicas que les permitan estar al nivel que los usuarios esperan en aspectos como usabilidad, conectividad y disponibilidad al alcance de la mano. Las redes sociales por ejemplo, en la industria financiera pueden ser un canal que incremente las ganancias de los bancos haciendo trascender su papel como medio de comunicación dentro del entorno digital, permitiendo especializar al recurso humano en tareas más avanzadas y menos técnicas (Maldonado, Burgos y Chávez 2018, 48 - 98).

El sistema financiero ecuatoriano representa alrededor del 3% del PIB pero su aporte al dinamismo y funcionamiento de la economía es mayor, ya que, de no ser por la intermediación, ninguna actividad podría desarrollarse de manera adecuada. Las tarjetas de crédito han contribuido a incrementar los ingresos de los bancos privados; mientras que, los nuevos canales electrónicos como: tarjetas de débito, cajeros multifunción, pagos de servicios, cancelación de tarjetas, pagos en la web y corresponsales no bancarios han ayudado a reducir costos. Es así que, el gasto de operación versus el total de activos promedio estimado es de 4,61% (Lizarzaburu 2018, 18). En los últimos años el tema central para las instituciones financieras ha sido la innovación, desde el 2016 la banca ecuatoriana ha impulsado en sus clientes el uso de aplicaciones móviles con el fin de simplificar procesos y evitar las tediosas filas en los bancos. Esta nueva forma de banca

va de la mano de la digitalización de la economía, por ello ofrecen atención personalizada, asesorías e información, motivo por el cual, el 44,1% de la población del Ecuador usa hoy en día los servicios bancarios en línea (Tapia 2018, 5).

Hace cinco años Banco Pichincha proporcionó a sus clientes una aplicación móvil y el servicio de mensajería, hoy en día permite abrir cuentas, realizar consultas, pagos, transferencias, recargas o solicitar certificados bancarios. En esta institución, el uso de canales digitales pasó de 27% en 2012 a 55% en 2018, es así que, las transacciones en las agencias decrecieron en 6%, mientras que las realizadas en cajeros automáticos registraron un crecimiento menor al 7%. Así también, las transacciones a través del app Banca Móvil hasta noviembre de 2018 crecieron en un 96% con respecto al mismo periodo en 2017 (Tapia 2018, 5).

Por otro lado, Banco Guayaquil redujo de 3 millones a 1,8 millones las transacciones en agencias físicas y ofrece desde marzo de 2018 la opción de contratar créditos desde la banca en línea, además ha implementado reconocimiento facial a sus aplicaciones para dar más confianza al usuario y ofrece la opción de chatear a través de Facebook con un asesor financiero. Banco ProCredit redujo de 26 a 10 agencias entre 2016 y 2017 lo que representó 3 millones de inversión y costo. La plataforma del banco permite a los clientes acceder a video llamadas y chats en línea con los ejecutivos. Produbanco en cambio, invirtió 700 millones USD en el desarrollo de la aplicación y marketing de la cuenta Be, además desde 2016 posee un app que permite a los jóvenes abrir cuentas sin depósito inicial desde el celular. En enero de 2018 Banco Pacífico lanzó la aplicación para que los clientes usen sus tarjetas de crédito y débito desde el celular BDP Wallet, así como, Banco Machala permite comprar y realizar pagos sin la necesidad de presentar su tarjeta física u otros dispositivos adicionales, solo con el celular y a través del escaneo del código QR, que estará en lavanderías, farmacias, gasolineras, restaurantes, boutiques, supermercados, etc. La Asobanca por su parte, desarrolla la plataforma Bimo con la que busca reemplazar el dinero electrónico que dejó de funcionar en marzo de 2018 (El Universo 2018, párr.8). Finalmente, Banco Bolivariano en los primeros meses del 2019 ha invertido en la publicidad de su nueva Banca Móvil y Avi24 asesor virtual inteligente para consultar movimientos, saldos y pagos.

Con estos antecedentes, en la siguiente tabla se muestran los principales productos y servicios que en la actualidad las instituciones del sistema financiero privado ecuatoriano ofrecen con ayuda de internet a través del uso de aplicativos móviles:

Tabla 6
Principales productos y servicios que instituciones financieras ecuatorianas ofrecen a través de internet

Institución financiera	Productos / Servicios
Produbanco	<ul style="list-style-type: none"> • App Be de Produbanco, permite la apertura de cuentas cargando una selfie, obtener en 48 horas la tarjeta de débito, transferencias y retiros en cajeros sin tarjeta de débito, pagos de servicios, compras por internet, depósitos por cajeros automáticos, chatear con un asesor para consultas. Todo desde el celular. • Payphone plataforma multinacional que le permite pagar con sus tarjetas de débito desde su celular.
Banco Pichincha	<ul style="list-style-type: none"> • Apertura cuenta de ahorros online “cuenta ahorra tiempo” • Solicitud de créditos online • Solicitud de código de retiro para terceros a través del celular.
Banco Guayaquil	<ul style="list-style-type: none"> • App YoDigital para pagos, transferencias y depósitos en cheque. Permite apertura de cuenta de ahorros a través del reconocimiento facial y sin depósito inicial.
Banco ProCredit	<ul style="list-style-type: none"> • ProCredit Direct aplicación móvil para consultas de saldos y transferencias sin ir a agencias. • Tarjeta de débito para empresas. • Depósitos y retiros sin necesidad de tarjeta de débito • Solicitud de apertura de cuenta y crédito. • Chatear con un asesor para consultas • Payphone plataforma multinacional que le permite pagar con sus tarjetas de débito desde su celular.
Banco Pacífico	<ul style="list-style-type: none"> • BdP Wallet primera billetera digital • Plataforma digital "Onboard BdP", aplicación con la cual se pueden abrir cuentas de ahorro desde el celular con una selfie en tan solo cinco minutos, sin depósito inicial y sin acudir al banco, pues la firma del contrato es digital. Así también, permite efectuar pagos, consultas y transferencias bancarias. • Crédito Ágil Pacífico, cuya aprobación es en línea.
Banco Bolivariano	<ul style="list-style-type: none"> • QuickPay para realizar transferencias y retiros de efectivo en cajeros usando el celular. • Avi24 asesor virtual inteligente para consultar movimientos, saldos y pagos. • 24Movil Banca celular al que se puede ingresar con Touch ID a QuickPay y Quickview para revisar movimientos de cuentas.
Banco Machala	<ul style="list-style-type: none"> • Machalawallet que con solo descargar el app y registrar sus tarjetas, permite efectuar pagos a través del escaneo del código QR que se encuentra en los establecimientos auspiciantes.

Fuente: Información de páginas web de las Instituciones Financieras
 Elaboración propia

La disponibilidad 24/7 para cubrir las necesidades de los clientes en cualquier momento y lugar del mundo, es una parte importante de la banca electrónica, por lo tanto, debe brindar todas las opciones requeridas para el desarrollo de las transacciones, proveer canales alternativos de comunicación para brindar respuestas oportunas y ágiles al cliente y sobre todo seguridad.

Tomando en consideración que Internet es una red pública y por ende cualquier información personal necesaria para la transacción puede ser visualizada o modificada por personas no autorizadas, la prevención del lavado de activos y financiamiento del terrorismo implica conocer plenamente al cliente o contraparte y contar con los mecanismos necesarios para (Peña Valenzuela 2007, 170):

1. La identificación de cada una de las partes que intervienen en la transacción, ¿quién eres?
2. La autenticación de la identidad de los involucrados en la transacción (ahora que te identificaste, demuéstreme que eres quien dices ser)
3. Control de acceso a los recursos como páginas web exclusivas para usuarios registrados (ahora que sé quién eres, te permito acceso a los recursos que quieres y nada más)

Entre los mecanismos empleados por las instituciones financieras, para evitar que personas no autorizadas accedan a la información o a fondos de un cliente e incluso se vinculen a una institución financiera suplantando la identidad de otra persona, están (Peña Valenzuela 2007, 173-8).

1. El uso de algo que como cliente sé, usuario y contraseña. Sin embargo, el usuario es vulnerable al conocimiento de una persona no autorizada y en el caso de la contraseña puede ser adivinada o descifrada. Por ello la autenticación no debe depender de la contraseña sino de uno o varios factores adicionales como algo que tengo (tarjeta de débito), algo que soy (biométricos—huella, voz, reconocimiento facial) estos incluso evitan la suplantación.
2. Tecnologías de encriptación que permiten cifrar la información mientras transita por internet y una o varias llaves para que cada parte pueda activar el algoritmo de encriptación y desencriptación.
3. Certificados digitales entregados por entidades confiables (reguladas y vigiladas) que hayan verificado exhaustivamente la identidad.

Ejemplos de los mecanismos implementados por algunas entidades financieras ecuatorianas las mostramos a continuación:

1. Produbanco, además de las claves, utiliza reconocimiento biométrico y un sistema de autenticación en el que el usuario debe ingresar un patrón de coordenadas y reconocer una imagen.
2. Banco Pichincha requiere múltiples claves de acceso para el uso de la banca en línea.
3. Banco Guayaquil, lanzó en el 2015 un sistema de reconocimiento facial para los usuarios de su aplicación móvil.

En cuanto a los mecanismos implementados por entidades financieras extranjeras, para transacciones a través de ATM tomamos como ejemplo el caso de Bank of America Corporation, la cual posee:

1. Cajeros que leen la tinta magnética, por lo que lee la cantidad escrita en un cheque usando un reconocimiento óptico de caracteres.
2. Los cajeros escanean los billetes depositados usando el reconocimiento óptico de caracteres y verifican su autenticidad al compararlo con las imágenes que el Departamento del Tesoro de EEUU proporciona.

Luego de que hemos revisado y entendido como el sistema financiero ecuatoriano ha incorporado estas nuevas tecnologías al giro de su negocio, empezamos con la aplicación y análisis de cada una de las etapas del proceso de administración de riesgo de LA/FT que definimos y explicamos en el capítulo segundo:

2. Identificación de eventos de riesgo de LA/FT

Con el objetivo de identificar aquellas vulnerabilidades que pueden ocasionar impactos negativos a la entidad, primero se diagrama los flujos de los procesos bajo análisis y segundo se enlista los eventos de riesgo de LA/FT hallados luego de entrevistar a cada uno de los involucrados y a las unidades de apoyo de los procesos de apertura de cuentas online y uso de los ATM de la institución financiera, cuyos resultados mostramos a continuación:

2.1. Apertura cuenta online

El proceso de apertura de cuentas on-line inicia cuando el interesado ingresa a la página web de la institución y completa en línea la solicitud de apertura de cuenta, en la

cual puede adjuntar documentos como: cédula, papeleta de votación, servicio básico, soporte de actividad económica e ingresos mensuales. Esta solicitud es recibida por el especialista de banca telefónica, quien verifica la información registrada por el cliente en páginas oficiales como: registro civil, CNT, SRI, función judicial, SB y listas nacionales e internacionales de restricción.

Si la solicitud está completa y el especialista de banca telefónica no encuentra señales de alerta para detener el proceso, llama al solicitante para confirmar su interés por abrir la cuenta con la institución, si la respuesta es positiva el especialista de banca telefónica informa que su solicitud está siendo procesada y que en un lapso de 72 horas un asesor al cliente tomará contacto con él. Enseguida, crea una incidencia, con la solicitud y todos los documentos presentados por el solicitante. Con esto, la tarea pasa a procesos centralizados, quienes validan que se encuentre la solicitud de apertura, los documentos soporte, la revisión en listas de restricción y verificaciones en las páginas web de la función judicial, SB y SRI, si el especialista de procesos centralizados no encuentra novedades procede a ingresar: datos personales, actividad económica, información financiera, datos del cónyuge (si aplica), origen de fondos y referencias en el sistema. Abre la cuenta y solicita tarjeta de débito y código de depósito, ya que la tarjeta demora en ser elaborada 10 días, finalmente responde la incidencia adjuntado número de cuenta y contratos para que el asesor al cliente se contacte con el solicitante para su visita y formalice la firma de contratos, tarifarios, entrega de tarjeta de débito, código de depósito y acceso a banca en línea.

Por el contrario, si el especialista de banca telefónica identifica que la solicitud está incompleta o el solicitante no adjuntó documentos soporte, procede a contactarlo para completar la información y solicitar la documentación pertinente. En caso de no poder comunicarse por teléfono o si el cliente no dispone de tiempo en ese momento para proporcionar la información requerida, el especialista de banca telefónica envía un correo al solicitante para darle a conocer los requisitos e información adicional que debe proporcionar previo la apertura de la cuenta. Una vez que cuenta con la información, procede a validarla y en el caso de encontrar novedades, como por ejemplo: casos en función judicial, inhabilitaciones de cuentas en otras instituciones por parte de la SB, deudas al SRI, coincidencias en listas PEP, clientes de alto riesgo, etc., que pueden ser autorizadas por el Coordinador de Punto de Servicio, Jefe de Procesos Centralizados y Gerencia General, notificará a estas personas del particular para su autorización según corresponda. Autorización que deberá adjuntar en la incidencia que enviará a procesos

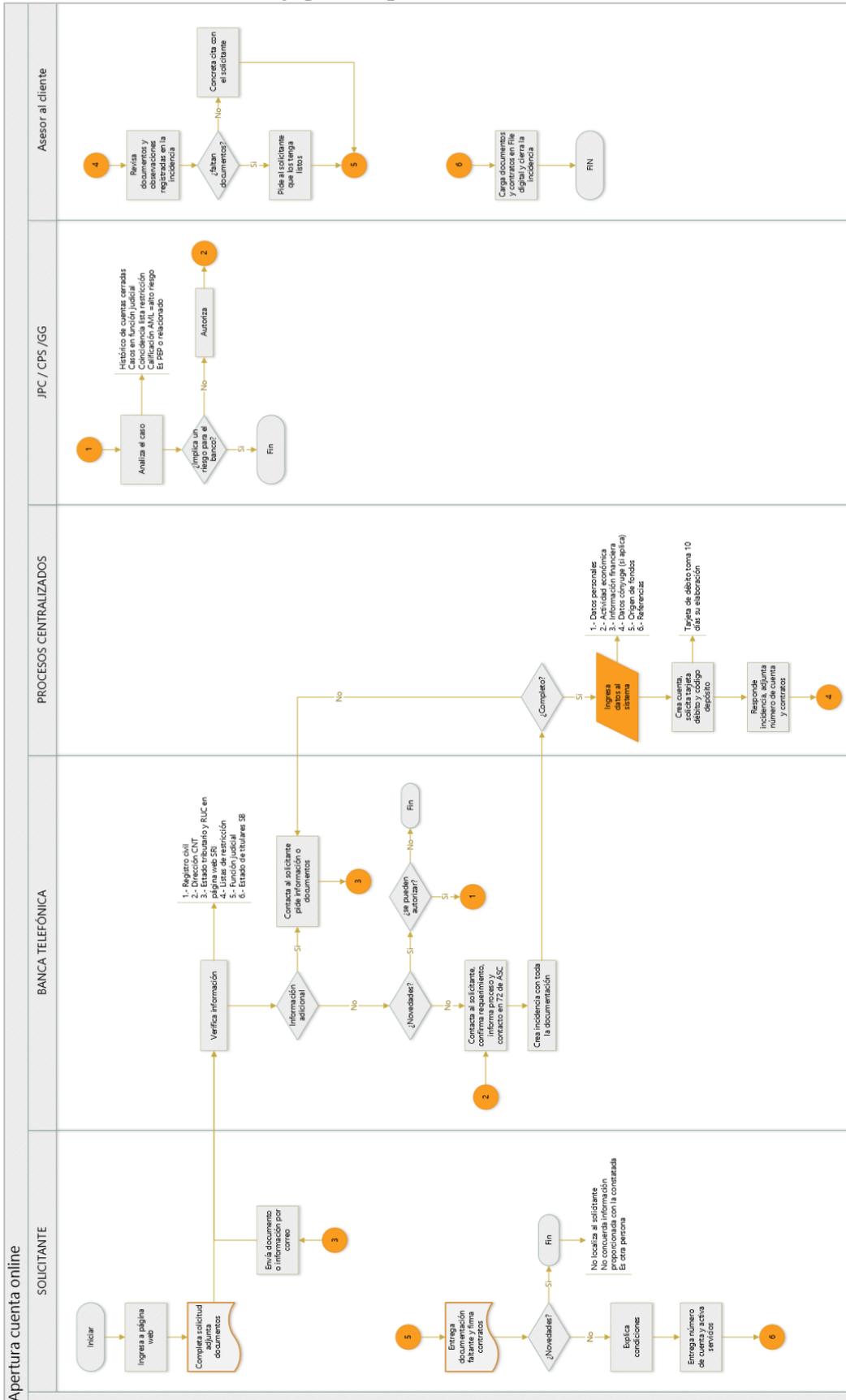
centralizados. En cambio, si son casos como por ejemplo: coincidencias en listas de sindicados por LA/FT, casos en la función judicial por narcotráfico y otros delitos precedentes, etc., el especialista de banca telefónica procederá a rechazar la solicitud.

Si procesos centralizados encuentra novedades en la verificación de datos o falta información/ documentación regresa la tarea al especialista de banca telefónica para su regularización, por el contrario, si son casos que el cliente ha indicado entregará información/ documentación al momento de firmar el contrato, el especialista de procesos centralizados notifica del particular al asesor al cliente para su regularización en la visita o cuando el solicitante se acerque a la agencia.

Cuando el Coordinador de Punto de Servicio, Jefe de Procesos Centralizados o Gerente General reciben la solicitud para su autorización deberán analizar el caso bajo un enfoque basado en riesgos, es decir si es un caso que no traerá consecuencias graves para la institución las autorizará, caso contrario el proceso termina.

Otra causa para terminar el proceso es cuando el asesor al cliente no localiza al solicitante en el lugar pactado para la visita, la información proporcionada no concuerda con la constatada y la persona no es quien dijo ser.

Ilustración 6
Flujograma apertura cuenta online



Fuente: La institución financiera
Elaboración propia

Se entrevistó a: especialista de banca telefónica, especialista de procesos centralizados, asesor al cliente sénior, especialista de cumplimiento, especialista de sistemas y especialista del área legal; siendo 22 los eventos de riesgo identificados en este proceso, los cuales enlistamos a continuación:

1. La carga de las listas de restricción no se efectúe correctamente.
2. Persona que conste en listas de restricción abre cuenta online
3. Empresa fachada o empresa de papel abre cuenta online
4. Persona que se dedica a actividades económicas con las cuales el banco ha decidido no trabajar abre cuenta online.
5. PEP abre una cuenta sin ser identificado.
6. Persona jurídica que no proporciona total o proporciona parcialmente información de sus beneficiarios finales abre cuenta online.
7. PEP que no proporciona información sobre su actividad económica y origen de fondos abre cuenta online.
8. Solicitante que proporciona información falsa abre cuenta online
9. No verificar la información en páginas oficiales como: función judicial y listas de restricción.
10. No verificar la información registrada por el solicitante con la referencia
11. Incorrecto registro de información en el sistema
12. No solicitar autorización del Jefe de Agencia para vincular a cliente con negocio de menos de un año de funcionamiento.
13. No solicitar autorización a Jefe de Agencia para vincular a cliente con ingresos mensuales superiores a los 100,000.00.
14. No solicitar autorización de la Gerencia por ser un cliente de alto riesgo
15. No solicitar autorización de la Gerencia para vincular a un cliente PEP.
16. Abrir la cuenta pese a que no se cuenta con la información requerida
17. Una vez abierta la cuenta el cliente cambia de domicilio a una jurisdicción lejana lo cual dificulta su seguimiento.
18. Entrega de tarjeta de débito y número de cuenta sin que el solicitante haya firmado el contrato.
19. No identificar que la cuenta no es para el cliente, sino para ser usada por un tercero.
20. No validar que el solicitante sea quien dijo ser
21. Solicitante no se acerca a regularizar la apertura de cuenta.

22. Asesor al cliente no guarda los documentos en el file digital del cliente.

Se elaboró una tabla descriptiva que se encuentra en el Anexo 1 del presente trabajo, para cada uno de los eventos de riesgo antes señalados y considerando los elementos que detallamos a continuación:

1. Factor de riesgo: cliente, empleado, canales de distribución, productos/servicios, jurisdicción.
2. Actividad: recopilación y validación de información, registro del cliente, inicio relación comercial.
3. Riesgos asociados: legal, reputacional, operativo y de contagio.
4. Responsable del proceso
5. Causas y consecuencias

2.2. Uso de ATM

El proceso inicia con la decisión que el cliente debe tomar en la zona 24/7 respecto al tipo de transacción a realizar, esta puede ser: depositar o retirar dinero, consultar su saldo o cambiar su clave. La zona 24/7 de la institución financiera ofrece tres tipos de ATM cuyo proceso de uso se detalla a continuación:

- **ATM para depósitos por montos menores a 5,000.00USD:** Para efectuar un depósito en este ATM, existen dos opciones: la primera a través de tarjeta de débito y la segunda a través de un código de depósito. En el caso de que el cliente cuente con su tarjeta de débito, debe ingresar ésta en la ranura destinada para ello en el ATM, digitar la clave o PIN y seleccionar si el depósito será en efectivo o cheque.

Si el depósito es en efectivo, el cliente debe: seleccionar la cuenta a depositar que puede ser cuenta propia o de otro cliente de la institución, ingresar los billetes por la ranura con la parte frontal hacia arriba (50 billetes - ATM full, 200 billetes - ATM reciclador), confirmar si el monto calculado por el ATM es correcto, caso contrario deberá ingresar nuevamente el dinero, confirmar si es correcto el monto, retirar su tarjeta y recibir el comprobante de depósito. Por el contrario, si el depósito es en cheque debe ingresar el documento con la parte frontal hacia arriba, verificar que la imagen presentada por el ATM sea adecuada, caso contrario deberá ingresar nuevamente el cheque, confirmar si la imagen del cheque es correcta, ingresar el monto del cheque

señalando miles y decimales, confirma el monto, selecciona la cuenta en la cual desea depositar que puede ser cuenta propia o de otro cliente del banco, retira su tarjeta y el recibo del depósito efectuado.

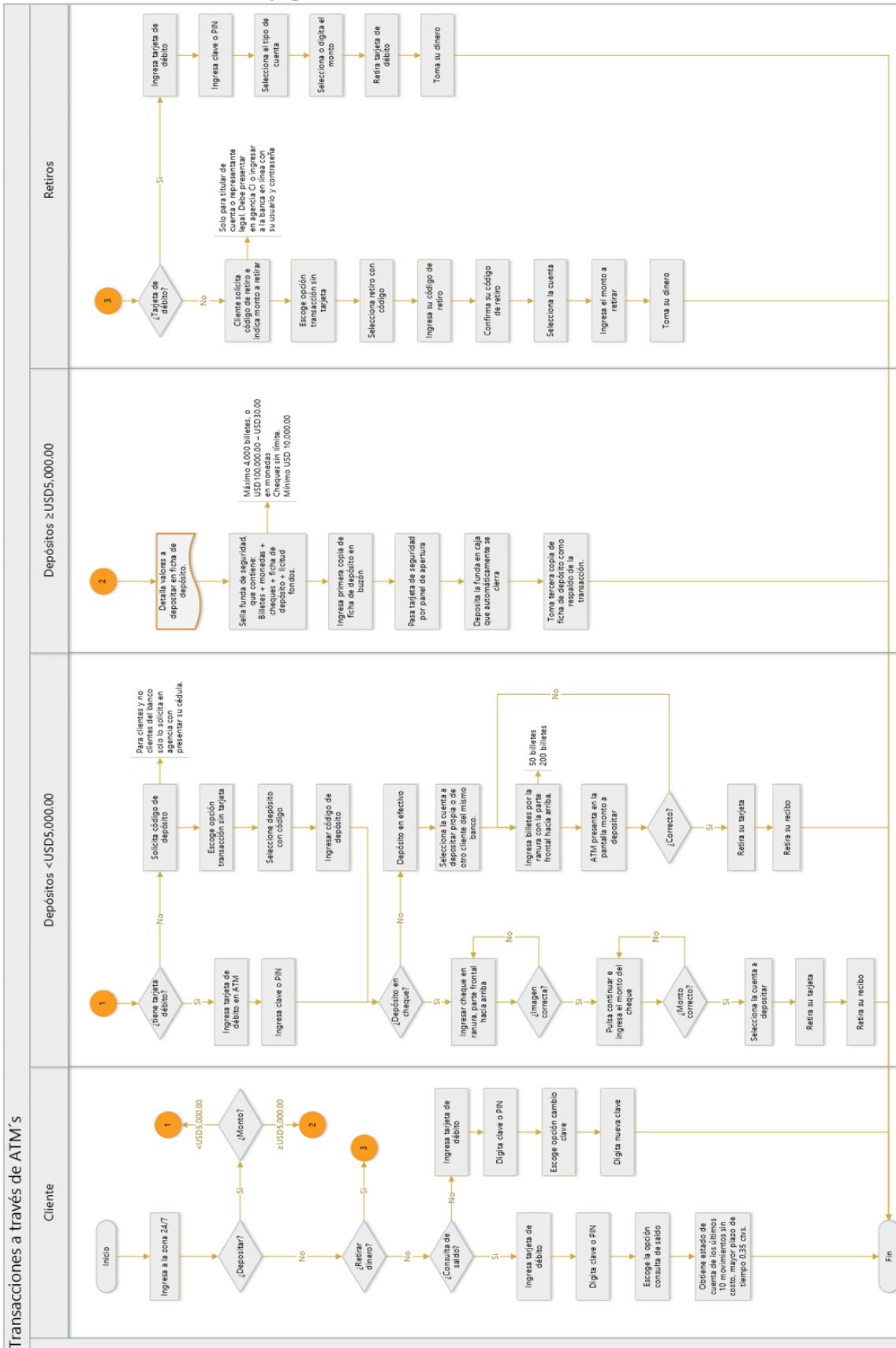
La diferencia de las transacciones antes detalladas, al ser efectuadas con un código de depósito radica que al inicio el cliente debe escoger en el ATM la opción transacción sin tarjeta, seleccionar depósito con código, ingresar el código de depósito y efectuar la transacción, tal y como se ha indicado previamente tanto para efectivo como cheque.

- **ATM para depósitos por montos iguales o mayores a 5,000.00USD:** Este es un servicio preferencial de la institución, para acceder a este, previamente la actividad y transaccionalidad del cliente tienen que ser analizadas por el asesor al cliente y expuesta al Gerente General, quien autoriza su uso. Con la autorización la institución entrega al cliente una tarjeta de seguridad, funda de seguridad, fichas de depósito y formularios de licitud de fondos numerados.

El proceso inicia cuando el cliente llena la ficha de depósito, continúa con la colocación de la segunda copia de ésta más la licitud de fondos, los billetes, monedas y cheques en la funda de seguridad y la sella; se acerca al ATM ingresa la primera copia de la ficha de depósito en el buzón junto a la caja, pasa la tarjeta de seguridad por la ranura que permite abrir la caja, deposita la funda de seguridad e inmediatamente la caja se cierra. La tercera copia de la ficha de depósito es el respaldo de la transacción efectuada.

- **ATM para retiro de efectivo:** Los retiros de efectivo, al igual que los depósitos se pueden efectuar a través de la tarjeta de débito o código de retiro. Si la transacción se realiza con tarjeta de débito el cliente debe ingresar ésta en la ranura destinada para ello en el ATM, digitar la clave o PIN, seleccionar el tipo de cuenta de la cual se realizará el retiro, seleccionar o digitar el monto, retirar la tarjeta de débito y tomar su dinero. En el caso de usar código de retiro, el cliente escoge la opción transacción sin tarjeta, selecciona la opción retiro con código, ingresa su código de retiro, confirma nuevamente su código, selecciona la cuenta, ingresa el monto a retirar y toma su dinero. Este código tiene una duración de 24 horas y se puede utilizar solo para efectuar el retiro por el monto indicado al momento de su solicitud, en un día se pueden solicitar hasta 10 códigos de retiro de hasta 800USD.

Ilustración 7 Flujograma transacciones a través de ATM



Fuente: La institución financiera
Elaboración propia

Se entrevistó a: especialista de procesos centralizados, especialista de canales electrónicos, asesor al cliente sénior, administrador de ATM, especialista de cumplimiento y especialista del área legal; siendo 28 los eventos de riesgo identificados en este proceso, los cuales enlistamos a continuación:

1. Cliente deposita cheques que no cumplen con los requisitos de forma.
2. Cliente no adjunta formulario de licitud de fondos.
3. Cliente no llena correctamente el formulario de licitud de fondos.
4. Cliente no regulariza formulario de licitud de fondos antes del segundo depósito.
5. No se acredita segundo depósito hasta que el cliente entregue licitud de fondos del primer depósito.
6. Cliente deposita billetes falsos.
7. Cliente no llena adecuadamente ficha de depósito.
8. Cliente digita monto a depositar en cheque distinto al realmente depositado.
9. Cliente frecuentemente registra faltantes o sobrantes en sus depósitos.
10. Contratos para depositar a través de ATM montos $\geq 5,000.00$ USD sin firma del cliente.
11. Acreditar monto señalado por el cliente sin comprobarlo, pues el administrador de ATM no alcanza a terminar el conteo en los cortes establecidos.
12. Administrador de ATM omite reportar sobrantes o faltantes.
13. Administrador de ATM no firma la ficha de depósito como aceptación de los valores contados.
14. Formulario físico de licitud de fondos no se encuentra en la carpeta de la agencia.
15. No se escanea el formulario de licitud de fondos.
16. Especialista de procesos centralizados omite notificar sobrantes al cliente.
17. Entregar material para depósito en ATM montos $\geq 5,000.00$ USD sin firma de acta entrega recepción.
18. No eliminar la exoneración anual del sistema cuando ya cumplió el año de vigencia.
19. Depósito en Ecuador e inmediato retiro de fondos en el exterior a través de tarjeta de débito.

20. No disponer con la documentación de respaldo e información de las transacciones efectuadas por el cliente, cuando el organismo de control lo solicite.
21. Cliente con frecuente reporte de pérdidas, sustracción o deterioro de tarjeta de seguridad y material para depósito.
22. Cliente con petición frecuente de material extra.
23. Cliente con varias tarjetas de débito activas.
24. Cliente con varios códigos de depósito activos.
25. NO clientes con más de un código de depósito activo.
26. Clientes con más de un código de depósito y una tarjeta activos.
27. Manejo de un mismo código de depósito por diferentes personas.
28. Cliente solicita varios códigos de retiro en varias agencias.

Se elaboró una tabla descriptiva que se encuentra en el Anexo 2 del presente trabajo, para cada uno de los eventos de riesgo antes señalados y considerando los elementos que detallamos a continuación:

1. Factor de riesgo: cliente, empleado, canales de distribución, productos/servicios, jurisdicción.
2. Actividad: Ejecución de depósito, revisión de transacciones, uso de material de depósito.
3. Riesgos asociados: legal, reputacional, operativo y de contagio.
4. Responsable del proceso
5. Causas y consecuencias

3. Medición del riesgo de LA/FT

Para la valoración de los riesgos de LA/FT se realizó una medición semicuantitativa, en la cual se valora la probabilidad de ocurrencia y el impacto de cada riesgo de acuerdo con una escala descriptiva.

El horizonte de tiempo para establecer la probabilidad de ocurrencia de los eventos de riesgo de LA/FT identificados será de un año, pues tanto la apertura de cuentas online como para las transacciones que se analizarán y que la institución financiera ofrece a través de ATM tuvieron mayor notoriedad en el 2018.

Una vez que se ha identificado el número de eventos ocurridos para cada riesgo, estos han sido divididos para los eventos posibles. Con estos resultados, se aplicó un

intervalo de clase que nos ha permitido clasificar estas probabilidades en una escala del 1 al 5 donde 1 es un evento de riesgo de LA/FT improbable, 2 es raro, 3 es posible, 4 probable y 5 casi seguro que suceda. Es decir, se ha organizado las probabilidades obtenidas en cada evento de riesgo de menor a mayor, el resultado de restar el dato menor del dato mayor lo dividimos para 5, que es la escala a utilizar en el presente trabajo y obtenemos los rangos que se muestran a continuación:

Tabla 7
Escala para probabilidades apertura cuentas online

Nivel de riesgo	Ponderación	Descripción	Probabilidad matemática
Casi seguro	5	Evento de riesgo LA/FT cuya materialización es casi seguro	De 18.72% en adelante
Probable	4	Evento de riesgo LA/FT cuya materialización es probable	Entre 2.38% y <18.72%
Posible	3	Evento de riesgo LA/FT cuya materialización es posible	Entre 0.45% y <2.38%
Raro	2	Evento de riesgo LA/FT cuya materialización es rara	Entre 0.09% y <0.45%
Improbable	1	Evento de riesgo LA/FT cuya materialización es improbable	Entre 0% y <0.09%

Fuente: Datos de la institución financiera
Elaboración propia

Tabla 8
Escala para probabilidades transacciones a través de ATM

Nivel de riesgo	Ponderación	Descripción	Probabilidad matemática
Casi seguro	5	Evento de riesgo LA/FT cuya materialización es casi seguro	De 12.50% en adelante
Probable	4	Evento de riesgo LA/FT cuya materialización es probable	Entre 5% y <12.50%
Posible	3	Evento de riesgo LA/FT cuya materialización es posible	Entre 2.76% y <5%
Raro	2	Evento de riesgo LA/FT cuya materialización es rara	Entre 0.05% y <2.76%
Improbable	1	Evento de riesgo LA/FT cuya materialización es improbable	Entre 0% y <0.05%

Fuente: Datos de la institución financiera
Elaboración propia

A continuación para una mayor comprensión, ejemplificamos el cálculo de la probabilidad de ocurrencia de un evento de riesgo de LA/FT: en la institución financiera la carga de las listas de restricción, que se realiza semanalmente no se efectuó

correctamente 15 veces en un año, dato que dividido para el número de resultados posibles (52 semanas en un año) nos demuestra que hay una probabilidad de 28.77% de que este evento de riesgo de LA/FT ocurra, acorde con la escala antes detallada significa que el evento de riesgo de LA/FT es casi seguro que suceda, por lo tanto, la ponderación asignada será de 5.

Ilustración 8
Ejemplo de cálculo de probabilidad

Actividad	Eventos	Resultado favorable	Resultado posible	%	Nivel de riesgo
Recopilación y validación de información	La carga de las listas de restricción no se efectúe correctamente	15	52	28.77%	5

Fuente: Datos de la institución financiera
Elaboración propia

El cálculo del impacto por riesgo asociado, lo hemos realizado tomando en consideración la sugerencia de ponderar la relevancia o importancia de cada riesgo asociado, del libro Sistema de Prevención de Lavado de Activos y de Financiación del Terrorismo. En ese sentido, debido a que el riesgo que generaría un mayor impacto en la institución sería el legal, le hemos asignado una ponderación del 40%, seguida por el riesgo reputacional con una ponderación del 30%, el riesgo operacional con 20% y al riesgo de contagio un 10% (Sintura, Martínez y Quintana 2011, 306).

Tabla 9
Escala de medición de impacto por riesgos asociados

Nivel de riesgo	Ponderación	Riesgo legal	Riesgo reputacional	Riesgo operacional	Riesgo de contagio	Riesgo de LA/FT
		40%	30%	20%	10%	100%
Catastrófico	5	Infracciones muy graves, multa de hasta 0.01% de los activos de la entidad infractora, remoción de los administradores y/o revocatoria de su licencia.	Pérdida de confianza por parte del público, intervención de entidades competentes.	Insuficiencia en procesos, recursos, infraestructura o tecnología para PLA/FT con impacto mayor al 0,003% del total de activos	Efectos legales y reputacionales de accionistas de la entidad o grupo económico involucrado en alguna actividad de LA/FT.	Pérdida o daño catastrófico, susceptible de cuantiosas amonestaciones económicas y estrictas sanciones de suspensión, inhabilitación o remoción de administradores, oficial de cumplimiento y otros funcionarios, cancelación de operaciones, suspensión de actividades, intervención de la organización. Pérdida de clientes, disminución de ingresos por desprestigio que puede colocar en peligro la solvencia de la entidad. Puede implicar el involucramiento de accionistas en actividades de LA/FT.
Crítico	4	Infracciones graves, multas de hasta 0,005% de los activos de la entidad infractora, la suspensión de los administradores hasta por noventa días y/o amonestación.	Divulgación de eventos y/o investigación por organismo regulador dado a conocer al público en medios informativos masivos y/o principales noticieros nacionales.	Insuficiencia en procesos, recursos, infraestructura o tecnología para PLA/FT con impacto hasta el 0,002% del total de activos	Efectos legales y reputacionales de un directivo (presidente, vicepresidente, miembros de la junta directiva, y oficial de cumplimiento) involucrado en alguna actividad de LA/FT.	Pérdida o daño crítico. Susceptible de una amonestación de índole económica a la mayor cuantía posible. Pérdida de clientes, disminución de los ingresos por mala imagen o publicidad. Puede implicar el involucramiento de directivos en actividades de LA/FT
Moderado	3	Infracciones leves, multas de hasta 0,001% de los activos de la entidad infractora.	Crítica de organismos de control o clientes en medios masivos de comunicación.	Insuficiencia en procesos, recursos, infraestructura o tecnología para PLA/FT con impacto hasta el 0,001% del total de activos	Efectos legales y reputacionales de un funcionario involucrado en alguna actividad de LA/FT	Pérdida o daño moderado. Susceptible de una amonestación de índole económico. Puede haber pérdida de clientes, disminución de ingresos por desprestigio, mala imagen o publicidad negativa. El riesgo de contagio se presenta por los funcionarios.
Leve	2	Multas de hasta 0,0001% de los activos de la entidad infractora.	Aviso sorpresivo de prensa u otro medio masivo	Insuficiencia en procesos, recursos, infraestructura o tecnología para PLA/FT con impacto hasta el 0,0006% del total de activos	Efectos legales y reputacionales de un cliente involucrado en alguna actividad de LA/FT.	Leve pérdida o daño. Puede ser susceptible de sanción moderada de índole económico. No genera pérdida de clientes, ni genera pérdida de ingresos o incremento de gastos por pérdida de reputación. Puede implicar el involucramiento de clientes en actividades de LA/FT
Insignificante	1	Advertencias que no implican sanciones monetarias.	Situaciones que no trascienden a los medios informativos.	Insuficiencia en procesos, recursos, infraestructura o tecnología para PLA/FT que no producen afectación.	Efectos legales y reputacionales de un proveedor involucrado en alguna actividad de LA/FT.	Sin perjuicios, baja pérdida financiera o daño reputacional.

Fuente: Sintura, Martínez y Quintana 2011, 307; EC 2014, art.264; datos de la institución.
Elaboración propia

Una vez que, cada evento de riesgos de LA/FT haya recibido una calificación por cada tipo de riesgo asociado, la consolidación de estas cuatro calificaciones se efectuará mediante la técnica del promedio ponderado, como se observa en el siguiente ejemplo:

Si la carga de las listas de restricción no se efectúa correctamente y la institución financiera no cuenta con una alerta que le permita identificar tal error, implica que la misma podría vincular a personas que tengan antecedentes penales relacionados con LA/FT. Ante una posible auditoría del ente de control este particular traería consecuencias graves para la entidad, lo que representa un riesgo legal, reputacional, operativo y de contagio por ese motivo y con base a los porcentajes antes detallados el cálculo del impacto queda expresado de la siguiente manera:

$$\text{Riesgo legal} \rightarrow 5 * 40\% = 2.0$$

$$\text{Riesgo reputacional} \rightarrow 5 * 30\% = 1.5$$

$$\text{Riesgo operativo} \rightarrow 5 * 20\% = 1.0$$

$$\text{Riesgo de contagio} \rightarrow 3 * 10\% = 0.3$$

Ilustración 9

Ejemplo de cálculo del impacto

Actividad	Eventos	RL 40%	RR 30%	RO 20%	RC 10%	Impacto
Recopilación y validación de información	La carga de las listas de restricción no se efectúe correctamente	2.0	1.5	1.0	0.3	4.8

Fuente: Datos de la institución financiera

Elaboración propia

En ese sentido, el valor del impacto oscilará en una escala de 1 a 5 para que exista uniformidad con la escala de probabilidades.

De igual manera como se establecieron los rangos de probabilidad e impacto, para el riesgo inherente hemos organizado de menor a mayor los resultados de multiplicar la probabilidad por el impacto, luego dividimos para 5, que es la escala utilizada por la entidad y obtenemos los rangos que se detallan en la siguiente tabla:

Tabla 10

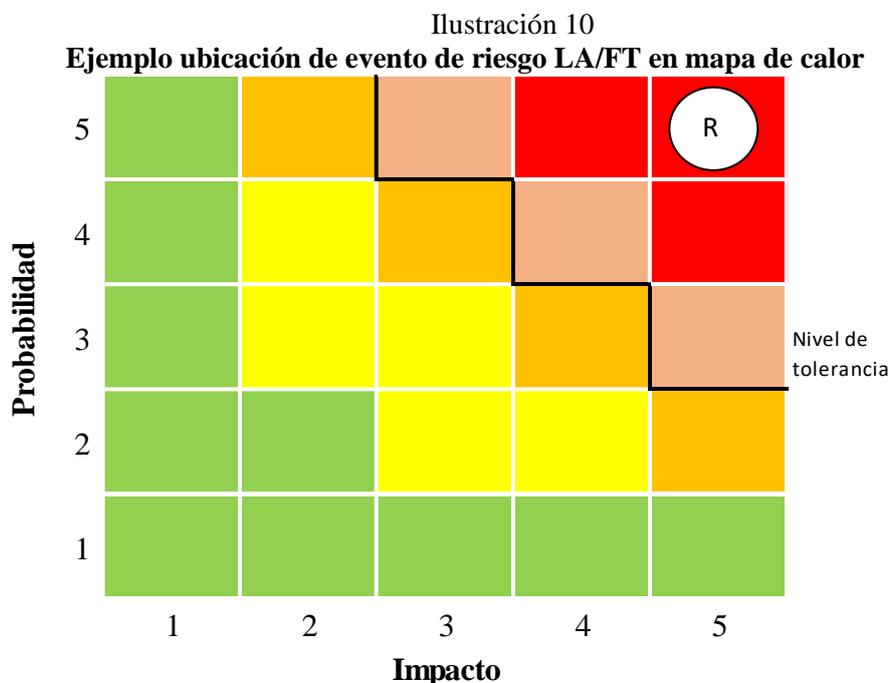
Escala de riesgo de LA/FT

Rangos riesgo (probabilidad * impacto)	Calificación del evento de riesgo de LA/FT	Escala de severidad
De 21 a 25	Evento de riesgo de LA/FT catastrófico	5
De 16 a 20	Evento de riesgo de LA/FT crítico	4
De 11 a 15	Evento de riesgo de LA/FT moderado	3
De 6 a 10	Evento de riesgo de LA/FT significativo	2
De 0 a 5	Evento de riesgo de LA/FT aceptable	1

Fuente: (Sintura, Martínez y Quintana 2011, 309); datos de la institución financiera

Elaboración propia

Por ejemplo, en el caso de la carga incorrecta de las listas de restricción existe una probabilidad de que este evento de riesgo de LA/FT ocurra de 5 y un impacto de 4.8 siendo el riesgo inherente 24, cuya equivalencia según la Tabla 10 es 5, valor que dentro del siguiente mapa se ubica sobre el nivel de tolerancia establecido por la entidad:



Fuente: Datos de la institución financiera
Elaboración propia

Con estos antecedentes se exponen a continuación los resultados obtenidos en la medición de riesgos, tanto en la apertura de cuentas online como en el uso de ATM en la institución financiera bajo análisis:

3.1. Apertura de cuentas online

Durante el año 2018 la institución financiera abrió 673 cuentas online y cerró el año con 39,900 clientes. Luego de efectuar el cálculo de la probabilidad e impacto, cuyo detalle se puede apreciar en el [Anexo 3](#) y [Anexo 5](#) respectivamente, a continuación presentamos el cálculo del riesgo inherente:

Tabla 11
Cálculo del riesgo inherente apertura de cuentas online

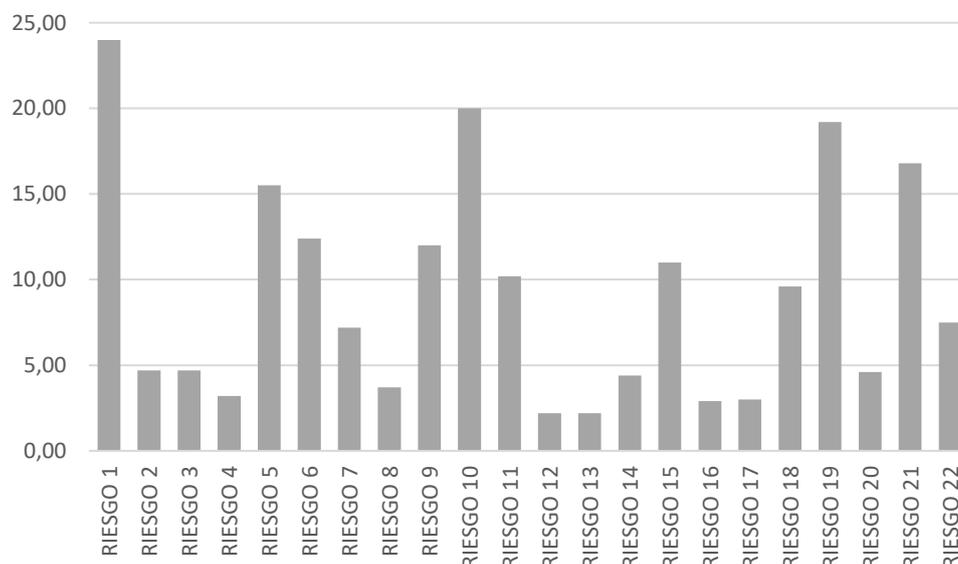
Código de Riesgo	Actividad	Descripción del Riesgo	Factor de Riesgo	Riesgo Inherente			
				Probabilidad	Impacto	Nivel de Riesgo Inherente	
RIESGO 1	Recopilación y validación de información	La carga de las listas no es correcta	Empleado	5	4.8	24.0	CATASTRÓFICO
RIESGO 2	Recopilación y validación de información	Persona que consta en listas de restricción abre cuenta online	Ciente	1	4.7	4.7	ACEPTABLE
RIESGO 3	Recopilación y validación de información	Empresa fachada o empresa de papel abre cuenta online	Ciente	1	4.7	4.7	ACEPTABLE
RIESGO 4	Recopilación y validación de información	Persona que se dedica a actividades con las cuales el banco no trabaja abre cuenta online	Ciente	2	1.6	3.2	ACEPTABLE
RIESGO 5	Recopilación y validación de información	PEP abre cuenta sin ser identificado	Ciente	5	3.1	15.5	CRÍTICO
RIESGO 6	Recopilación y validación de información	Persona jurídica que no proporciona total o parcialmente información de sus beneficiarios finales abre cuenta online	Ciente	4	3.1	12.4	MODERADO
RIESGO 7	Recopilación y validación de información	PEP que no proporciona mayor información sobre sus actividades y origen de fondos abre cuenta online	Ciente	3	2.4	7.2	SIGNIFICATIVO
RIESGO 8	Recopilación y validación de información	Solicitante que proporciona información falsa abre cuenta on line	Ciente	1	3.7	3.7	ACEPTABLE
RIESGO 9	Recopilación y validación de información	No verificar la información en páginas oficiales, función judicial y listas de restricción	Empleado	3	4.0	12.0	MODERADO
RIESGO 10	Recopilación y validación de información	No verificar la información registrada por el solicitante con la referencia	Empleado	5	4.0	20.0	CRÍTICO
RIESGO 11	Registro del cliente	Incorrecto registro de información en el sistema	Empleado	3	3.4	10.2	MODERADO
RIESGO 12	Registro del cliente	No solicitar autorización Jefe de Agencia para cliente con negocio de menos de un año de funcionamiento	Empleado	1	2.2	2.2	ACEPTABLE
RIESGO 13	Registro del cliente	No solicitar autorización Jefe de Agencia para cliente con ingresos mensuales superiores a los 100,000.00	Empleado	1	2.2	2.2	ACEPTABLE
RIESGO 14	Registro del cliente	No solicitar autorización de la Gerencia por ser un cliente de alto riesgo	Empleado	2	2.2	4.4	ACEPTABLE
RIESGO 15	Registro del cliente	No solicitar autorización de la Gerencia para vincular a un cliente PEP	Empleado	5	2.2	11.0	MODERADO
RIESGO 16	Registro del cliente	Abrir la cuenta pese a que no se cuenta con la información requerida	Empleado	1	2.9	2.9	ACEPTABLE
RIESGO 17	Inicio relación comercial	Una vez abierta la cuenta el cliente cambia de domicilio a una jurisdicción lejana lo cual dificulta su verificación.	Jurisdicción	2	1.5	3.0	ACEPTABLE
RIESGO 18	Inicio relación comercial	Entregar tarjeta de débito y número de cuenta sin que el cliente haya firmado el contrato	Empleado	2	4.8	9.6	SIGNIFICATIVO
RIESGO 19	Inicio relación comercial	No identificar que la cuenta no es para el cliente, sino para ser usada por un tercero.	Empleado	4	4.8	19.2	CRÍTICO

Código de Riesgo	Actividad	Descripción del Riesgo	Factor de Riesgo	Riesgo Inherente			
				Probabilidad	Impacto	Nivel de Riesgo Inherente	
RIESGO 20	Inicio relación comercial	No validar que el solicitante sea quien dijo ser	Empleado	1	4.6	4.6	ACEPTABLE
RIESGO 21	Inicio relación comercial	Cliente no se acerca a regularizar la apertura	Cliente	4	4.2	16.8	CRÍTICO
RIESGO 22	Inicio relación comercial	Asesor al cliente no carga documentos en el file digital de cliente	Empleado	3	2.5	7.5	SIGNIFICATIVO

Fuente: La institución financiera
Elaboración propia

Gráficamente se presenta el nivel de riesgo inherente de la institución financiera:

Gráfico 1
Riesgo Inherente en la apertura de cuentas online



Fuente: La institución financiera
Elaboración propia

Que la carga de las listas de restricción no sea correcta es un evento de riesgo de LA/FT catastrófico que tendría la institución sin implementar controles en la apertura de cuentas online, así como, cuatro eventos de riesgo de LA/FT críticos (5, 10, 19, 21) a los cuales debería prestar especial atención. Por otra parte, de 22 eventos de riesgo de LA/FT 13 tienen como factor de riesgo al empleado, 8 al cliente y 1 jurisdicción. Es decir, la institución es más propensa de ser usada para el lavado de activos en la apertura de cuentas online por sus empleados que por sus clientes, principalmente se debe a omisiones por parte de los empleados de los procedimientos, políticas y procesos de PLA/FT y fallas en los sistemas. Finalmente, cuatro eventos de riesgo de LA/FT son moderados (6, 9, 11, 15) tres eventos de riesgo de LA/FT son significativos (7,18,22) y siete son aceptables (2, 3, 4, 8, 12, 13, 14, 16, 17, 20) sin la presencia de controles.

3.2. Uso de ATM

Durante el año 2018 la institución financiera cuenta con 40 clientes que usan ATM para depositar montos mayores o iguales a 5,000.00USD; de estos, 18 cuentan con la exoneración anual para no firmar el formulario de licitud de fondos, mientras que 21 clientes deben firmarlo. Luego de efectuar el cálculo de la probabilidad e impacto, cuyo detalle se puede apreciar en el Anexo 4 y Anexo 6 respectivamente, a continuación presentamos el cálculo del riesgo inherente:

Tabla 12
Cálculo del riesgo inherente uso de ATM

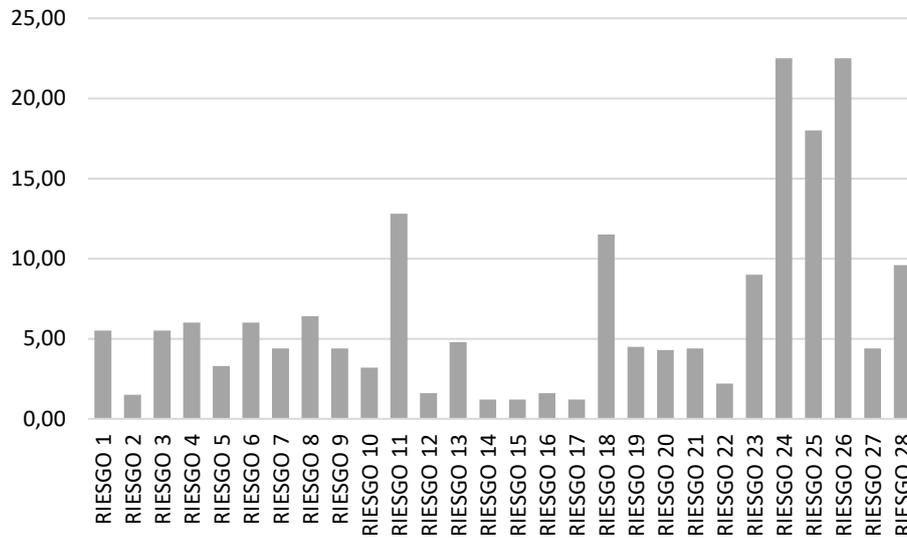
Código de Riesgo	Actividad	Descripción del Riesgo	Factor de Riesgo	Riesgo Inherente			
				Probabilidad	Impacto	Nivel de Riesgo Inherente	
RIESGO 1	Ejecución de depósito	Ciente deposita cheques que no cumplen con los requisitos de forma	Ciente	5	1	6	SIGNIFICATIVO
RIESGO 2	Ejecución de depósito	Ciente no adjunta formulario de licitud de fondos	Ciente	1	2	2	ACEPTABLE
RIESGO 3	Ejecución de depósito	Ciente no llena correctamente el formulario de licitud de fondos	Ciente	5	1	6	SIGNIFICATIVO
RIESGO 4	Ejecución de depósito	Ciente no regulariza formulario de licitud de fondos antes del segundo depósito	Ciente	4	2	6	SIGNIFICATIVO
RIESGO 5	Ejecución de depósito	No se acredita segundo depósito hasta que el cliente entregue licitud de fondos del primer depósito	Ciente	3	1	3	ACEPTABLE
RIESGO 6	Ejecución de depósito	Ciente deposita billetes falsos	Ciente	4	2	6	SIGNIFICATIVO
RIESGO 7	Ejecución de depósito	Ciente no llena adecuadamente ficha de depósito	Ciente	4	1	4	ACEPTABLE
RIESGO 8	Ejecución de depósito	Ciente digita monto a depositar en cheque distinto al realmente depositado	Canales de distribución	2	3	6	SIGNIFICATIVO
RIESGO 9	Revisión de transacciones	Ciente frecuentemente registra faltantes o sobrantes en sus depósitos	Canales de distribución	4	1	4	ACEPTABLE
RIESGO 10	Revisión de transacciones	Contratos para depositar a través de ATM montos \geq USD5,000.00 sin firma del cliente	Empleado	1	3	3	ACEPTABLE
RIESGO 11	Revisión de transacciones	Acreditar monto señalado por el cliente sin comprobarlo, pues Administrador de ATM no alcanza a terminar el conteo en los cortes establecidos	Canales de distribución	4	3	13	MODERADO
RIESGO 12	Revisión de transacciones	Administrador de ATM omite reportar sobrantes o faltantes	Empleado	1	2	2	ACEPTABLE

Código de Riesgo	Actividad	Descripción del Riesgo	Factor de Riesgo	Riesgo Inherente			
				Probabilidad	Impacto	Nivel de Riesgo Inherente	
RIESGO 13	Revisión de transacciones	Administrador de ATM no firma la ficha de depósito como aceptación de los valores contados	Empleado	4	1	5	ACEPTABLE
RIESGO 14	Revisión de transacciones	Formulario físico de licitud de fondos no se encuentra en la carpeta de la agencia	Empleado	1	1	1	ACEPTABLE
RIESGO 15	Revisión de transacciones	No se escanea el formulario de licitud de fondos	Empleado	1	1	1	ACEPTABLE
RIESGO 16	Revisión de transacciones	Especialista de procesos centralizados omite notificar sobranes al cliente	Empleado	1	2	2	ACEPTABLE
RIESGO 17	Revisión de transacciones	Entregar material para depósito en ATM montos \geq USD5,000.00 sin firma de acta entrega recepción	Empleado	1	1	1	ACEPTABLE
RIESGO 18	Revisión de transacciones	No eliminar la exoneración anual del sistema cuando ya cumplió el año de vigencia	Empleado	5	2	12	MODERADO
RIESGO 19	Revisión de transacciones	Depósito en Ecuador e inmediato retiro de fondos en el exterior a través de tarjeta de débito sin que sea identificado	Productos/ Servicios	1	5	5	ACEPTABLE
RIESGO 20	Revisión de transacciones	No disponer con la documentación de respaldo e información de las transacciones efectuadas por el cliente, cuando el organismo de control lo solicite	Cliente	1	4	4	ACEPTABLE
RIESGO 21	Uso de material de depósito	Cliente con frecuente reporte de pérdidas, sustracción o deterioro de tarjeta de seguridad y material para depósito	Cliente	4	1	4	ACEPTABLE
RIESGO 22	Uso de material de depósito	Cliente con petición frecuente de material extra	Cliente	2	1	2	ACEPTABLE
RIESGO 23	Uso de material de depósito	Cliente con varias tarjetas de débito activas.	Empleado	2	5	9	SIGNIFICATIVO
RIESGO 24	Uso de material de depósito	Cliente con varios códigos de depósito activos.	Empleado	5	5	23	CATASTRÓFICO
RIESGO 25	Uso de material de depósito	NO clientes con más de un código de depósito activo	Empleado	4	5	18	CRÍTICO
RIESGO 26	Uso de material de depósito	Cientes con más de un código de depósito y una tarjeta activos.	Empleado	5	5	23	CATASTRÓFICO
RIESGO 27	Uso de material de depósito	Manejo de un mismo código de depósito por diferentes personas	Productos/ Servicios	1	4	4	ACEPTABLE
RIESGO 28	Uso de material de depósito	Cliente solicita varios códigos de retiro en varias agencias	Cliente	3	3	10	SIGNIFICATIVO

Fuente: La institución financiera
Elaboración propia

Gráficamente se presenta el nivel de riesgo inherente de la institución financiera:

Gráfico 2
Riesgo Inherente uso de ATM



Fuente: La institución financiera
Elaboración propia

Dentro de este proceso, que los clientes tengan más de un código de depósito y una tarjeta de débito activos representan eventos de riesgo de LA/FT (24 y 26) que sin considerar controles son catastróficos para la institución. Esto se debe al desconocimiento de algunas funcionalidades del sistema y omisiones por parte de los empleados, así como, debilidades del proceso. Esta unidad estratégica presenta 16 eventos de riesgo aceptables (2,5,7,9,10,12,13,14,15,16,17,19,20,21,22,27) 7 eventos de riesgos de LA/FT significativos (1,3,4,6,8,23,28) y 2 eventos de riesgo de LA/FT moderados (11,18).

4. Evaluación de controles

Una vez determinado el nivel de riesgo inherente procederemos a calcular la exposición real de la institución al riesgo, para ello agregaremos en la matriz “los controles”, pues estos fueron diseñados por la institución para mitigar estos riesgos.

4.1. Apertura de cuentas online

A continuación enlistamos para cada uno de los 22 eventos de riesgo los controles con los cuales cuenta la institución financiera:

Tabla 13
Detalle de controles para la apertura de cuentas online

Nº evento de riesgo	Control existente
1	Cada lunes el especialista de cumplimiento, valida una muestra de personas que constan en la lista de restricción para verificar que el sistema los busque.
2	Los viernes el sistema a las 4pm valida que estén los archivos de las listas de restricción y envía un correo informativo a TI y Unidad de Cumplimiento. Antes de otorgar el producto/servicio el sistema muestra un mensaje si el cliente está en listas de restricción.
3	Cargar el listado de empresas fachada al sistema. Capacitaciones anuales para personal permanente y al momento de su ingreso para personal nuevo sobre la importancia de la aplicación de procesos y política de PLA/FT.
4, 6, 7, 19	El asesor al cliente antes de ir a su cargo tiene 3 meses de capacitación tiempo en el cual también debe leer los manuales.
5	El sistema al cierre del scoring valida a los clientes contra las listas PEP. A fin de mes el especialista de cumplimiento solicita un listado de clientes vinculados en ese mes y valida que si son PEP estén marcados como tal en el sistema.
8	Especialista de procesos centralizados verifica que la información sea coherente con la documentación, que esté vigente y la compara con páginas oficiales SRI, CNT, SB etc.
9	Especialista de procesos centralizados da dos días para regularizar observaciones, caso contrario rechaza la incidencia.
10, 11, 14, 16, 17, 18	No existe control
12, 13	No pasan la revisión de UBOS que efectúa el especialista de cumplimiento.
15	A fin de mes el especialista de cumplimiento solicita un listado de clientes vinculados en ese mes y valida que si son PEP estén marcados como tal en el sistema.
20	Todos los solicitantes deben acercarse a la agencia o ser visitados por el asesor.
21	Cada mes se envía a cerrar estas cuentas.
22	Especialista de banca telefónica continuamente está dando seguimiento a la carga de contratos. Asesor senior realiza arqueo de cuentas y valida que estén cargados todos los documentos para considerarlo como completo y cerrar la incidencia.

Fuente: La institución financiera
 Elaboración propia

Una vez identificados los controles se debe valorar la eficiencia de los mismos, para ejemplificar lo detallado en el capítulo segundo y explicar lo que se muestra en la Tabla 14, nos basamos en el evento de riesgo de LA/FT número uno, que hace referencia a la carga incorrecta de las listas de restricción. La institución financiera ha establecido como control, que cada lunes el especialista de cumplimiento valide una muestra de personas que constan en la lista de restricción para verificar que el sistema los busque. En ese sentido, la naturaleza del control es detectivo, manual y periódico, que acorde a la Tabla 4 significa que es un control regular cuya puntuación asignada es 2. El control implementado por la institución financiera ayuda a reducir la probabilidad de que este evento de riesgo de LA/FT se presente, sin embargo, el impacto de que la institución financiera sea objeto de una sanción y su reputación se vea afectada no disminuye. En ese sentido, el riesgo residual se ha obtenido de dividir la probabilidad inherente sobre la efectividad de los controles, resultado que se ha considerado como la probabilidad residual de 2.5, el cual multiplicado por el impacto residual de 4.8 permite obtener el riesgo residual de 12 que de acuerdo con la escala de la Tabla 10 representa un nivel de riesgo moderado cuyo equivalente es 3.

Con estos antecedentes a continuación se muestran los resultados obtenidos para cada uno de los eventos de riesgo de LA/FT identificados:

Tabla 14
Cálculo del riesgo residual

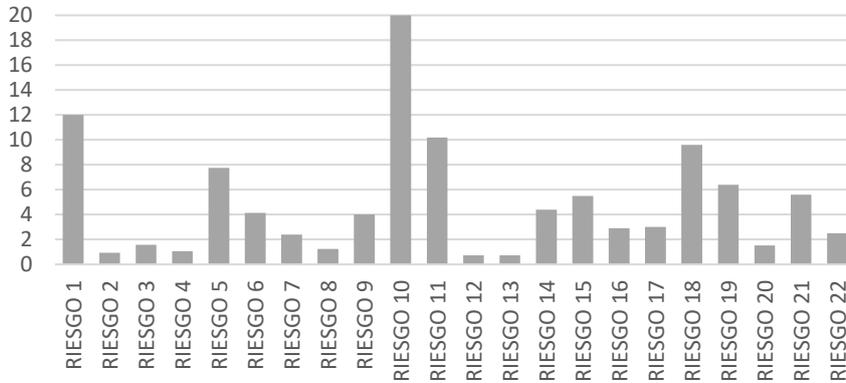
Código de Riesgo	Controles existentes	Análisis de controles			Efectividad	Riesgo residual			
		Naturaleza de control	Automatización	Frecuencia		Probabilidad	Impacto	Nivel de Riesgo Residual	
RIESGO 1	Cada lunes el especialista de cumplimiento valida una muestra de personas que constan en la lista de restricción para verificar que el sistema los busque.	Detectivo	Manual	Periodico	2	2.50	4.80	12.00	MODERADO
RIESGO 2	1.- Los viernes el sistema a las 4pm valida que estén los archivos de las listas de restricción y envía un correo informativo a TI y Unidad de Cumplimiento. 2.- Antes de otorgar el producto/servicio el sistema muestra un mensaje si el cliente está en listas de restricción	Preventivo	Automático	Permanente	5	0.20	4.70	0.94	ACEPTABLE
RIESGO 3	1.- Cargar el listado de empresas fichada al sistema 2.- Capacitaciones anuales para personal permanente y al momento de su ingreso para personal nuevo sobre la importancia de la aplicación de procesos y política de PLA/FT.	Preventivo	Manual	Periodico	3	0.33	4.70	1.57	ACEPTABLE
RIESGO 4	El asesor al cliente antes de ir a su cargo tiene 3 meses de capacitación tiempo en el cual también debe leer los manuales.	Preventivo	Manual	Periodico	3	0.67	1.60	1.07	ACEPTABLE

Código de Riesgo	Controles existentes	Análisis de controles			Efectividad	Riesgo residual			
		Naturaleza de control	Automatización	Frecuencia		Probabilidad	Impacto	Nivel de Riesgo Residual	
RIESGO 5	1.-El sistema al cierre del scoring valida a los clientes contra las listas de PEP's 2.-A fin de mes el especialista de cumplimiento solicita un listado de clientes vinculados en ese mes y valida que si son PEP's estén marcados como tal en el sistema.	Detectivo	Semiautomático	Permanente	2	2.50	3.10	7.75	SIGNIFICATIVO
RIESGO 6	No pasan la revisión de UBOS que efectúa el especialista de cumplimiento.	Correctivo	Manual	Permanente	3	1.33	3.10	4.13	ACEPTABLE
RIESGO 7	El asesor al cliente antes de ir a su cargo tiene 3 meses de capacitación tiempo en el cual también debe leer los manuales.	Preventivo	Manual	Periodico	3	1.00	2.40	2.40	ACEPTABLE
RIESGO 8	Especialista de procesos centralizados verifica que la información sea coherente con la documentación, que esté vigente y la compara con páginas oficiales SRI, CNT, SB etc.	Correctivo	Manual	Permanente	3	0.33	3.70	1.23	ACEPTABLE
RIESGO 9	Especialista de procesos centralizados da dos días para regularizar observaciones, caso contrario rechaza la incidencia	Correctivo	Manual	Permanente	3	1.00	4.00	4.00	ACEPTABLE
RIESGO 10	No hay	No determinado	No determinado	No determinado	0	5.00	4.00	20.00	CRÍTICO
RIESGO 11	No hay	No determinado	No determinado	No determinado	0	3.00	3.40	10.20	MODERADO
RIESGO 12	No pasan la revisión de UBOS que efectúa el especialista de cumplimiento.	Correctivo	Manual	Permanente	3	0.33	2.20	0.73	ACEPTABLE
RIESGO 13	No pasan la revisión de UBOS que efectúa el especialista de cumplimiento.	Correctivo	Manual	Permanente	3	0.33	2.20	0.73	ACEPTABLE
RIESGO 14	No hay	No determinado	No determinado	No determinado	0	2.00	2.20	4.40	ACEPTABLE
RIESGO 15	A fin de mes el especialista de cumplimiento solicita un listado de clientes vinculados en ese mes y valida que si son PEP's estén marcados como tal en el sistema.	Detectivo	Manual	Periodico	2	2.50	2.20	5.50	SIGNIFICATIVO
RIESGO 16	No hay	No determinado	No determinado	No determinado	0	1.00	2.90	2.90	ACEPTABLE
RIESGO 17	No hay	No determinado	No determinado	No determinado	0	2.00	1.50	3.00	ACEPTABLE
RIESGO 18	No hay	No determinado	No determinado	No determinado	0	2.00	4.80	9.60	SIGNIFICATIVO
RIESGO 19	El asesor al cliente antes de ir a su cargo tiene 3 meses de capacitación tiempo en el cual también debe leer los manuales.	Preventivo	Manual	Periodico	3	1.33	4.80	6.40	SIGNIFICATIVO
RIESGO 20	Todos los solicitantes deben acercarse a la agencia o ser visitados por el asesor	Correctivo	Manual	Permanente	3	0.33	4.60	1.53	ACEPTABLE
RIESGO 21	Cada mes se envía a cerrar estas cuentas	Correctivo	Manual	Periodico	3	1.33	4.20	5.60	SIGNIFICATIVO
RIESGO 22	1.-Especialista de banca telefónica continuamente está dando seguimiento a la carga de contratos 2.- Asesor senior realiza arqueo de cuentas y valida que estén cargados todos los documentos para considerarlo como completo y cerrar la incidencia	Correctivo	Manual	Periodico	3	1.00	2.50	2.50	ACEPTABLE

Fuente: La institución financiera
Elaboración propia

Gráficamente se presenta el nivel de riesgo residual de la institución financiera en la apertura de cuentas online:

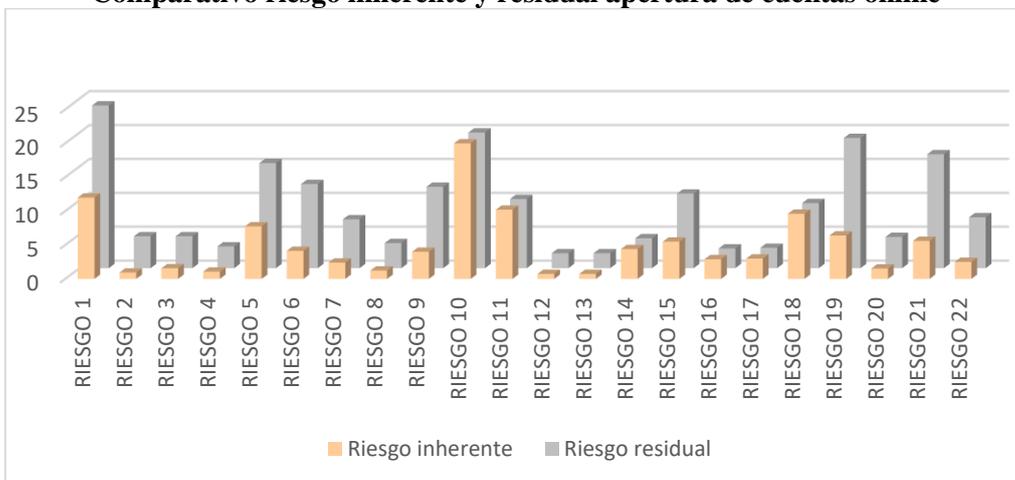
Gráfico 3
Riesgo residual en la apertura de cuentas online



Fuente: Datos de la institución financiera
Elaboración propia

Luego de la aplicación de controles se puede observar que éstos han tenido un efecto positivo sobre la severidad de los eventos de riesgo de LA/FT 1, 5, 6, 7, 9, 15, 19, 21 y 22, porque el valor de estos para el riesgo residual es menor que el riesgo inherente, lo que significa que el control es eficiente. Los eventos de riesgo de LA/FT 14, 16, 17 y 18 que no tienen controles definidos si bien reflejan un riesgo significativo y aceptable para la entidad, representan deficiencias que también deben ser revisadas. Los riesgos 10 y 11, los cuales se mantiene como crítico y moderado por no tener controles deben ser analizados por la entidad, de tal manera que se establezcan controles oportunos y adecuados.

Gráfico 4
Comparativo riesgo inherente y residual apertura de cuentas online



Fuente: Datos de la institución financiera
Elaboración propia

4.2. Uso de ATM

A continuación enlistamos para cada uno de los 28 eventos de riesgo los controles con los cuales cuenta la institución financiera:

Tabla 15
Detalle de controles para uso de ATM

Nº evento de riesgo	Control existente
1	El cheque no se deposita se devuelve al cliente.
2	Administrador de ATM al momento de efectuar el conteo del dinero, valida que esté el documento, si no está lo reporta en el campo de observaciones para que el asesor al cliente lo regularice antes del segundo depósito.
3	Previo efectuar el segundo depósito el cliente debe regularizar la licitud de fondos.
4	No se procesa el depósito.
5	Si es un cliente que en reiteradas ocasiones no ha regularizado el formulario se cancela el servicio.
6	Administrador de ATM identifica billetes falsos antes de registrar el depósito.
7	No se procesa el depósito.
8	Especialista de procesos centralizados verifica el cheque y valor digitado, corrige el valor y procesa.
9	Es una causa para cancelar el contrato.
10	Especialista de procesos centralizados valida que todos los documentos estén regularizados previo activar la tarjeta de seguridad.
11	Una vez concluido el conteo de valores se compara con lo acreditado y de no ser correcto el valor se realizan los ajustes correspondientes.
12, 16, 18, 19, 20, 22, 23, 26, 27	No existe control
13	Especialista de procesos centralizados revisa la ficha y solicita la firma del responsable si no lo está.
14	Asesor senior revisa que los formularios estén en la carpeta.
15	Asesor senior revisa que los formularios estén escaneados.
17	Mientras no recibe el contrato, acta y todos los documentos habilitantes firmados por el cliente el EPC no habilita el servicio.
21	Se desactiva la tarjeta de seguridad cuando pide una nueva.
24, 25, 28	Asesor al cliente previo a otorgar otro código, valida si el solicitante ya tiene uno.

Fuente: La institución financiera
Elaboración propia

Una vez identificados los controles, se calcula la efectividad de los mismos, con este resultado obtenemos el riesgo residual para las transacciones efectuadas a través de ATM, cuyos resultados mostramos a continuación:

Tabla 16
Cálculo del riesgo residual

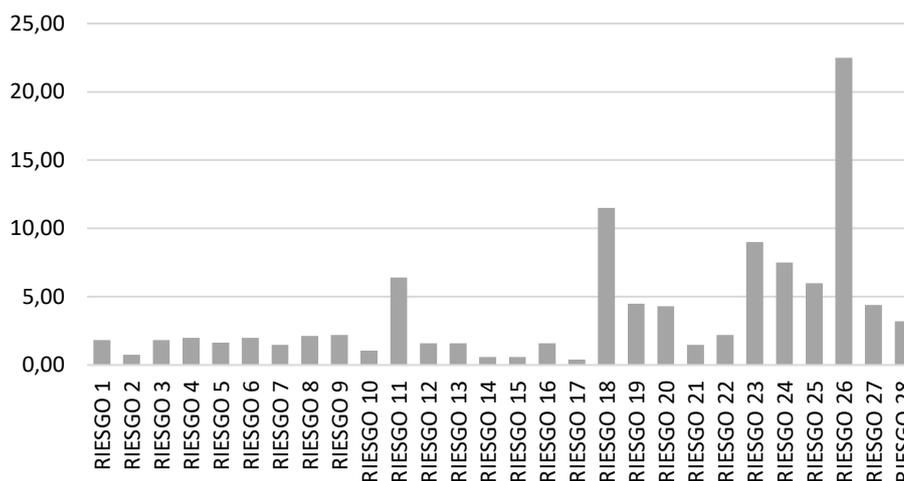
Código de Riesgo	Controles existentes	Análisis de controles			Efectividad	Riesgo residual			
		Naturaleza de control	Automatización	Frecuencia		Probabilidad	Impacto	Nivel de Riesgo Residual	
RIESGO 1	El cheque no se deposita se devuelve al cliente.	Preventivo	Manual	Permanente	3	1.67	1.10	1.83	ACEPTABLE
RIESGO 2	Administrador de ATM al momento de efectuar el conteo del dinero, valida que esté el documento, si no está lo reporta en el campo de observaciones para que el asesor al cliente lo regularice antes del segundo depósito.	Detectivo	Manual	Permanente	2	0.50	1.50	0.75	ACEPTABLE
RIESGO 3	Previo efectuar el segundo depósito el cliente debe regularizar la licitud de fondos.	Preventivo	Manual	Permanente	3	1.67	1.10	1.83	ACEPTABLE
RIESGO 4	No se procesa el depósito.	Preventivo	Manual	Permanente	3	1.33	1.50	2.00	ACEPTABLE
RIESGO 5	Si es un cliente que en reiteradas ocasiones no ha regularizado el formulario se cancela el servicio.	Detectivo	Manual	Permanente	2	1.50	1.10	1.65	ACEPTABLE
RIESGO 6	Administrador de ATM identifica billetes falsos antes de registrar el depósito.	Preventivo	Manual	Permanente	3	1.33	1.50	2.00	ACEPTABLE
RIESGO 7	No se procesa el depósito.	Preventivo	Manual	Permanente	3	1.33	1.10	1.47	ACEPTABLE
RIESGO 8	Especialista de procesos centralizados verifica el cheque y valor digitado, corrige el valor y procesa.	Correctivo	Manual	Permanente	3	0.67	3.20	2.13	ACEPTABLE
RIESGO 9	Es una causa para cancelar el contrato.	Detectivo	Manual	Permanente	2	2.00	1.10	2.20	ACEPTABLE
RIESGO 10	Especialista de procesos centralizados valida que todos los documentos estén regularizados previo activar la tarjeta de seguridad.	Preventivo	Manual	Permanente	3	0.33	3.20	1.07	ACEPTABLE
RIESGO 11	Una vez concluido el conteo de valores se compara con lo acreditado y de no ser correcto el valor se realizan los ajustes correspondientes.	Detectivo	Manual	Permanente	2	2.00	3.20	6.40	SIGNIFICATIVO
RIESGO 12	No existe control	No determinado	No determinado	No determinado	0	1	1.60	1.60	ACEPTABLE
RIESGO 13	Especialista de procesos centralizados revisa la ficha y solicita la firma del responsable si no lo está.	Correctivo	Manual	Permanente	3	1.33	1.20	1.60	ACEPTABLE
RIESGO 14	Asesor senior revisa que los formularios estén en la carpeta.	Detectivo	Manual	Periódico	2	0.50	1.20	0.60	ACEPTABLE
RIESGO 15	Asesor senior revisa que los formularios estén escaneados.	Detectivo	Manual	Periódico	2	0.50	1.20	0.60	ACEPTABLE
RIESGO 16	No existe control	No determinado	No determinado	No determinado	0	1	1.60	1.60	ACEPTABLE
RIESGO 17	Mientras no recibe el contrato, acta y todos los documentos habilitantes firmados por el cliente el EPC no habilita el servicio.	Preventivo	Manual	Permanente	3	0.33	1.20	0.40	ACEPTABLE
RIESGO 18	No existe control	No determinado	No determinado	No determinado	0	5	2.30	11.50	MODERADO

Código de Riesgo	Controles existentes	Análisis de controles			Efectividad	Riesgo residual			Nivel de Riesgo Residual
		Naturaleza de control	Automatización	Frecuencia		Probabilidad	Impacto		
RIESGO 19	No existe control	No determinado	No determinado	No determinado	0	1	4.50	4.50	ACEPTABLE
RIESGO 20	No existe control	No determinado	No determinado	No determinado	0	1	4.30	4.30	ACEPTABLE
RIESGO 21	Se desactiva la tarjeta de seguridad cuando pide una nueva.	Preventivo	Manual	Permanente	3	1.33	1.10	1.47	ACEPTABLE
RIESGO 22	No existe control	No determinado	No determinado	No determinado	0	2	1.10	2.20	ACEPTABLE
RIESGO 23	No existe control	No determinado	No determinado	No determinado	0	2	4.50	9.00	SIGNIFICATIVO
RIESGO 24	Asesor al cliente previo a otorgar otro código, valida si el solicitante ya tiene uno.	Preventivo	Manual	Ocasional	3	1.67	4.50	7.50	SIGNIFICATIVO
RIESGO 25	Asesor al cliente previo a otorgar otro código, valida si el solicitante ya tiene uno.	Preventivo	Manual	Ocasional	3	1.33	4.50	6.00	SIGNIFICATIVO
RIESGO 26	No existe control	No determinado	No determinado	No determinado	0	5	4.50	22.50	CATASTRÓFICO
RIESGO 27	No existe control	No determinado	No determinado	No determinado	0	1	4.40	4.40	ACEPTABLE
RIESGO 28	Asesor al cliente previo a otorgar otro código, valida si el solicitante ya tiene uno.	Preventivo	Manual	Ocasional	3	1.00	3.20	3.20	ACEPTABLE

Fuente: La institución financiera
Elaboración propia

Gráficamente se presenta el nivel de riesgo residual de la institución financiera en el uso de ATM:

Gráfico 5
Riesgo residual en el uso de ATM

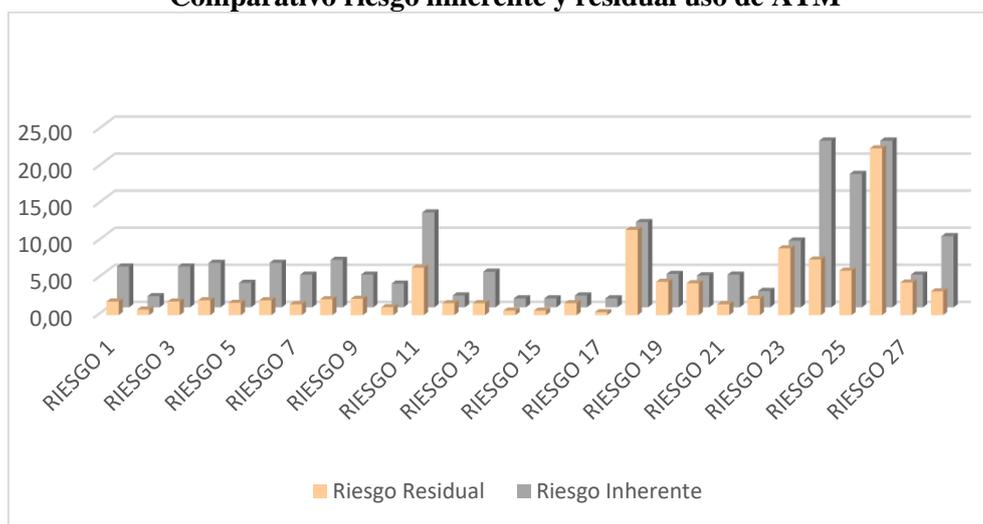


Fuente: Datos de la institución financiera
Elaboración propia

Luego de la aplicación de controles se puede observar que éstos han tenido un efecto positivo sobre la severidad de los eventos de riesgo de LA/FT 1, 3, 4, 6, 8, 11, 24, 25, 28 porque el valor de estas para el riesgo residual es menos que el riesgo inherente,

lo que significa que el control es eficiente. Por otro lado, los eventos de riesgo de LA/FT 12, 16, 18, 19, 20, 22, 23, 26 y 27 que no tienen controles definidos representan debilidades para la institución financiera, por lo que deben ser revisados. En ese sentido, los eventos de riesgo 18 y 26 requiere especial atención pues al no tener controles su severidad continúa siendo moderado y catastrófica respectivamente para la institución.

Gráfico 6
Comparativo riesgo inherente y residual uso de ATM



Fuente: Datos de la institución financiera
Elaboración propia

5. Tratamiento del riesgo

Una vez que hemos analizado los controles establecidos por la institución, se concluye que para el caso del uso de los ATM estos son controles preventivos, manuales y permanentes, en cambio en la apertura de cuentas online son controles preventivos, manuales y periódicos. En ese sentido, varias de las propuestas que detallamos a continuación se enfocan en automatizar los controles que de continuar siendo manuales representan una debilidad para la institución:

5.1. Apertura de cuentas online

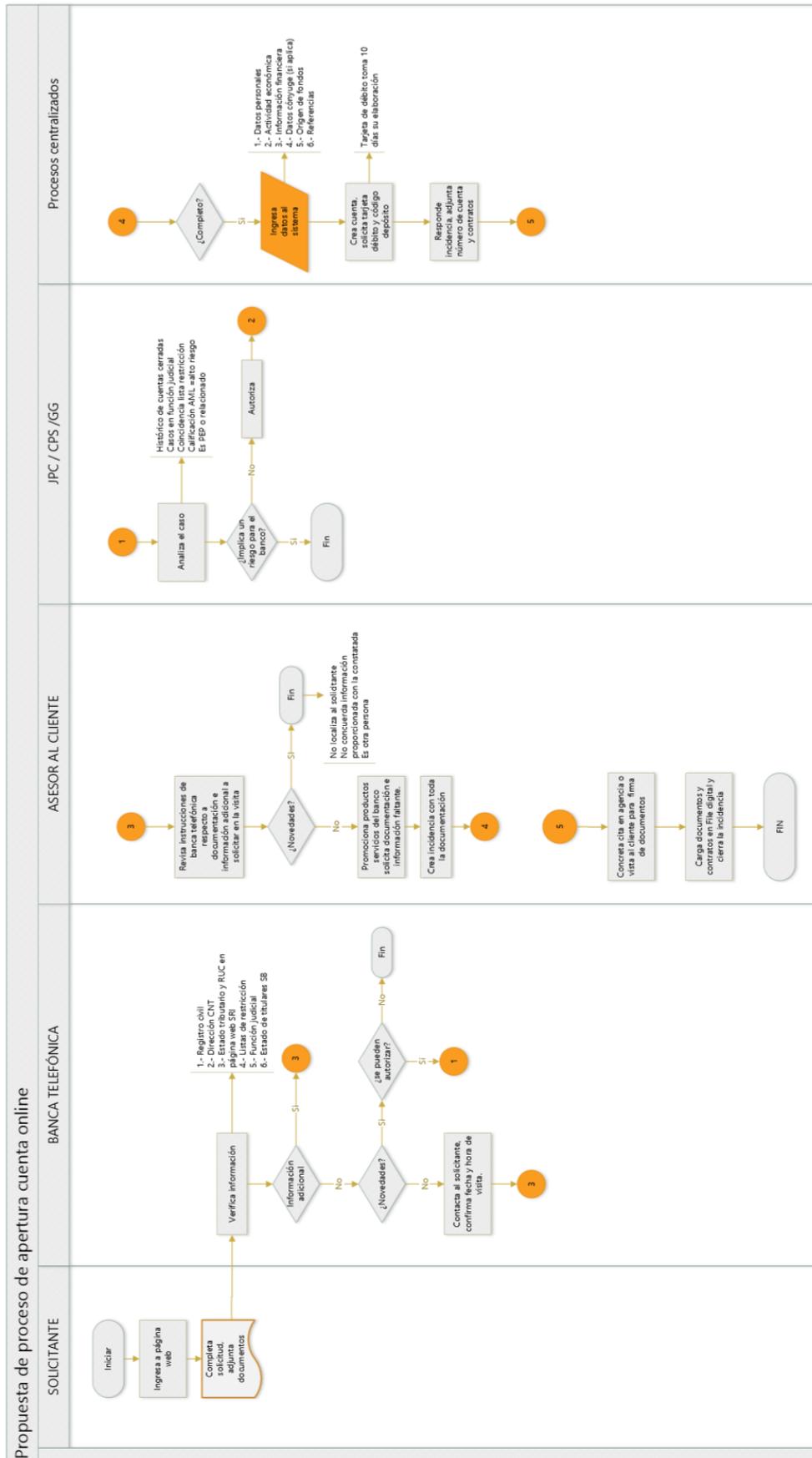
Si bien en este proceso no hubo eventos de riesgo catastróficos luego de la aplicación de controles, 1 de ellos representan un riesgo crítico, 2 son moderados y 5 significativos para la institución, mientras que 14 son aceptables. En ese sentido, consideramos que existen mejoras que se pueden implementar en este proceso, las cuales detallamos a continuación:

1. Se identificó que una debilidad del proceso es que no todos los especialistas de banca telefónica efectúan la verificación de referencias al momento de la apertura de la cuenta online, debido a que no existe un campo en el sistema donde se registre dicha verificación. Por lo tanto, se sugiere que en el sistema se incluya un campo para dicho registro, de esta manera se evita que los especialistas de banca telefónica omitan esta validación, a la vez que se contaría con un sustento de la ejecución del proceso de conocimiento del cliente, en el caso de una auditoría.
2. Se sugiere a la institución financiera invertir en la compra de bases de datos completas y confiables, de las cuales se pueda extraer información básica de los solicitantes como por ejemplo: nombres completos, fecha de nacimiento, dirección, número de teléfono, entre otros datos imprescindibles al momento de abrir una cuenta, de tal manera que se minimiza la probabilidad de que los especialistas de procesos centralizados comentan errores al momento de ingresar la información al sistema, ya sea, por el volumen de cuentas a abrir o porque la caligrafía de los clientes es poco entendible. Así también, la compra de estas bases de datos representa una ventaja para la institución porque puede corroborar los datos proporcionados por el solicitante y obtener mayor información sobre el mismo, útil para la toma de decisiones.
3. Es recomendable que la institución invierta en la implementación de nuevas tecnologías como: reconocimiento facial, huella digital, etc, ya que, más allá de permitirle a la institución ser competitiva, optimiza recursos y reduce el tiempo de apertura de las cuentas, pues en la actualidad demora alrededor de 72 horas lo que comparado con la competencia no es atractivo para el cliente.
4. Si bien los especialistas de banca telefónica previo a la apertura de cuenta online validan que el solicitante no conste en listas, es una etapa del proceso que al ser manual puede ser susceptible de omisiones y errores, por lo que se sugiere, que sea el sistema que valide si el solicitante consta en listas de restricción solo con el registro de nombres y documento de identidad, antes de crear un perfil como está establecido en la actualidad.
5. La carga correcta de las listas de restricción, de las listas PEP y listas de empresas fantasmas, es uno de los mecanismos más importantes para evitar que personas que estén involucradas en LA/FT, altos funcionarios públicos y empresas que no existen se vinculen a la institución sin ser identificados, por

lo tanto, la verificación de la carga de las mismas debe ser automatizada, pues en la actualidad es un proceso manual que por la extensión de las listas no puede ser validada en su totalidad y evita conocer si existieron errores en el proceso lo que no garantiza su efectividad. El implementar una notificación para informar cuando las listas de restricción hayan sido cargadas o cuando las mismas hayan presentado errores o inconvenientes es lo que se sugiere.

6. Por el momento para un asesor al cliente o especialista de banca telefónica no es fácil identificar cuando un cliente ha sido calificado como de alto riesgo de LA/FT, no porque el sistema no lo permita, pero algunos funcionarios desconocen u omiten que deben validar constantemente este aspecto. En ese sentido, se recomienda que el sistema alerte cuando un cliente es calificado de alto riesgo al especialista de banca telefónica o asesor al cliente a cargo para que efectúe la debida diligencia ampliada, solicite autorización a la gerencia y demás procesos que se detallan en el manual de PLA/FT para estos casos.
7. No se debería generar un número de cuenta, ni solicitar una tarjeta de débito y código de depósito si no se ha verificado la identidad del solicitante. En ese sentido, se recomienda cambiar el orden del proceso de apertura de cuenta online actual, de tal manera que la visita al solicitante, se realice luego de haber verificado la información ingresada en la solicitud. Visita que, en la actualidad se realiza después de haber registrado al solicitante en el sistema y generado la cuenta. Con esta medida consideramos se mitigan los eventos de riesgo de LA/FT 16, 17, 18, 19 y 20. Como se muestra en el siguiente flujograma:

Ilustración 11
Flujograma del proceso propuesto para apertura de cuenta online



Fuente y elaboración propia

5.2. Uso de ATM

A diferencia del proceso de apertura de cuentas online, en el uso de ATM existe un evento de riesgo LA/FT catastrófico para la institución, porque éste no cuenta con procedimientos claros ni controles que lo mitiguen. Así también, hay un evento de riesgo de LA/FT moderado, 4 eventos de riesgo de LA/FT significativos y 22 eventos de riesgo de LA/FT aceptables. En ese sentido, nuestra propuesta una vez que hemos conocido el proceso a profundidad es:

1. Se ha identificado que una debilidad de la institución financiera es el archivo de documentación soporte de las transacciones efectuadas a través de ATM, pues anteriormente contaba con un sistema donde diariamente se escaneaban los documentos respaldo de las transacciones. Sin embargo, desde el 2015 se dejó de utilizar y pese a que cada responsable archiva el documento de su competencia, se recomienda contar con un archivo centralizado para evitar inasequibilidad o pérdida de documentación, lo cual podría ser un motivo de sanción por parte de los organismos de control.
2. Si la institución financiera ofrece la posibilidad de efectuar transacciones sin la necesidad de tarjeta de débito debe contar con los procedimientos y controles adecuados para ello. En ese sentido, debido a que la institución por política interna debe identificar al depositante, nuestra sugerencia es que, los códigos de depósito deben ser temporales, máximo 24 horas y solo para depositar el monto especificado, caso contrario el sistema no debería permitir la asignación de un nuevo código sin la cancelación del anterior. Si es cliente lo solicita por la aplicación móvil. Ver ilustración 11.
3. En el caso de que un no cliente desee realizar un depósito a un cliente de la institución, la propuesta es: que en la página web de la institución se coloque la opción solicitud de código de depósito, en la cual al dar clic, solicite nombres completos, número de documento de identidad, monto a depositar, número de cuenta y número de celular al cual llegará el código de depósito cuya duración será de 24 horas y servirá solo para depositar el monto antes señalado. En el caso de ser un monto igual o mayor a 5,000.00USD, una vez que el depositante coloca el monto el sistema genera el formulario de licitud de fondos que deberá ser llenada y aceptado online por el no cliente para poder obtener el código de depósito. O en su defecto, según el apetito de riesgo de

la institución se puede mantener que solo clientes pueden depositar montos mayores o iguales a 5,000.00USD; destinando el código de depósito solo para depósitos menores o iguales a 4,999.99USD. Toda la información requerida para generar el código de depósito deberá quedar registrada en el core bancario. Ver ilustración 11.

4. En la actualidad para depósitos con código de depósito, la institución financiera asume que quien lo solicitó es quien realiza el depósito. Sin embargo, el presente trabajo nos ha permitido evidenciar que no es así, pues en la actualidad el código de depósito es solicitado por una persona quien proporciona información general a la institución, la cual es registrada en el sistema. Debido a que el código de depósito no tiene un tiempo límite de vigencia es susceptible de ser transferido a terceras personas de las cuales el banco desconoce y no posee un registro. En ese sentido, se sugiere que al momento de efectuar el depósito tanto con tarjeta de débito como con código de depósito el ATM solicite el número de cédula de quien efectúa el mismo, pues esta es información que entidades como la Fiscalía y la UAFE solicitan para las investigaciones de casos de LA/FT. Ver ilustración 11.
5. Así también, consideramos que otra opción para minimizar la entrega de códigos de depósitos, es impulsar el uso de transferencias bancarias y ofrecer a los clientes la billetera digital, como mecanismo para admitir pagos y realizar depósitos, pues el cliente al contar con su tarjeta de débito en su celular reduce la necesidad de contar con medios alternativos para realizar transacciones.
6. Tomando como ejemplo los cajeros automáticos de los bancos estadounidenses, se recomienda invertir en mejorar la tecnología de los ATM que en la actualidad posee la institución financiera, pues sería interesante que la misma contara con un ATM capaz de identificar billetes falsos y leer el monto que se registra en el cheque, convirtiendo de esta manera los procesos más eficientes.
7. Finalmente, para evitar que la institución tenga clientes con varias tarjetas de débito activas, nuestra sugerencia es que el sistema no permita sobrepasar los límites planteados por la institución para tarjetas de débito principales y adicionales.

Ilustración 12
Flujograma del proceso propuesto para uso de ATM



Fuente y elaboración propia

Capítulo quinto

Conclusiones y recomendaciones

1. Conclusiones

Los bancos privados representan el 80% del total del sistema financiero ecuatoriano, motivo por el cual son el sector más susceptible para lavar dinero y financiar al terrorismo, pues por su conexión con otros sectores económicos, rapidez y seguridad para efectuar transacciones es el sector favorito por los delincuentes para dar apariencia de legalidad al dinero de procedencia ilegal, dar continuidad a sus actividades ilegales y financiar actos terroristas. Por esta razón, las instituciones financieras no pueden dejar de lado invertir en implementar, evaluar y mejorar sus controles al desarrollar nuevas aplicaciones, procesos, productos o modelos de negocio, de tal manera que permitan disminuir los riesgos de LA/FT para salvaguardar el bienestar de los depositantes y de la institución.

Al identificar las características de la banca electrónica hemos comprendido que mediante la banca electrónica el sistema financiero ha podido llegar a lugares donde la banca tradicional no llegaba, lo que implica el cambio y desarrollo de todos los miembros que integran el sistema financiero y de los procesos de negocio. Sin embargo, hemos descubierto también que, las tipologías de lavado de activos y financiamiento del terrorismo en la banca electrónica son las mismas que existían para la banca tradicional la diferencia es que se han acoplado con facilidad a estas nuevas tecnologías y han encontrado en ellas oportunidades para evitar ser identificados, lamentablemente son los controles los que no han podido adaptarse y desarrollarse conforme a los avances tecnológicos, pues se requiere recursos y personal especializados para poder evolucionar. Es en este punto, donde la entidad debe conocer sus riesgos de LA/FT para poder administrarlos con base a su realidad, pues es parte integral de las buenas prácticas gerenciales para minimizar pérdidas y maximizar oportunidades.

El enfoque de los gobiernos en los últimos años ha sido la bancarización porque permite el acceso a instrumentos financieros a personas con menores ingresos, su formalización y pago de impuestos. Sin embargo, existe una brecha entre las normativas que lo fomentan y las de prevención de LA/FT, pues mientras las primeras buscan la inclusión financiera a través de nuevos mecanismos y tecnologías, las segundas aún no

han evolucionado y se mantiene ajena a las nuevas tendencias de hacer banca. La recomendación de los organismos internacionales ha sido el enfoque basado en riesgos, pero si por un lado la normativa señala que se debe buscar e implementar los medios para involucrar a más sectores al sistema financiero y por otro lado se sugiere ser restrictivo, la relación costo beneficio se convierte en un factor determinante para las instituciones financieras, ya que, para aquellas instituciones grandes el costo de ser más accesible a los sectores informales será más llevadero, mientras que para una institución pequeña visitar al cliente, levantar su información financiera, verificar la razonabilidad de sus ingresos, en sí llevar un procesos adecuado de KYC para minimizar riesgos de LA/FT frente al beneficio de vincular a este nuevo cliente significa dejar de hacer negocio.

El analizar lo planteado en las mejores prácticas internacionales y la normativa nacional en cuanto a la administración del riesgo de LA/FT, permite concluir que, con ayuda de internet y a través del uso de aplicativos móviles los bancos han podido llegar a lugares donde establecer una agencia sería muy costoso, han podido reducir costos y se han vuelto más eficientes, pues abren cuentas, receptan solicitudes de crédito, permiten pagos de servicios básicos y reducen el riesgo que implica transportar efectivo. Sin embargo, no importa la forma en cómo se vincule al cliente, la única manera de administrar el riesgo de LA/FT es conociendo plenamente al cliente. El uso de reconocimiento biométrico, claves, certificados digitales son algunas de las opciones que el sistema financiero utiliza para este fin, pero aún falta capacitación, infraestructura, regulación e inversión que permitan la incorporación de nuevas tecnologías para mejorar la administración de riesgos.

Luego del análisis a los procesos y controles existentes en la institución financiera, a través de una matriz de riesgo de LA/FT se concluye que entre las medidas que la misma debería tomar para mitigar estos riesgo están: invertir en sistemas de monitoreo pues existen transacciones que representan posibles casos de lavado de activos que no están siendo detectadas, así también, debe adecuar su core bancario para contar con la información adecuada para además de responder a los requerimientos de los organismos de control pueda contar con insumos para un adecuado monitoreo y establecimiento de perfiles transaccionales y de comportamiento del cliente; la capacitación es otro factor que la institución debe tomar en consideración, pues la misma es susceptible de ser usada para LA/FT a través de sus empleados, ya sea porque estos omiten cumplir con ciertos controles o porque desconocen de las políticas y procedimientos de PLA/FT. Por otro lado, es importante que la institución revise y rediseñe nuevos controles acordes a los

nuevos procesos, pues se evidencia que hay controles que no se apegan a la realidad del giro del negocio incluso la mayoría de estos son manuales y aunque esto no implique que sea un mal control, por la rapidez que implica la banca electrónica es necesario que los controles sean automatizados y vayan de la mano de los procesos realizados. Finalmente el input de todo proceso de administración de riesgos es una buena data, particular que también se identifica como una debilidad de la institución.

2. Recomendaciones

Si bien los sujetos obligados son el primer mecanismo de defensa contra el LA/FT no se debe asignar toda la responsabilidad de la lucha contra estos delitos a este segmento, pues para que el resultado sea efectivo debe existir un trabajo conjunto entre los gobiernos, entidades de control y sujetos obligados. Por ello es recomendable que cada uno de los actores en el ciclo de PLA/FT se capacite continuamente, para que puedan asumir su papel de manera adecuada, coordinada y responsable. Ya que, solo la capacitación permitirá la actualización de nuevos conceptos, tipologías, mecanismos de defensa que harán el trabajo de PLA/FT efectivo. Pues la falta de conocimiento es el impedimento para que buenos proyectos no puedan ser puestos en práctica.

Son empresas exitosas aquellas que han sabido administrar sus riesgos, por eso sugerimos a las instituciones financieras no escatimar en incorporar nuevos mecanismos, sistemas y directrices para la prevención del riesgo de LA/FT e involucrar a todo el personal de la institución, pues solo de esta manera la institución podrá conseguir el comprometimiento de todas las áreas y la efectividad de las políticas, procedimientos y controles establecidos.

Es importante que los supervisores apoyen el cumplimiento de las normas, pero partiendo de hacer negocio, centren sus revisiones en un enfoque basado en riesgos, ya que, si la revisión es estandarizada para todas las entidades financieras la administración del riesgo de LA/FT basada en un enfoque en riesgos pasa a ser irrelevante para convertirse en mero cumplimiento normativo y por ende ineficiente para el sistema financiero en la prevención del LA/FT. Así también, es importante que trabajen en conseguir que las normas vayan de la mano con el desarrollo de la banca, pues en ella se debería contemplar el uso de nuevas tecnologías para realizar eficientemente el trabajo de PLA/FT, regular el uso de bases de datos, pues mejoran el conocimiento del cliente a la vez que reducen costos y mejoran los procesos de debida diligencia.

Es importante que las instituciones financieras se actualicen y traten de incorporar dentro de su estructura equipos especializados en inteligencia artificial, ya que, ofrecen la posibilidad de realizar seguimientos de las transacciones de los clientes lo que apoyan el monitoreo y el establecimiento de perfiles de comportamiento útiles para identificar transacciones inusuales y posibles casos de lavado de activos y financiamiento del terrorismo a tiempo.

Luego del análisis realizado a los procedimientos de apertura de cuentas online y uso de ATM, con la finalidad de minimizar los riesgos de LA/FT se sugiere a la institución: invertir en la implementación de nuevas tecnologías como reconocimiento facial y huella digital para minimizar costos, riesgos y tiempo en la apertura de cuentas, visitar al solicitante después de verificar la información registrada por éste en su solicitud de apertura, ya que, evitará que se genere un número de cuenta, tarjeta de débito y código de depósito sin antes verificar la identidad del solicitante. Para dificultar la presentación de tipologías de LA/FT los códigos de depósito deben tener un tiempo de vigencia, caso contrario la institución debe adecuar el sistema para evitar que otorgue un nuevo código de depósito sin cancelar el anterior y no sobrepasar los límites establecidos en la institución al otorgar tarjetas de débito principal y adicional. Así también, consideramos que otra opción para minimizar la entrega de códigos de depósito, es impulsar el uso de transferencias bancarias y ofrecer a los clientes la billetera digital, pues el cliente al contar con su tarjeta de débito en su celular reduce la necesidad de contar con medios alternativos para realizar transacciones. En el caso de que un no cliente desee realizar un depósito a un cliente de la institución, la propuesta es: que en la página web de la institución se coloque la opción solicitud de código de depósito, en la cual al dar clic, solicite nombres completos, número de documento de identidad, monto a depositar, número de cuenta y número de celular al cual llegará el código de depósito cuya duración será de 24 horas y servirá solo para depositar el monto antes señalado. En el caso de ser un monto igual o mayor a 5,000.00USD, una vez que el depositante coloca el monto el sistema genera el formulario de licitud de fondos que deberá ser llenada y aceptado online por el no cliente para poder obtener el código de depósito. O en su defecto, según el apetito de riesgo de la institución se puede mantener que solo clientes pueden depositar montos mayores o iguales a 5,000.00USD; destinando el código de depósito solo para depósitos menores o iguales a 4,999.99USD. Toda la información requerida para generar el código de depósito deberá quedar registrada en el core bancario.

Si bien la institución cuenta con una metodología escrita, la cual ha tomado en consideración el SARLAFT, la debilidad de la institución es que esta metodología no se ve plasmada en la matriz de riesgo. Por ello sugerimos que el área de prevención de LA/FT de la institución financiera bajo análisis, levante un listado de eventos de riesgo enfocados en el nuevo modelo de negocio del banco. Así también, es importante el reevaluar la matriz de riesgo existente pues la actual es subjetiva y no contempla varias de las etapas de la administración de riesgos, lo que la convierte en una matriz de riesgo débil, de nulo soporte en el proceso de gestión y administración de riesgo de la entidad.

Debido a que, una escala de 3x3 permite una menor amplitud en los cuadrantes de riesgo, reduce la escala e incrementa la probabilidad de que el factor de riesgo se ubiquen en niveles de riesgo alto, sugerimos a la entidad ampliar su escala, tomando como ejemplo la que hemos usado en este trabajo, una escala 5x5, pues permite mayor amplitud y desplazamiento de los factores de riesgo, de tal manera, que el tratamiento de los mismos sea más específico y asertivo.

Entre las recomendaciones para ciertos riesgos operativos identificados en la apertura de cuentas online y uso de ATM que pueden llevar al riesgo de LA/FT están: comprar bases de datos con información básica de personas como número de cédula, nombres completos, dirección, número de teléfono, etc., para minimizar la probabilidad de tener registros incorrectos e incompletos de clientes en el sistema. Para minimizar el riesgo de omisión de validación de potenciales clientes en las listas de restricción, se recomienda incorporar un campo en el sistema donde quede constancia de la ejecución de esta tarea o, en su defecto adaptar al sistema para que automáticamente solo con el registro del nombre completo y documento de identidad del solicitante se valide si éste consta o no en las listas de restricción. Contar con una notificación de la carga de las listas de restricción, para que los responsables puedan tomar acciones correctivas cuando se presenten inconvenientes o errores en su carga. Así como, una notificación para cuando el cliente ha sido catalogado como de riesgo alto, de tal manera que, minimicen las omisiones de debida diligencia y autorizaciones de gerencia por desconocimiento de la calificación inicial del cliente. Implementar cajeros automáticos capaces de identificar billetes falsos, leer el monto que se registra en el cheque y solicitar el número de cédula del depositante, para evitar el registro erróneo del monto del cheque y falta de información de quien deposita el mismo. Contar con un archivo centralizado de documentos tanto físico como digital para evitar sanciones por pérdida o inasequibilidad de documentos.

Lista de referencias

- Astudillo, Erika. 2018. “Emprendimientos ofrecen soluciones digitales para la banca y sus clientes”. *El Telégrafo*, 19 de Junio. <https://www.eltelegrafo.com.ec/noticias/desde/1/emprendimientos-ofrecen-soluciones-digitales-para-la-banca-y-sus-clientes>.
- Banco Central del Ecuador. 2012. *Inclusión Financiera aproximaciones teóricas y prácticas*. Quito: El Chasqui ediciones.
- Barriga Bedoya, Franklin. 2011. *El lavado de activos en Iberoamérica y la necesidad de la armonización legislativa*. Quito: Artes gráficas señal impreseñal Cia. Ltda
- Cabuli, Ezequiel y Griselda Jatib. 2006. “La prevención del lavado de activos y el ejercicio profesional en el mundo globalizado”. *Revista del Notariado* 884. Abril-Junio. <https://www.colegio-escribanos.org.ar/biblioteca/cgi-bin/ESCRI/ARTICULOS/48676.pdf>.
- Caldas Blanco, María Eugenia, María Isabel Murias Bermejo y Alicia Gregorio Arroyo. 2015. *Iniciación a la actividad emprendedora y empresarial*. Madrid: Editex S.A.
- Castillo Merino, David, Patricia Gabaldón Quiñones, Elisabet Ruiz Dotras y Jorge Sainz González. 2010. *Hacia la banca multicanal la transformación del sector financiero en la economía del conocimiento*. Madrid: ESIC Editorial.
- Cifuentes Muñoz, Manuel Enrique, Jaime Ospina Velasco y Carlos Mario Serna Jaramillo. 2002. *Globalización de las transferencias electrónicas de fondos a través de cajeros automáticos*. Bogotá: Ediciones Jurídicas Gustavo Ibáñez Ltda.
- Comisión Andina de Juristas. 2000. *Lavado de dinero: El sistema legal y su impacto socio económico*. Lima: Comisión Andina de Juristas.
- Comité de Basilea para la Supervisión Bancaria. *Gestión de Riesgos para la Banca Electrónica y Actividades con Dinero Electrónico*. 1998. <http://www.asbasupervision.com/es/todos/biblioteca-virtual-asba/gestion-de-riesgos/otros-1/129-gr-ot03/file>.

- Committee of Sponsoring Organizations. 2001. *Control Interno de los nuevos instrumentos financieros*. Traducido por Samuel Alberto Mantilla Blanco. Bogotá: Ecoe Ediciones.
- DO. Unidad de Análisis Financiero (UAF). “¿Qué es el financiamiento del terrorismo?”. *Unidad de Análisis Financiero*. Acceso el: 27 de Mayo de 2018. <https://www.uaf.gob.do/index.php/que-es-el-financiamiento-del-terrorismo>.
- EC. 2002. *Ley de Comercio Electrónico, Firma y Mensajes de Datos*. Registro Oficial 557, Suplemento, 17 de abril.
- EC. 2014. *Código Orgánico Monetario y Financiero*. Registro Oficial 332, Segundo Suplemento, 12 de septiembre.
- EC. 2016. *Ley de Prevención de Lavado de Activos y del Financiamiento de Delitos*. Registro Oficial Suplemento 802. 21 de julio.
- EC. 2018. *Libro I Norma de Control para las Entidades de los Sectores Financieros Público y Privado Título X Del Control Interno Capítulo III Normas para las entidades de los sectores financieros público y privado sobre prevención de lavado de activos, financiamiento del terrorismo y otros delitos*. Reformado con SB-2018-1207. 6 de diciembre.
- EC. Junta Bancaria del Ecuador. 2012. Resolución JB-2012-2148. 26 de abril.
- El Universo. 2018. “Bancos ya ofrecen más canales electrónicos en Ecuador”. *El Universo*. 29 de enero. <https://www.eluniverso.com/noticias/2018/01/30/nota/6591958/bancos-ya-ofrecen-mas-canales-electronicos>.
- Forester, Tom. 1992. *Sociedad de alta tecnología*. México: Siglo veintiuno editores s.a. de c.v.
- GAFI. *Estándares internacionales sobre la lucha contra el lavado de activos y el financiamiento del terrorismo y la proliferación, Las Recomendaciones del GAFI*. 2012. <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF-40-Rec-2012-Spanish.pdf>.

- González, Patricia Carolina. 2017. “La banca ofrece más servicios en línea”. *El Comercio*. 20 de mayo.
- HelpMyCash. 2017. “3 bancos que permiten abrir una cuenta bancaria en 5 minutos”. *HelpMyCash*. 26 de Abril. <https://www.helpmycash.com/blog/3-bancos-permiten-abrir-una-cuenta-bancaria-5-minutos/>.
- . 2017. “Así son los cajeros automáticos 50 años después de su aparición”. *HelpMyCash*. 24 de Abril. <https://www.helpmycash.com/blog/asi-los-cajeros-automaticos-50-anos-despues-aparicion/>.
- Infolaft Anticorrupción, fraude y LA/FT. 2017. “¿Qué es Sarlaft?”. *Infolaft*. 21 de julio. <https://www.infolaft.com/que-es-sarlaft/>.
- Lizarzaburu, Guillermo. 2018. “La banca inicia el 2018 con una envidiable salud”. *Expreso*. 16 de Marzo.
- Maldonado, Fausto, Dominic Burgos y Sofia Chávez. 2018. “El sector financiero es fuerte”. *Revista EKOS*. 4 de abril.
- Nando Lefort, Victor Manuel. 2014. *El lavado de dinero nuevo problema para el campo jurídico*. México: Trillas.
- Páucar Chappa, Marcial Eloy. 2013. *La investigación del delito de lavado de activos tipologías y jurisprudencia*. Lima: ARA Editores E.I.R.L.
- Peláez Martos, José María. 2014. *Manual práctico para la prevención del blanqueo de capitales*. Valencia: CISS grupo Wolters Kluwer.
- Peña Valenzuela, Daniel, comp. 2007. *Sociedad de la información digital: perspectivas y alcances*. Bogotá: Editoriales Curcio Penen.
- Reyes Hiedra, Patricio. 2012. *Administración de riesgos medición, seguimiento, análisis y control*. Quito: Killari.
- Robles, Daniel Elías, 2015. “Principios de Gestión de Riesgo basados en ISO 31000”. Video de YouTube. <https://www.youtube.com/watch?v=12E6XG-mlxQ>.
- Sintura, Francisco, Wilson Martinez y Fernando Quintana. 2011. *Sistemas de prevención de lavado de activos y de financiación del terrorismo*. Colombia: Legis Editores S.A.

Standards Australia/ Standards New Zealand Committee. *Estándar Australiano AS/NZS 4360:1999 Administración de Riesgos*. 1999. <https://www.edesaesp.com.co/wp-content/uploads/2013/05/ASNZ-4360-de-1999.pdf>.

Tapia, Evelyn. 2018. “73% de las transacciones bancarias se realizan en línea”. *El Comercio*. 12 de Febrero.

Tapia Evelyn, Pedro Maldonado. 2018. “Ecuador se conecta con la ola global de las ‘fintech’”. *Líderes*. 6 de Marzo. <https://www.revistalideres.ec/lideres/ecuador-fintech-tecnologia-desarrollo-banca.html>.

The Wolfsberg Group. *Directrices Globales sobre Prevención de Blanqueo de Capitales para Banca Privada*. 2002. <https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/translations/spanish/107.%20private-spanish.pdf>.

Torres Soto, Ulises. 2010. *El delito de lavado de activos*. Quito: Jurídica del Ecuador.

Zabala, Victor, Sofia Chávez y Andrés Calvopiña. 2019. “Ranking Financiero 2019”. *Revista EKOS*. Edición 301. Mayo.

Anexos

Anexo 1: Identificación de eventos de riesgo apertura de cuenta online

RIESGO 1	
Factor de Riesgo	Empleado
Actividad	Recopilación y validación de información
Descripción del Riesgo de LA/FT	La carga de las listas no es correcta
Riesgo Asociado	1 Operativo
	2 Legal
	3 Reputacional
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Especialista de Cumplimiento Especialista de Sistemas
Identificación de causas / vulnerabilidades	1.- Fallas de conexión en el sistema 2.- La carga de listas de restricción demoró más de lo habitual lo que generó fallas 3.- Especialista de cumplimiento cometió un error en la actualización de listas 4.- Actualización del sistema transaccional lo que genera incompatibilidad con las listas
Identificación de consecuencias	1.-Fondos ilícitos ingresen a la institución 2.-Facilitar transacciones para lavar activos 3.-La institución puede ser sancionada por no contar con adecuados controles
RIESGO 2	
Factor de Riesgo	Cliente
Actividad	Recopilación y validación de información
Descripción del Riesgo de LA/FT	Persona que consta en listas de restricción abre cuenta online
Riesgo Asociado	1 Operativo
	2 Legal
	3 Reputacional
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Especialista de Banca Telefónica Especialista de Cumplimiento
Identificación de causas / vulnerabilidades	1.-Especialista de cumplimiento desconoce que la carga de listas de restricción no se realizó correctamente en el sistema 2.-Deficiencia en la actualización de listas de restricción (proveedor) 3.-Especialista de cumplimiento omite actualizar listas de restricción 4.-Especialista de Banca Telefónica no efectúa correctamente la búsqueda en el sistema 5.-Especialista de Banca Telefónica omite revisar en listas de restricción
Identificación de consecuencias	1.-Fondos ilícitos ingresen a la institución 2.-Facilitar transacciones para lavar activos 3.-La institución puede ser sancionada por no contar con adecuados controles
RIESGO 3	
Factor de Riesgo	Cliente
Actividad	Recopilación y validación de información
Descripción del Riesgo de LA/FT	Empresa fachada o empresa de papel abre cuenta online
Riesgo Asociado	1 Operativo
	2 Legal
	3 Reputacional
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Especialista de Banca Telefónica Asesor al Cliente
Identificación de causas / vulnerabilidades	1.-Deficiencia en la aplicación de la política conozca su cliente 2.-Complicidad del empleado de la institución 3.-Anteponer el cumplimiento de metas comerciales a las políticas y procesos establecidos 4.-Especialista de Banca Telefónica no efectúa correctamente la búsqueda en el sistema 5.-No se visita el negocio previo su vinculación
Identificación de consecuencias	1.-Fondos ilícitos ingresen a la institución 2.-Facilitar transacciones para lavar activos 3.-La institución puede ser sancionada por no contar con adecuados controles

RIESGO 4	
Factor de Riesgo	Cliente
Actividad	Recopilación y validación de información
Descripción del Riesgo de LA/FT	Persona que se dedica a actividades con las cuales el banco no trabaja abre cuenta online
Riesgo Asociado	1 Operativo
	2 Reputacional
	3 Contagio
	4 Legal
Responsable del proceso (Propietario del Riesgo)	Especialista de Banca Telefónica
Identificación de causas / vulnerabilidades	1.-Especialista desconoce las políticas y procedimientos del banco (capacitación deficiente) 2.- Especialista omite el cumplimiento de las políticas y procedimientos del banco 3.-Anteponer el cumplimiento de metas comerciales a las políticas y procesos establecidos 4.-Complicidad del empleado de la institución
Identificación de consecuencias	1.-Si es una cuenta de ahorro por resolución de la junta bancaria, las IFI's no pueden cerrar estas cuentas, por lo tanto, el banco se ve obligado a mantenerla. 2.-El cliente puede presentar un reclamo ante la Superintendencia de Bancos contra la institución. 3.-Si las explicaciones para la SB no son suficientes puede la institución ser sancionada.

RIESGO 5	
Factor de Riesgo	Cliente
Actividad	Recopilación y validación de información
Descripción del Riesgo de LA/FT	PEP abre cuenta sin ser identificado
Riesgo Asociado	1 Operativo
	2 Contagio
	3 Reputacional
	4 Legal
Responsable del proceso (Propietario del Riesgo)	Especialista de Banca Telefónica Especialista de Cumplimiento Especialista de Sistemas
Identificación de causas / vulnerabilidades	1.-Especialista de Banca Telefónica omite revisar en listas de restricción 2.-Deficiencia del especialista para determinar que el posible cliente es PEP 3.-Especialista de cumplimiento desconoce que la carga de listas de restricción no se realizó correctamente en el sistema 4.-Deficiencias en la actualización de la lista de PEP's (proveedor) 5.-La carga de la lista de PEP's no se realizó correctamente en el sistema 6.-Especialista de Banca Telefónica no efectúa correctamente la búsqueda en el sistema 7.-Especialista de cumplimiento omite actualizar la lista de PEP's
Identificación de consecuencias	Dinero producto de la corrupción ingrese a la institución La institución puede ser sancionada por no contar con adecuados controles Se permitan transacciones de lavado de activos

RIESGO 6	
Factor de Riesgo	Cliente
Actividad	Recopilación y validación de información
Descripción del Riesgo de LA/FT	Persona jurídica que no proporciona total o parcialmente información de sus beneficiarios finales
Riesgo Asociado	1 Operativo
	2 Reputacional
	3 Contagio
	4 Legal
Responsable del proceso (Propietario del Riesgo)	Asesor al cliente
Identificación de causas / vulnerabilidades	1.-Ineficacia en la aplicación de los procesos de debida diligencia por parte del asesor al cliente 2.-Asesor al cliente desconoce las políticas y procedimientos del banco (capacitación deficiente) 3.-Asesor al cliente omite el cumplimiento de las políticas y procedimientos del banco 4.-Complicidad del empleado de la institución 5.-Anteponer el cumplimiento de metas comerciales a las políticas y procesos establecidos
Identificación de consecuencias	1.-Desconocer que los accionistas presentan coincidencias en listas de restricción 2.-Fondos ilícitos ingresen a la institución 3.-Facilitar transacciones para lavar activos 4.-La institución puede ser sancionada por no contar con adecuados controles

RIESGO 7	
Factor de Riesgo	Cliente
Actividad	Recopilación y validación de información
Descripción del Riesgo de LA/FT	PEP que no proporciona mayor información sobre sus actividades y origen de fondos abre cuenta online
Riesgo Asociado	1 Operativo
	2 Contagio
	3 Reputacional
	4 Legal
Responsable del proceso (Propietario del Riesgo)	Asesor al cliente
Identificación de causas / vulnerabilidades	1.-Debilidad en la aplicación de la política conozca a su cliente 2.-Asesor al cliente omite el cumplimiento de las políticas y procedimientos del banco 3.-Complicidad del empleado de la institución
Identificación de consecuencias	1.-Dinero producto de la corrupción ingrese a la institución 2.-La institución puede ser sancionada por no capacitar adecuadamente al personal 3.-Se permitan transacciones de lavado de activos

RIESGO 8	
Factor de Riesgo	Cliente
Actividad	Recopilación y validación de información
Descripción del Riesgo de LA/FT	Solicitante que proporciona información falsa abre cuenta on line
Riesgo Asociado	1 Legal
	2 Reputacional
	3 Operativo
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Especialista de Banca Telefónica Asesor al Cliente
Identificación de causas / vulnerabilidades	1.-Complicidad del empleado de la institución 2.-Sistema no está conectado con bases de validación de documento de identidad 3.-Empleado omite verificar la información en páginas oficiales y referencias 4.-Falta de capacitación y conocimiento de políticas y procedimientos del banco
Identificación de consecuencias	1.-Fondos ilícitos ingresen a la institución 2.-Facilitar transacciones para lavar activos 3.-La institución puede ser sancionada por no contar con adecuados controles

RIESGO 9	
Factor de Riesgo	Empleado
Actividad	Recopilación y validación de información
Descripción del Riesgo de LA/FT	No verificar la información en páginas oficiales, función judicial y listas de restricción
Riesgo Asociado	1 Operativo
	2 Legal
	3 Reputacional
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Especialista de Banca Telefónica
Identificación de causas / vulnerabilidades	1.-Especialista omite el cumplimiento de las políticas y procedimientos del banco 2.-Especialista desconoce las políticas y procedimientos del banco (capacitación deficiente) 3.-Especialista de Banca Telefónica no realiza adecuadamente la búsqueda en las páginas oficiales 4.-Complicidad del empleado de la institución
Identificación de consecuencias	1.-La información proporcionada por el cliente sea falsa 2.-Fondos ilícitos ingresen a la institución 3.-Facilitar transacciones para lavar activos 4.-La institución puede ser sancionada por no contar con adecuados controles

RIESGO 10	
Factor de Riesgo	Empleado
Actividad	Recopilación y validación de información
Descripción del Riesgo de LA/FT	No verificar la información registrada por el solicitante con la referencia
Riesgo Asociado	1 Operativo
	2 Legal
	3 Reputacional
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Especialista de Banca Telefónica
Identificación de causas / vulnerabilidades	1.-Especialista omite el cumplimiento de las políticas y procedimientos del banco 2.-Especialista desconoce las políticas y procedimientos del banco (capacitación deficiente) 3.-No hay un campo en el sistema para identificar a los clientes que han sido referenciados 4.-Complicidad del empleado de la institución
Identificación de consecuencias	1.-La información proporcionada por el cliente sea falsa 2.-Fondos ilícitos ingresen a la institución 3.-Facilitar transacciones para lavar activos 4.-La institución puede ser sancionada por no contar con adecuados controles

RIESGO 11	
Factor de Riesgo	Empleado
Actividad	Registro del cliente
Descripción del Riesgo de LA/FT	Incorrecto registro de información en el sistema
Riesgo Asociado	1 Operativo
	2 Contagio
	3 Legal
	4 Reputacional
Responsable del proceso (Propietario del Riesgo)	Especialista de procesos centralizados
Identificación de causas / vulnerabilidades	1.-Excesiva carga laboral 2.-Desconcentración en el registro de información 3.-Fallas en el sistema al momento de guardar la información 4.-Falta de validadores en el sistema 5.-Fallas en los reportes obtenidos del sistema
Identificación de consecuencias	1.-Se obtiene un perfil distinto del cliente 2.-La calificación de riesgo AML discrepa de la realidad 3.-No se puede efectuar un monitoreo adecuado del cliente

RIESGO 12	
Factor de Riesgo	Empleado
Actividad	Registro del cliente
Descripción del Riesgo de LA/FT	No solicitar autorización Jefe de Agencia para cliente con negocio de menos de un año de funcionamiento
Riesgo Asociado	1 Operativo
	2 Contagio
	3 Legal
	4 Reputacional
Responsable del proceso (Propietario del Riesgo)	Especialista de Banca Telefónica Asesor al Cliente
Identificación de causas / vulnerabilidades	1.-Especialista omite el cumplimiento de las políticas y procedimientos del banco 2.-Especialista desconoce las políticas y procedimientos del banco (capacitación deficiente) 3.-Falta de supervisión en la apertura de cuenta
Identificación de consecuencias	1.-Incumplimiento de la política de cuatro ojos 2.-Puede vincularse a negocios pantalla o de papel 3.-La institución puede ser sancionada por no tener controles adecuados

RIESGO 13	
Factor de Riesgo	Empleado
Actividad	Registro del cliente
Descripción del Riesgo de LA/FT	No solicitar autorización Jefe de Agencia para cliente con ingresos mensuales superiores a los 100,000.00
Riesgo Asociado	1 Operativo
	2 Contagio
	3 Legal
	4 Reputacional
Responsable del proceso (Propietario del Riesgo)	Especialista de Banca Telefónica Asesor al Cliente
Identificación de causas / vulnerabilidades	1.-Especialista omite el cumplimiento de las políticas y procedimientos del banco 2.-Especialista desconoce las políticas y procedimientos del banco (capacitación deficiente) 3.-Falta de supervisión en la apertura de cuenta
Identificación de consecuencias	1.-Incumplimiento de la política de cuatro ojos 2.-Puede vincularse a negocios pantalla o de papel 3.-La institución puede ser sancionada por no tener controles adecuados

RIESGO 14	
Factor de Riesgo	Empleado
Actividad	Registro del cliente
Descripción del Riesgo de LA/FT	No solicitar autorización de la Gerencia por ser un cliente de alto riesgo
Riesgo Asociado	1 Operativo
	2 Contagio
	3 Legal
	4 Reputacional
Responsable del proceso (Propietario del Riesgo)	Especialista de Banca Telefónica Asesor al Cliente
Identificación de causas / vulnerabilidades	1.-Especialista omite el cumplimiento de las políticas y procedimientos del banco 2.-Especialista desconoce las políticas y procedimientos del banco (capacitación deficiente) 3.-Fallas en el sistema para generar la calificación inicial 4.-Falta de supervisión en la apertura de cuenta
Identificación de consecuencias	1.-Incumplimiento de la normativa nacional por la cual puede ser sancionada la IFI 2.-No efectuar la debida diligencia que aplica para los clientes de alto riesgo 3.-Desconocer el riesgo que como institución se está asumiendo

RIESGO 15	
Factor de Riesgo	Empleado
Actividad	Registro del cliente
Descripción del Riesgo de LA/FT	No solicitar autorización de la Gerencia para vincular a un cliente PEP
Riesgo Asociado	1 Operativo
	2 Contagio
	3 Legal
	4 Reputacional
Responsable del proceso (Propietario del Riesgo)	Especialista de Banca Telefónica Asesor al Cliente
Identificación de causas / vulnerabilidades	1.-Especialista omite el cumplimiento de las políticas y procedimientos del banco 2.-Especialista desconoce las políticas y procedimientos del banco (capacitación deficiente) 3.-Falta de supervisión en la apertura de cuenta
Identificación de consecuencias	1.-Incumplimiento de la normativa nacional por la cual puede ser sancionada la IFI 2.-No efectuar la debida diligencia que aplica para los clientes PEP 3.-Desconocer el riesgo que como institución se está asumiendo

RIESGO 16	
Factor de Riesgo	Empleado
Actividad	Registro del cliente
Descripción del Riesgo de LA/FT	Abrir la cuenta pese a que no se cuenta con la información requerida
Riesgo Asociado	1 Operativo
	2 Legal
	3 Reputacional
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Especialista de procesos centralizados Asesor Senior
Identificación de causas / vulnerabilidades	1.-Autorizaciones para abrir cuenta y luego regularizar la información 2.-Especialista de procesos centralizados no informa la documentación que queda pendiente por regularizar 3.-Asesor senior no se percata que están documentos pendientes de regularizar 4.-Los clientes reciben un mensaje de que su tarjeta está lista y acuden a retirarla sin llevar ni mencionar que tienen pendiente de completar información en su solicitud 5.-Complicidad del empleado de la institución 6.-Anteponer el cumplimiento de metas comerciales a las políticas y procesos establecidos
Identificación de consecuencias	1.-La institución no conoce plenamente al cliente 2.-Por la falta de información no se puede establecer adecuadamente el nivel de riesgo AML que representa el cliente para la institución 3.-Mayor riesgo de que una persona distinta a la que indica ser transaccione en la institución

RIESGO 17	
Factor de Riesgo	Jurisdicción
Actividad	Inicio relación comercial
Descripción del Riesgo de LA/FT	Una vez abierta la cuenta el cliente cambia de domicilio a una jurisdicción lejana lo cual dificulta su verificación.
Riesgo Asociado	1 Operativo
	2 Contagio
	3 Reputacional
	4 Legal
Responsable del proceso (Propietario del Riesgo)	Especialista de Banca Telefónica
Identificación de causas / vulnerabilidades	1.-El especialista de Banca Telefónica omite preguntar el propósito de la cuenta 2.-Deficiencia en la aplicación de la política conozca su cliente 3.-Falta de competencia del especialista para identificar señales de alerta
Identificación de consecuencias	1.-No poder actualizar la información a futuro 2.-No verificar si los fondos provienen de donde el cliente indica que son 3.-No poder efectuar una debida diligencia 4.-Facilitar el lavado de activos en el banco 5.-Ser objeto de sanción por la SB por incumplimiento a las políticas de PLA/FT

RIESGO 18	
Factor de Riesgo	Empleado
Actividad	Inicio relación comercial
Descripción del Riesgo de LA/FT	Entregar tarjeta de débito y número de cuenta sin que el cliente haya firmado el contrato
Riesgo Asociado	1 Legal
	2 Operativo
	3 Contagio
	4 Reputacional
Responsable del proceso (Propietario del Riesgo)	Asesor al cliente Asesor senior
Identificación de causas / vulnerabilidades	1.-Asesores no verifican en el sistema si hay algo pendiente antes de entregar los servicios 2.-Personal temporal como los Floor Manager son en ocasiones los encargados de entregar las tarjetas de débito, quienes no tienen acceso al sistema 3.-Los clientes reciben un mensaje de que su tarjeta está lista y acuden a retirarla sin mencionar que tienen pendiente la firma del contrato 4.-Falta de capacitación y conocimiento de políticas y procedimientos del banco por parte del
Identificación de consecuencias	1.-Personas que no han entregado toda la información y documentación tengan acceso a la cuenta y tarjeta de débito 2.-Personas a las cuales no se ha podido validar su identidad empiecen a usar los productos del banco 3.-Incumplimiento de la normativa nacional por la cual puede ser sancionada la IFI

RIESGO 19	
Factor de Riesgo	Empleado
Actividad	Inicio relación comercial
Descripción del Riesgo de LA/FT	No identificar que la cuenta no es para el cliente, sino para ser usada por un tercero.
Riesgo Asociado	1 Contagio
	2 Reputacional
	3 Legal
	4 Operativo
Responsable del proceso (Propietario del Riesgo)	Asesor al cliente Especialista de cumplimiento
Identificación de causas / vulnerabilidades	1.- Fallas en la identificación del propósito de la apertura de la cuenta 2.- Fallas en el proceso de entrevista al cliente 3.- Fallas en la identificación del origen de recursos a manejar en la cuenta 4.- Fallas en los sistemas de monitoreo y alertas 5.- Falta de monitoreo por parte del asesor al cliente
Identificación de consecuencias	1.- Fondos ilícitos ingresen a la institución 2.- Fomentar transacciones para lavar activos 3.- La institución puede ser sancionada por no contar con adecuados controles

RIESGO 20	
Factor de Riesgo	Empleado
Actividad	Inicio relación comercial
Descripción del Riesgo de LA/FT	No validar que el solicitante sea quien dijo ser
Riesgo Asociado	1 Legal
	2 Reputacional
	3 Operativo
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Asesor al cliente Asesor Senior
Identificación de causas / vulnerabilidades	1.- Asesores desconoce las políticas y procedimientos del banco (capacitación deficiente) 2.- Asesores omite el cumplimiento de las políticas y procedimientos del banco 3.- Complicidad del empleado de la institución
Identificación de consecuencias	1.- Fondos ilícitos ingresen a la institución 2.- Fomentar transacciones para lavar activos 3.- La institución puede ser sancionada por no contar con adecuados controles

RIESGO 21	
Factor de Riesgo	Cliente
Actividad	Inicio relación comercial
Descripción del Riesgo de LA/FT	Cliente no se acerca a regularizar la apertura
Riesgo Asociado	1 Legal
	2 Operativo
	3 Contagio
	4 Reputacional
Responsable del proceso (Propietario del Riesgo)	Especialista de Banca Telefónica Asesor Senior
Identificación de causas / vulnerabilidades	1.- Complicidad del empleado de la institución 2.- Falta de competencia del especialista para identificar señales de alerta 3.- Deficiencia en la aplicación de la política conozca su cliente
Identificación de consecuencias	1.- Tener cuentas abiertas sin formalizar la apertura 2.- Cuentas que pueden ser mal usadas por empleados del banco 3.- Ser sancionados por la SB por tener cuentas que pueden ser mal usadas

RIESGO 22	
Factor de Riesgo	Empleado
Actividad	Inicio relación comercial
Descripción del Riesgo de LA/FT	Asesor al cliente no carga documentos en el file digital de cliente
Riesgo Asociado	1 Operativo
	2 Legal
	3 Reputacional
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Asesor al cliente Asesor Senior Especialista de Banca Telefónica
Identificación de causas / vulnerabilidades	1.- Asesor al cliente omite el cumplimiento de las políticas y procedimientos del banco 2.- Asesor senior no da seguimiento de los casos asignados a los asesores al cliente 3.- Especialista de Banca Telefónica no da seguimiento a incidencias pendientes de cierre
Identificación de consecuencias	1.- Observaciones de auditoría interna y externa 2.- No contar con todos los documentos de sustento en el file del cliente 3.- Pérdida de documentos por no ser archivados a tiempo 4.- Incumplimiento de la normativa nacional por la cual puede ser sancionada la IFI

Fuente: Datos de la institución financiera
Elaboración propia

Anexo 2: Identificación de eventos de riesgo transacciones a través de ATM

RIESGO 1	
Factor de Riesgo	Cliente
Actividad	Ejecución de depósito
Descripción del Riesgo de LA/FT	Cliente deposita cheques que no cumplen con los requisitos de forma
Riesgo Asociado	1 Operativo
	2 Reputacional
	3 Contagio
	4 Legal
Responsable del proceso (Propietario del Riesgo)	Personal Externo Especialista de procesos centralizados
Identificación de causas / vulnerabilidades	1.- Cliente no se percató que el cheque no cumple con los requisitos de forma. 2.- Cliente desconoce de los requisitos que deben cumplir los cheques para ser válidos.
Identificación de consecuencias	1.- Que el depósito no se realice. 2.- En el caso de que el cliente considere ese dinero para sus finanzas no pueda ser acreditado dichos fondos en su cuenta, por los errores de forma del documento. 3.- Molestias en el cliente, pues enterarse que el cheque no cumple con los requisitos de forma no será inmediatamente como cuando depositaba en caja.

RIESGO 2	
Factor de Riesgo	Cliente
Actividad	Ejecución de depósito
Descripción del Riesgo de LA/FT	Cliente no adjunta formulario de licitud de fondos
Riesgo Asociado	1 Legal
	2 Reputacional
	3 Operativo
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Personal Externo Asesor al cliente Especialista procesos centralizados
Identificación de causas / vulnerabilidades	1.-No instruir a los clientes sobre los requisitos que debe cumplir para procesar el depósito. 2.-Cliente olvida adjuntar el formulario
Identificación de consecuencias	1.-No cumplir con la normativa local 2.-La institución financiera puede ser sancionada por no contar con los procesos y procedimientos adecuados para cumplir con la normativa nacional.

RIESGO 3	
Factor de Riesgo	Cliente
Actividad	Ejecución de depósito
Descripción del Riesgo de LA/FT	Cliente no llena correctamente el formulario de licitud de fondos
Riesgo Asociado	1 Legal
	2 Reputacional
	3 Operativo
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Personal Externo Asesor al cliente
Identificación de causas / vulnerabilidades	1.- No instruir a los clientes como llenar correctamente el formulario de licitud de fondos. 2.- Clientes no toman en consideración las instrucciones sobre como llenar el formulario 3.- Clientes no comprenden como llenar el formulario de licitud de fondos. 4.- Falta de costumbre en llenar el formulario de licitud de fondos.
Identificación de consecuencias	1.-No cumplir con la normativa local 2.-La institución financiera puede ser sancionada por no contar con los procesos y procedimientos adecuados para cumplir con la normativa nacional.

RIESGO 4	
Factor de Riesgo	Cliente
Actividad	Ejecución de depósito
Descripción del Riesgo de LA/FT	Cliente no regulariza formulario de licitud de fondos antes del segundo depósito
Riesgo Asociado	1 Legal
	2 Reputacional
	3 Operativo
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Asesor al cliente
Identificación de causas / vulnerabilidades	1.- No se realiza un seguimiento del caso por parte del asesor al cliente. 2.- El cliente no desea regularizar el formulario 3.- No se localiza al cliente
Identificación de consecuencias	1.-No cumplir con la normativa local 2.-La institución financiera puede ser sancionada por no contar con los procesos y procedimientos adecuados para cumplir con la normativa nacional.

RIESGO 5	
Factor de Riesgo	Cliente
Actividad	Ejecución de depósito
Descripción del Riesgo de LA/FT	No se acredita segundo depósito hasta que el cliente entregue licitud de fondos del primer depósito
Riesgo Asociado	1 Legal
	2 Reputacional
	3 Operativo
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Asesor al cliente Especialista de procesos centralizados
Identificación de causas / vulnerabilidades	1.- No se realiza un seguimiento del caso por parte del asesor al cliente. 2.- El cliente no desea regularizar el formulario 3.- Cliente no dispone de tiempo para regularizar el formulario
Identificación de consecuencias	1.-No cumplir con la normativa local 2.-La institución financiera puede ser sancionada por no contar con los procesos y procedimientos adecuados para cumplir con la normativa nacional. 3.-Cliente puede presentar queja ante la SB porque la institución no procesa su depósito. 4.-SB puede llamar la atención a la institución financiera por no contar con un proceso que evite que sea el cliente quien se vea perjudicado en sus transacciones.

RIESGO 6	
Factor de Riesgo	Cliente
Actividad	Ejecución de depósito
Descripción del Riesgo de LA/FT	Cliente deposita billetes falsos
Riesgo Asociado	1 Operativo
	2 Legal
	3 Reputacional
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Personal externo
Identificación de causas / vulnerabilidades	1.-Personal externo no cuenta con las destrezas para detectar billetes falsos. 2.-Personal externo no cuenta con las herramientas para detectar billetes falsos.
Identificación de consecuencias	1.-Sanciones a la institución financiera por no contar con los mecanismos adecuados para la identificación de billetes falsos.

RIESGO 7	
Factor de Riesgo	Cliente
Actividad	Ejecución de depósito
Descripción del Riesgo de LA/FT	Cliente no llena adecuadamente ficha de depósito
Riesgo Asociado	1 Operativo
	2 Legal
	3 Reputacional
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Asesor al cliente
Identificación de causas / vulnerabilidades	1.- No instruir a los clientes como llenar correctamente la ficha de depósito. 2.- Clientes no toman en consideración las instrucciones sobre como llenar la ficha de depósito. 3.- Clientes no comprenden como llenar la ficha de depósito. 4.- Falta de costumbre en llenar la ficha de depósito. 5.- Diseño del formulario de presta para confusiones
Identificación de consecuencias	1.-No cumplir con la normativa local 2.-La institución financiera puede ser sancionada por no contar con los procesos y procedimientos adecuados para cumplir con la normativa nacional.

RIESGO 8	
Factor de Riesgo	Canales de distribución
Actividad	Ejecución de depósito
Descripción del Riesgo de LA/FT	Cliente digita monto a depositar en cheque distinto al realmente depositado
Riesgo Asociado	1 Operativo
	2 Legal
	3 Reputacional
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Especialista de procesos centralizados
Identificación de causas / vulnerabilidades	1.-ATM no puede validar por si solo el valor del cheque, se requiere que el cliente lo registre. 2.-Cliente no diferencia ni registra adecuadamente la separación de miles y decimales. 3.-Cliente registra dolosamente un valor superior o diferente al del cheque. 4.-Registrar en el sistema el monto digitado por el cliente previo a la verificación del cheque.
Identificación de consecuencias	1.-Acreditar un valor diferente al realmente depositado. 2.-Realizar ajustes administrativos para corregir los valores en el sistema. 3.-Reportar en las estructuras que envía la institución a la SB transacciones que no son correctas. 4.-Sanciones de la SB por enviar estructuras con información inadecuada sobre las transacciones de los clientes.

RIESGO 9	
Factor de Riesgo	Canales de distribución
Actividad	Revisión de transacciones
Descripción del Riesgo de LA/FT	Cliente frecuentemente registra faltantes o sobrantes en sus depósitos
Riesgo Asociado	1 Operativo
	2 Reputacional
	3 Legal
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Personal externo. Especialista de procesos centralizados.
Identificación de causas / vulnerabilidades	1.-Cliente no está familiarizado con el proceso de depósitos a través de ATM's
Identificación de consecuencias	1.-No contar con la licitud de fondos por el monto correspondiente al sobrante. 1.-Incumplimiento de la normativa local 2.-La institución financiera puede ser sancionada por no contar con los procesos y procedimientos adecuados para cumplir con la normativa nacional.

RIESGO 10	
Factor de Riesgo	Empleado
Actividad	Revisión de transacciones
Descripción del Riesgo de LA/FT	Contratos para depositar a través de ATM montos \geq USD5,000.00 sin firma del cliente
Riesgo Asociado	1 Operativo
	2 Legal
	3 Reputacional
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Asesor al cliente Especialista de procesos centralizados
Identificación de causas / vulnerabilidades	1.-Especialista procesos centralizados active el servicio sin constatar previamente la firma del contrato. 2.-Complicidad del especialista de procesos centralizados con el cliente
Identificación de consecuencias	1.-Cliente empieza a transaccionar pese a que no firmó el contrato en donde acepta los términos y condiciones del servicio. 2.-La institución financiera puede ser sancionada por no contar con los procesos y procedimientos adecuados para cumplir con la normativa nacional.

RIESGO 11	
Factor de Riesgo	Canales de distribución
Actividad	Revisión de transacciones
Descripción del Riesgo de LA/FT	Acreditar monto señalado por el cliente sin comprobarlo, pues Administrador de ATM no alcanza a terminar el conteo en los cortes establecidos
Riesgo Asociado	1 Operativo
	2 Legal
	3 Reputacional
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Personal Externo Especialista de procesos centralizados
Identificación de causas / vulnerabilidades	1.-Existen muchos depósitos a esa hora y no se puede terminar con el conteo a tiempo
Identificación de consecuencias	1.-Acreditar un valor diferente al realmente depositado. 2.-Realizar ajustes administrativos para corregir los valores en el sistema. 3.-Reportar en las estructuras que envía la institución a la SB transacciones que no son correctas. 4.-Sanciones por parte de la SB por reportar estructuras idóneas

RIESGO 12	
Factor de Riesgo	Empleado
Actividad	Revisión de transacciones
Descripción del Riesgo de LA/FT	Administrador de ATM omite reportar sobrantes o faltantes
Riesgo Asociado	1 Operativo
	2 Legal
	3 Reputacional
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Especialista de procesos centralizados
Identificación de causas / vulnerabilidades	1.-Por la tensión de contar todos los depósitos a tiempo, omite reportar los sobrantes o faltantes. 2.-Dolosamente el empleado omite reportar sobrantes de dinero 3.-Para no perjudicar las transacciones del cliente, si el depósito ingresó en los horarios establecidos, pese a que el personal externo no concluya con el conteo se acredita el valor indicado por el cliente. 4.-Cliente no se percató que depositó un monto mayor al indicado en la ficha de depósito.
Identificación de consecuencias	1.-Fraudes internos 2.-Quejas de los clientes 3.-Sanciones de la SB por no contar con procesos y procedimientos adecuados para salvaguardar las transacciones de los clientes.

RIESGO 13	
Factor de Riesgo	Empleado
Actividad	Revisión de transacciones
Descripción del Riesgo de LA/FT	Administrador de ATM no firma la ficha de depósito como aceptación de los valores contados
Riesgo Asociado	1 Operativo
	2 Contagio
	3 Reputacional
	4 Legal
Responsable del proceso (Propietario del Riesgo)	Especialista de procesos centralizados
Identificación de causas / vulnerabilidades	1.-Por la tensión de contar todos los depósitos a tiempo, omite firmar la ficha de depósitos 2.-Especialista de procesos centralizados no valida que se encuentre la firma del responsable
Identificación de consecuencias	1.-Desconocer el responsable de procesar la transacción, en el caso de que presente alguna novedad con el depósito, no se podría validar directamente con el encargado y conocer las razones de estas novedades.

RIESGO 14	
Factor de Riesgo	Empleado
Actividad	Revisión de transacciones
Descripción del Riesgo de LA/FT	Formulario físico de licitud de fondos no se encuentra en la carpeta de la agencia
Riesgo Asociado	1 Operativo
	2 Legal
	3 Reputacional
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Personal externo Asesor al cliente senior Especialista de cumplimiento
Identificación de causas / vulnerabilidades	1.-Personal externo omite guardar el formulario en la carpeta física asignada. 2.-Asesor al cliente senior no revisa periódicamente que los formularios sean archivados. 3.-Especialista de cumplimiento no monitorea el proceso de archivo de licitudes de fondos.
Identificación de consecuencias	1.-No contar con la documentación soporte de la transacción para poder responder a requerimientos de los organismos de control. 2.-La institución financiera puede ser sancionada por no contar con los procesos y procedimientos adecuados para cumplir con la normativa nacional.

RIESGO 15	
Factor de Riesgo	Empleado
Actividad	Revisión de transacciones
Descripción del Riesgo de LA/FT	No se escanea el formulario de licitud de fondos
Riesgo Asociado	1 Operativo
	2 Legal
	3 Reputacional
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Personal externo Asesor al cliente senior Especialista de cumplimiento
Identificación de causas / vulnerabilidades	1.-Personal externo omite guardar el formulario en la carpeta digital asignada. 2.-Asesor al cliente senior no revisa periódicamente que los formularios sean archivados en la carpeta digital. 3.-Especialista de cumplimiento no monitorea el proceso de archivo de licitudes de fondos.
Identificación de consecuencias	1.-No contar con la documentación soporte de la transacción para poder responder a requerimientos de los organismos de control. 2.-La institución financiera puede ser sancionada por no contar con los procesos y procedimientos adecuados para cumplir con la normativa nacional.

RIESGO 16	
Factor de Riesgo	Empleado
Actividad	Revisión de transacciones
Descripción del Riesgo de LA/FT	Especialista de procesos centralizados omite notificar sobrantes al cliente
Riesgo Asociado	1 Contagio
	2 Operativo
	3 Legal
	4 Reputacional
Responsable del proceso (Propietario del Riesgo)	Especialista de procesos centralizados
Identificación de causas / vulnerabilidades	1.-Personal externo no reporta el sobrante 2.-Cliente no ha presentado un reclamo
Identificación de consecuencias	1.-Fraudes internos 2.-Quejas de los clientes 3.-Sanciones de la SB por no contar con procesos y procedimientos adecuados para salvaguardar las transacciones de los clientes.

RIESGO 17	
Factor de Riesgo	Empleado
Actividad	Revisión de transacciones
Descripción del Riesgo de LA/FT	Entregar material para depósito en ATM montos \geq USD5,000.00 sin firma de acta entrega recepción
Riesgo Asociado	1 Operativo
	2 Contagio
	3 Legal
	4 Reputacional
Responsable del proceso (Propietario del Riesgo)	Asesor al cliente
Identificación de causas / vulnerabilidades	1.-Desconocimiento del proceso 2.-Falta de capacitación a personal nuevo 3.-Complicidad del empleado con el cliente 4.-Anteponer el cumplimiento de metas a los controles
Identificación de consecuencias	1.-La entidad no cuenta con sustento legal para demostrar que el cliente es quien efectúa las transacciones con el material proporcionado por la institución. Pues el cliente puede alegar que nunca a recibido el material y él no es quien efectúa las transacciones.

RIESGO 18	
Factor de Riesgo	Empleado
Actividad	Revisión de transacciones
Descripción del Riesgo de LA/FT	No eliminar la exoneración anual del sistema cuando ya cumplió el año de vigencia
Riesgo Asociado	1 Operativo
	2 Legal
	3 Reputacional
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Especialista de procesos centralizados Especialista de cumplimiento
Identificación de causas / vulnerabilidades	1.-Seguimiento manual del vencimiento de la exoneración lo que puede provocar omisión 2.-Cambio de personal lo que puede provocar el desconocimiento de las exoneraciones próximas a vencerse.
Identificación de consecuencias	1.-No realizar un seguimiento a la razonabilidad de los ingresos del cliente. 2.-No realizar un nuevo análisis del cliente. 3.-Evitar detectar señales de alerta 4.-La institución podría ser objeto de sanción por no contar con procesos y procedimientos de control adecuados.

RIESGO 19	
Factor de Riesgo	Productos/Servicios
Actividad	Revisión de transacciones
Descripción del Riesgo de LA/FT	Depósito en Ecuador e inmediato retiro de fondos en el exterior a través de tarjeta de débito
Riesgo Asociado	1 Operativo
	2 Legal
	3 Reputacional
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Asesor al cliente Especialista de canales electrónicos Oficial de Cumplimiento
Identificación de causas / vulnerabilidades	1.-No existen límites para depósitos diarios 2.-Sistema de monitoreo no identifica depósitos y retiros inmediatos 3.-Sistema de monitoreo no identifica retiros en el exterior
Identificación de consecuencias	1.-Ingreso de fondos ilícitos a través de la tipología de Pitufeo 2.-Sanciones por no contar con los sistemas adecuados para monitorear transacciones inusuales.

RIESGO 20	
Factor de Riesgo	Cliente
Actividad	Revisión de transacciones
Descripción del Riesgo de LA/FT	No disponer con la documentación de respaldo e información de las transacciones efectuadas por el cliente, cuando el organismo de control lo solicite
Riesgo Asociado	1 Operativo
	2 Legal
	3 Reputacional
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Asesor al cliente Especialista de procesos centralizados
Identificación de causas / vulnerabilidades	1.-No identificar al depositante porque no se solicita número de documento de identidad del mismo, solo se toma como tal al dueño del código de depósito. 2.-No disponer de un sistema de almacenamiento de documentos general. Cada responsable archiva en sus carpetas compartidas los documentos de su competencia.
Identificación de consecuencias	1.-No responder a tiempo incluso no poder enviar la documentación e información requerida porque no se cuenta con ella. 2.-La institución puede ser objeto de sanciones por no contar con un archivo adecuado de la información y documentación como lo determina la normativa.

RIESGO 21	
Factor de Riesgo	Cliente
Actividad	Uso de material de depósito
Descripción del Riesgo de LA/FT	Cliente con frecuente reporte de pérdidas, sustracción o deterioro de tarjeta de seguridad y material para depósito
Riesgo Asociado	1 Contagio
	2 Operativo
	3 Legal
	4 Reputacional
Responsable del proceso (Propietario del Riesgo)	Asesor al cliente Especialista de procesos centralizados
Identificación de causas / vulnerabilidades	1.-No existen límites para la entrega de material.
Identificación de consecuencias	1.-Entrega de material a terceras personas para efectuar depósitos

RIESGO 22	
Factor de Riesgo	Cliente
Actividad	Uso de material de depósito
Descripción del Riesgo de LA/FT	Cliente con petición frecuente de material extra
Riesgo Asociado	1 Operativo
	2 Contagio
	3 Legal
	4 Reputacional
Responsable del proceso (Propietario del Riesgo)	Asesor al cliente Especialista de procesos centralizados
Identificación de causas / vulnerabilidades	1.-Desconocer la transaccionalidad del cliente de tal manera que no se puede proporcionar el material necesario para sus transacciones.
Identificación de consecuencias	1.-Entrega de material a terceras personas para efectuar depósitos

RIESGO 23	
Factor de Riesgo	Empleado
Actividad	Uso de material de depósito
Descripción del Riesgo de LA/FT	Cliente con varias tarjetas de débito activas.
Riesgo Asociado	1 Operativo
	2 Legal
	3 Reputacional
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Asesor al cliente Especialista de procesos centralizados
Identificación de causas / vulnerabilidades	1.-No se aplican los límites establecidos para otorgar tarjetas de débito. 2.-Asesor al cliente y especialista de procesos centralizados no verifican cuantas tarjetas activas posee el clientes antes de solicitar y entregar una nueva. 3.-Asesor al cliente y especialista de procesos centralizados no desactivan la tarjeta anterior. 4.-No se consulta al cliente la razón por la cual se solicita una nueva tarjeta y el motivo para mantener la anterior o anteriores activas.
Identificación de consecuencias	1.-Las tarjetas de débito pueden ser mal usadas, pues pueden ser destinadas a varias personas en distintos lugares. 2.-Facilita que sean terceras personas quienes manejen la cuenta del cliente. 3.-La institución puede ser sancionada por no contar con procesos y procedimientos adecuados.

RIESGO 24	
Factor de Riesgo	Empleado
Actividad	Uso de material de depósito
Descripción del Riesgo de LA/FT	Cliente con varios códigos de depósito activos.
Riesgo Asociado	1 Operativo
	2 Legal
	3 Reputacional
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Asesor al cliente Especialista de procesos centralizados
Identificación de causas / vulnerabilidades	1.-Personal desconoce donde verificar si un código de depósito está activo 2.-No hay límites para códigos de depósito 3.-Por el tiempo que toma en elaborar la tarjeta al inicio de la relación comercial otorgan tarjeta de débito y código de depósito. 4.-Una vez que llega la tarjeta de débito no desactiva el código de depósito. 5.-Antes de otorgar un nuevo código de depósito no se verifica si ya tiene otro (s) activos 6.-No se consulta al cliente la razón para mantener más de un código de depósito activo
Identificación de consecuencias	1.-Terceras personas pueden efectuar depósitos en la cuenta del cliente sin ser identificados, solo con conocer el código de depósito del cliente. 2.-Facilita que sean terceras personas quienes manejen la cuenta del cliente "Testaferro". 3.-Ingreso de dinero ilícito a la institución 4.-La institución puede ser sancionada por no contar con procesos y procedimientos de control adecuados.

RIESGO 25	
Factor de Riesgo	Empleado
Actividad	Uso de material de depósito
Descripción del Riesgo de LA/FT	NO clientes con más de un código de depósito activos
Riesgo Asociado	1 Operativo
	2 Legal
	3 Reputacional
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Asesor al cliente Especialista de procesos centralizados
Identificación de causas / vulnerabilidades	1.-Personal desconoce donde verificar si un código de depósito está activo 2.-No hay límites para códigos de depósito. 3.-Antes de otorgar un nuevo código de depósito no se verifica si ya tiene otro (s) activos 4.-No se consulta al NO cliente la razón para mantener más de un código de depósito activo
Identificación de consecuencias	1.-Terceras personas pueden efectuar depósitos en la cuenta del cliente sin ser identificados, solo con conocer el código de depósito del NO cliente. 2.-Facilita que sean terceras personas quienes manejen la cuenta del cliente "Testaferro". 3.-Ingreso de dinero ilícito a la institución 4.-La institución puede ser sancionada por no contar con procesos y procedimientos de control adecuados.

RIESGO 26	
Factor de Riesgo	Empleado
Actividad	Uso de material de depósito
Descripción del Riesgo de LA/FT	Clientes con más de un código de depósito y una tarjeta activos.
Riesgo Asociado	1 Operativo
	2 Legal
	3 Reputacional
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Asesor al cliente Especialista de procesos centralizados
Identificación de causas / vulnerabilidades	1.-No se aplican los límites establecidos para otorgar tarjetas de débito. 2.-Personal desconoce donde verificar si un código de depósito está activo 3.-No hay límites para códigos de depósito 4.-Por el tiempo que toma en elaborar la tarjeta al inicio de la relación comercial otorgan tarjeta de débito y código de depósito. 5.-Una vez que llega la tarjeta de débito no desactiva el código de depósito. 6.-Antes de otorgar un nuevo código de depósito o tarjeta de débito no se verifica si ya tiene otro (s) activos 7.-No se consulta al cliente la razón para mantener más de un código de depósito o tarjeta de débito activos. 8.-Asesor al cliente y especialista de procesos centralizados no desactivan la tarjeta anterior
Identificación de consecuencias	1.-Terceras personas pueden efectuar depósitos en la cuenta del cliente sin ser identificados, solo con conocer el código de depósito o tener una tarjeta de débito. 2.-Facilita que sean terceras personas quienes manejen la cuenta del cliente "Testaferro". 3.-Ingreso de dinero ilícito a la institución 4.-La institución puede ser sancionada por no contar con procesos y procedimientos de control adecuados.

RIESGO 27	
Factor de Riesgo	Productos/Servicios
Actividad	Uso de material de depósito
Descripción del Riesgo de LA/FT	Manejo de un mismo código de depósito por diferentes personas
Riesgo Asociado	1 Operativo
	2 Legal
	3 Reputacional
	4 Contagio
Responsable del proceso (Propietario del Riesgo)	Especialista canales electrónicos Gerencia
Identificación de causas / vulnerabilidades	1.-No tiene límite de duración 2.-No puede ser identificado por el sistema de monitoreo
Identificación de consecuencias	1.-Terceras personas pueden efectuar depósitos en la cuenta del cliente sin ser identificados, solo con conocer el código de depósito. 2.-Facilita que sean terceras personas quienes manejen la cuenta del cliente "Testaferro". 3.-Ingreso de dinero ilícito a la institución 4.-La institución puede ser sancionada por no contar con procesos y procedimientos de control adecuados.

RIESGO 28	
Factor de Riesgo	Cliente
Actividad	Uso de material de depósito
Descripción del Riesgo de LA/FT	Cliente solicita varios códigos de retiro en varias agencias
Riesgo Asociado	1 Contagio
	2 Operativo
	3 Legal
	4 Reputacional
Responsable del proceso (Propietario del Riesgo)	Asesor al cliente Especialista de procesos centralizados
Identificación de causas / vulnerabilidades	1.-Personal desconoce donde verificar si un código de depósito está activo 2.-Antes de otorgar un nuevo código de depósito no se verifica si ya tiene otro (s) activos 3.-No se consulta al cliente la razón para mantener más de un código de depósito activo
Identificación de consecuencias	1.-Facilita que sean terceras personas quienes manejen la cuenta del cliente "Testaferro". 2.-Ingreso de dinero ilícito a la institución 3.-La institución puede ser sancionada por no contar con procesos y procedimientos de control adecuados.

Fuente: Datos de la institución financiera
Elaboración propia

Anexo 3: Cálculo de probabilidades apertura cuenta online

Nro.	EVENTOS	Resultado favorable	Resultados posibles	Probabilidad Porcentaje
1	La carga de las listas de restricción no se efectúe correctamente	15	52	28.77%
2	Persona que consta en listas de restricción abre cuenta	1	38740	0.00%
3	Empresa fachada o empresa de papel abre cuenta online	1	1160	0.09%
4	Persona que se dedica a actividades económicas con las cuales el banco ha decidido no trabajar abre cuenta online	1	673	0.15%
5	PEP abre cuenta sin ser identificado	1	4	25.00%
6	Persona jurídica que no proporciona total o parcialmente información de sus beneficiarios finales abre cuenta online	1	8	12.50%
7	PEP que no proporciona información sobre su actividad económica y origen de fondos abre cuenta online	2	108	1.85%
8	Solicitante que proporciona información falsa abre cuenta on line	0	673	0.00%
9	No verificar la información en páginas oficiales como: función judicial y listas de restricción	12	673	1.78%
10	No verificar la información registrada por el solicitante con la referencia	126	673	18.72%
11	Incorrecto registro de información en el sistema	8	673	1.19%
12	No solicitar autorización a Jefe de Agencia para vincular a cliente con negocio de menos de un año de funcionamiento	0	673	0.00%
13	No solicitar autorización a Jefe de Agencia para vincular a cliente con ingresos mensuales superiores a los	0	673	0.00%
14	No solicitar autorización de la Gerencia por ser un cliente de alto riesgo	2	673	0.30%
15	No solicitar autorización de la Gerencia para vincular a un cliente PEP	1	4	25.00%
16	Abrir la cuenta pese a que no se cuenta con la información requerida	0	673	0.00%
17	Una vez abierta la cuenta el cliente cambia de domicilio a una jurisdicción lejana lo cual dificulta su seguimiento.	64	16460	0.39%
18	Entrega de tarjeta de débito y número de cuenta sin que el cliente haya firmado el contrato	3	673	0.45%
19	No identificar que la cuenta no es para el cliente, sino para ser usada por un tercero.	39	802	4.86%
20	No validar que el solicitante sea quien dijo ser	0	673	0.00%
21	Cliente no se acerca a regularizar la apertura de cuenta	18	673	2.67%
22	Asesor al cliente no guarda los documentos en el file digital de cliente	16	673	2.38%

Fuente: Datos de la institución financiera
Elaboración propia

Anexo 4: Cálculo de probabilidades transacciones a través de ATM

Nro.	EVENTOS	Resultado favorable	Resultados posibles	Probabilidad Porcentaje
1	Cliente deposita cheques que no cumplen con los requisitos de forma	5	40	12.50%
2	Cliente no adjunta formulario de licitud de fondos	0	40	0.00%
3	Cliente no llena correctamente el formulario de licitud de fondos	5	21	23.81%
4	Cliente no regulariza formulario de licitud de fondos antes del segundo depósito	2	21	9.52%
5	No se acredita segundo depósito hasta que el cliente entregue licitud de fondos del primer depósito	1	21	4.76%
6	Cliente deposita billetes falsos	4	40	10.00%
7	Cliente no llena adecuadamente ficha de depósito	2	40	5.00%
8	Cliente digita monto a depositar en cheque distinto al realmente depositado	248	134,110	0.18%
9	Cliente frecuentemente registra faltantes o sobrantes en sus depósitos	2	40	5.00%
10	Contratos para depositar a través de ATM montos \geq USD5,000.00 sin firma del cliente	0	40	0.00%
11	Acreditar monto señalado por el cliente sin comprobarlo, pues Administrador de ATM no alcanza a terminar el conteo en los cortes establecidos	2	40	5.00%
12	Administrador de ATM omite reportar sobrantes o faltantes	0	40	0.00%
13	Administrador de ATM no firma la ficha de depósito como aceptación de los valores contados	2	40	5.00%
14	Formulario físico de licitud de fondos no se encuentra en la carpeta de la agencia	0	21	0.00%
15	No se escanea el formulario de licitud de fondos	0	21	0.00%
16	Especialista de procesos centralizados omite notificar sobrantes al cliente	0	40	0.00%
17	Entregar material para depósito en ATM montos \geq USD5,000.00 sin firma de acta entrega recepción	0	40	0.00%
18	No eliminar la exoneración anual del sistema cuando ya cumplió el año de vigencia	3	21	14.29%
19	Depósito en Ecuador e inmediato retiro de fondos en el exterior a través de tarjeta de débito	6	39,900	0.02%
20	No disponer con la documentación de respaldo e información de las transacciones efectuadas por el cliente, cuando el organismo de control lo solicite	0	39,900	0.00%
21	Cliente con frecuente reporte de pérdidas, sustracción o deterioro de tarjeta de seguridad y material para depósito	2	40	5.00%
22	Cliente con petición frecuente de material extra	1	40	2.50%
23	Cliente con varias tarjetas de débito activas.	138	19,966	0.69%
24	Cliente con varios códigos de depósito activos.	1,056	6,474	16.31%
25	NO clientes con más de un código de depósito activo	515	8,947	5.76%
26	Clientes con más de un código de depósito y una tarjeta activos.	880	4,052	21.72%
27	Manejo de un mismo código de depósito por diferentes personas	7	15,421	0.05%
28	Cliente solicita varios códigos de retiro en varias agencias	426	15,421	2.76%

Fuente: Datos de la institución financiera
Elaboración propia

Anexo 5: Cálculo del impacto del evento de riesgo de LA/FT apertura cuentas online

Nro.	EVENTOS	RL 40%	RR 30%	RO 20%	RC 10%	40%	30%	20%	10%	Impacto
1	La carga de las listas de restricción no se efectúe correctamente	5	5	5	3	2.0	1.5	1.0	0.3	4.8
2	Persona que consta en listas de restricción abre cuenta online	5	5	5	2	2.0	1.5	1.0	0.2	4.7
3	Empresa fachada o empresa de papel abre cuenta online	5	5	5	2	2.0	1.5	1.0	0.2	4.7
4	Persona que se dedica a actividades económicas con las cuales el banco ha decidido no trabajar abre cuenta online	1	2	2	2	0.4	0.6	0.4	0.2	1.6
5	PEP abre cuenta sin ser identificado	4	3	2	2	1.6	0.9	0.4	0.2	3.1
6	Persona jurídica que no proporciona total o parcialmente información de sus beneficiarios finales abre cuenta online	4	3	2	2	1.6	0.9	0.4	0.2	3.1
7	PEP que no proporciona información sobre su actividad económica y origen de fondos abre cuenta online	3	2	2	2	1.2	0.6	0.4	0.2	2.4
8	Solicitante que proporciona información falsa abre cuenta on line	4	3	5	2	1.6	0.9	1.0	0.2	3.7
9	No verificar la información en páginas oficiales como: función judicial y listas de restricción	5	3	4	3	2.0	0.9	0.8	0.3	4.0
10	No verificar la información registrada por el solicitante con la referencia	5	3	4	3	2.0	0.9	0.8	0.3	4.0
11	Incorrecto registro de información en el sistema	4	2	5	2	1.6	0.6	1.0	0.2	3.4
12	No solicitar autorización a Jefe de Agencia para vincular a cliente con negocio de menos de un año de funcionamiento	3	1	2	3	1.2	0.3	0.4	0.3	2.2
13	No solicitar autorización a Jefe de Agencia para vincular a cliente con ingresos mensuales superiores a los 100,000.00	3	1	2	3	1.2	0.3	0.4	0.3	2.2
14	No solicitar autorización de la Gerencia por ser un cliente de alto riesgo	3	1	2	3	1.2	0.3	0.4	0.3	2.2
15	No solicitar autorización de la Gerencia para vincular a un cliente PEP	3	1	2	3	1.2	0.3	0.4	0.3	2.2
16	Abrir la cuenta pese a que no se cuenta con la información requerida	4	2	2	3	1.6	0.6	0.4	0.3	2.9
17	Una vez abierta la cuenta el cliente cambia de domicilio a una jurisdicción lejana lo cual dificulta su seguimiento.	2	1	1	2	0.8	0.3	0.2	0.2	1.5
18	Entrega de tarjeta de débito y número de cuenta sin que el solicitante haya firmado el contrato	5	5	5	3	2.0	1.5	1.0	0.3	4.8
19	No identificar que la cuenta no es para el cliente, sino para ser usada por un tercero.	5	5	5	3	2.0	1.5	1.0	0.3	4.8
20	No validar que el solicitante sea quien dijo ser	5	5	4	3	2.0	1.5	0.8	0.3	4.6
21	Solicitante no se acerca a regularizar la apertura de cuenta	5	4	4	2	2.0	1.2	0.8	0.2	4.2
22	Asesor al cliente no guarda los documentos en el file digital de cliente	4	1	2	2	1.6	0.3	0.4	0.2	2.5

Fuente: Datos de la institución financiera
Elaboración propia

Anexo 6: Cálculo del impacto del evento de riesgo de LA/FT uso de ATM

Nro	EVENTOS	RL 40%	RR 30%	RO 20%	RC 10%	40%	30%	20%	10%	Impacto
1	Cliente deposita cheques que no cumplen con los requisitos de forma	1	1	1	2	0.4	0.3	0.2	0.2	1.10
2	Cliente no adjunta formulario de licitud de fondos	2	1	1	2	0.8	0.3	0.2	0.2	1.50
3	Cliente no llena correctamente el formulario de licitud de fondos	1	1	1	2	0.4	0.3	0.2	0.2	1.10
4	Cliente no regulariza formulario de licitud de fondos antes del segundo depósito	2	1	1	2	0.8	0.3	0.2	0.2	1.50
5	No se acredita segundo depósito hasta que el cliente entregue licitud de fondos del primer depósito	1	1	1	2	0.4	0.3	0.2	0.2	1.10
6	Cliente deposita billetes falsos	2	1	1	2	0.8	0.3	0.2	0.2	1.50
7	Cliente no llena adecuadamente ficha de depósito	1	1	1	2	0.4	0.3	0.2	0.2	1.10
8	Cliente digita monto a depositar en cheque distinto al realmente depositado	3	4	3	2	1.2	1.2	0.6	0.2	3.20
9	Cliente frecuentemente registra faltantes o sobrantes en sus depósitos	1	1	1	2	0.4	0.3	0.2	0.2	1.10
10	Contratos para depositar a través de ATM montos \geq USD5,000.00 sin firma del cliente	3	3	4	3	1.2	0.9	0.8	0.3	3.20
11	Acreditar monto señalado por el cliente sin comprobarlo, pues Administrador de ATM no alcanza a terminar el conteo en los cortes establecidos	3	3	4	3	1.2	0.9	0.8	0.3	3.20
12	Administrador de ATM omite reportar sobrantes o faltantes	2	1	1	3	0.8	0.3	0.2	0.3	1.60
13	Administrador de ATM no firma la ficha de depósito como aceptación de los valores contados	1	1	1	3	0.4	0.3	0.2	0.3	1.20
14	Formulario físico de licitud de fondos no se encuentra en la carpeta de la agencia	1	1	1	3	0.4	0.3	0.2	0.3	1.20
15	No se escanea el formulario de licitud de fondos	1	1	1	3	0.4	0.3	0.2	0.3	1.20
16	Especialista de procesos centralizados omite notificar sobrantes al cliente	2	1	1	3	0.8	0.3	0.2	0.3	1.60
17	Entregar material para depósito en ATM montos \geq USD5,000.00 sin firma de acta entrega recepción	1	1	1	3	0.4	0.3	0.2	0.3	1.20
18	No eliminar la exoneración anual del sistema cuando ya cumplió el año de vigencia	2	2	3	3	0.8	0.6	0.6	0.3	2.30
19	Depósito en Ecuador e inmediato retiro de fondos en el exterior a través de tarjeta de débito sin que sea identificado	5	4	5	3	2.0	1.2	1.0	0.3	4.50
20	No disponer con la documentación de respaldo e información de las transacciones efectuadas por el cliente, cuando el organismo de control lo solicite	5	4	4	3	2.0	1.2	0.8	0.3	4.30
21	Cliente con frecuente reporte de pérdidas, sustracción o deterioro de tarjeta de seguridad y material para depósito	1	1	1	2	0.4	0.3	0.2	0.2	1.10
22	Cliente con petición frecuente de material extra	1	1	1	2	0.4	0.3	0.2	0.2	1.10
23	Cliente con varias tarjetas de débito activas.	5	4	5	3	2.0	1.2	1.0	0.3	4.50
24	Cliente con varios códigos de depósito activos.	5	4	5	3	2.0	1.2	1.0	0.3	4.50
25	NO clientes con más de un código de depósito activo	5	4	5	3	2.0	1.2	1.0	0.3	4.50
26	Clientes con más de un código de depósito y una tarjeta activos.	5	4	5	3	2.0	1.2	1.0	0.3	4.50
27	Manejo de un mismo código de depósito por diferentes personas	5	4	5	2	2.0	1.2	1.0	0.2	4.40
28	Cliente solicita varios códigos de retiro en varias agencias	4	2	4	2	1.6	0.6	0.8	0.2	3.20

Fuente: Datos de la institución financiera
Elaboración propia

Anexo 7: Cálculo de la efectividad de los controles apertura cuenta online

Código de Riesgo	Descripción del Riesgo	Factor de Riesgo	Controles existentes	Análisis de controles			Efectividad
				Naturaleza de control	Automatización	Frecuencia	
RIESGO 1	La carga de las listas no es correcta	Empleado	Cada lunes el especialista de cumplimiento valida una muestra de personas que constan en la lista de restricción para verificar que el sistema los busque.	Detectivo	Manual	Periodico	2
RIESGO 2	Persona que consta en listas de restricción abre cuenta online	Ciente	1.- Los viernes el sistema a las 4pm valida que estén los archivos de las listas de restricción y envía un correo informativo a TI y Unidad de Cumplimiento. 2.- Antes de otorgar el producto/servicio el sistema muestra un mensaje si el cliente está en listas de restricción	Preventivo	Automático	Permanente	5
RIESGO 3	Empresa fachada o empresa de papel abre cuenta online	Ciente	1.- Cargar el listado de empresas fachada al sistema 2.- Capacitaciones anuales para personal permanente y al momento de su ingreso para personal nuevo sobre la importancia de la aplicación de procesos y política de PLA/FT.	Preventivo	Manual	Periodico	3
RIESGO 4	Persona que se dedica a actividades con las cuales el banco no trabaja abre cuenta online	Ciente	El asesor al cliente antes de ir a su cargo tiene 3 meses de capacitación tiempo en el cual también debe leer los manuales.	Preventivo	Manual	Periodico	3
RIESGO 5	PEP abre cuenta sin ser identificado	Ciente	1.- El sistema al cierre del scoring valida a los clientes contra las listas de PEP's 2.- A fin de mes el especialista de cumplimiento solicita un listado de clientes vinculados en ese mes y valida que si son PEP's estén marcados como tal en el sistema.	Detectivo	Semiautomático	Permanente	2
RIESGO 6	Persona jurídica que no proporciona total o parcialmente información de sus beneficiarios finales abre cuenta online	Ciente	No pasan la revisión de UBOS que efectúa el especialista de cumplimiento.	Correctivo	Manual	Permanente	3
RIESGO 7	PEP que no proporciona mayor información sobre sus actividades y origen de fondos abre cuenta online	Ciente	El asesor al cliente antes de ir a su cargo tiene 3 meses de capacitación tiempo en el cual también debe leer los manuales.	Preventivo	Manual	Periodico	3
RIESGO 8	Solicitante que proporciona información falsa abre cuenta on line	Ciente	Especialista de procesos centralizados verifica que la información sea coherente con la documentación, que esté vigente y la compara con páginas oficiales SRI, CNT, SB etc.	Correctivo	Manual	Permanente	3
RIESGO 9	No verificar la información en páginas oficiales, función judicial y listas de restricción	Empleado	Especialista de procesos centralizados da dos días para regularizar observaciones, caso contrario rechaza la incidencia	Correctivo	Manual	Permanente	3

RIESGO 10	No verificar la información registrada por el solicitante con la referencia	Empleado	No hay	No determinado	No determinado	No determinado	0
RIESGO 11	Incorrecto registro de información en el sistema	Empleado	No hay	No determinado	No determinado	No determinado	0
RIESGO 12	No solicitar autorización Jefe de Agencia para cliente con negocio de menos de un año de funcionamiento	Empleado	No pasan la revisión de UBOS que efectúa el especialista de cumplimiento.	Correctivo	Manual	Permanente	3
RIESGO 13	No solicitar autorización Jefe de Agencia para cliente con ingresos mensuales superiores a los 100,000.00	Empleado	No pasan la revisión de UBOS que efectúa el especialista de cumplimiento.	Correctivo	Manual	Permanente	3
RIESGO 14	No solicitar autorización de la Gerencia por ser un cliente de alto riesgo	Empleado	No hay	No determinado	No determinado	No determinado	0
RIESGO 15	No solicitar autorización de la Gerencia para vincular a un cliente PEP	Empleado	A fin de mes el especialista de cumplimiento solicita un listado de clientes vinculados en ese mes y valida que si son PEP's estén marcados como tal en el sistema.	Detectivo	Manual	Periodico	2
RIESGO 16	Abrir la cuenta pese a que no se cuenta con la información requerida	Empleado	No hay	No determinado	No determinado	No determinado	0
RIESGO 17	Una vez abierta la cuenta el cliente cambia de domicilio a una jurisdicción lejana lo cual dificulta su verificación.	Jurisdicción	No hay	No determinado	No determinado	No determinado	0
RIESGO 18	Entregar tarjeta de débito y número de cuenta sin que el cliente haya firmado el contrato	Empleado	No hay	No determinado	No determinado	No determinado	0
RIESGO 19	No identificar que la cuenta no es para el cliente, sino para ser usada por un tercero.	Empleado	El asesor al cliente antes de ir a su cargo tiene 3 meses de capacitación tiempo en el cual también debe leer los manuales.	Preventivo	Manual	Periodico	3
RIESGO 20	No validar que el solicitante sea quien dijo ser	Empleado	Todos los solicitantes deben acercarse a la agencia o ser visitados por el asesor	Correctivo	Manual	Permanente	3
RIESGO 21	Cliente no se acerca a regularizar la apertura	Cliente	Cada mes se envía a cerrar estas cuentas	Correctivo	Manual	Periodico	3
RIESGO 22	Asesor al cliente no carga documentos en el file digital de cliente	Empleado	1.-Especialista de banca telefónica continuamente está dando seguimiento a la carga de contratos 2.- Asesor senior realiza arqueo de cuentas y valida que estén cargados todos los documentos para considerarlo como completo y cerrar la incidencia	Correctivo	Manual	Periodico	3

Fuente: Datos de la institución financiera
Elaboración propia

Anexo 8: Cálculo de la efectividad de los controles en el uso de ATM

Código de Riesgo	Descripción del Riesgo	Factor de Riesgo	Controles existentes	Análisis de controles			Efectividad
				Naturaleza de control	Automatización	Frecuencia	
RIESGO 1	Cliente deposita cheques que no cumplen con los requisitos de forma	Cliente	El cheque no se deposita se devuelve al cliente.	Preventivo	Manual	Permanente	3
RIESGO 2	Cliente no adjunta formulario de licitud de fondos	Cliente	Administrador de ATM al momento de efectuar el conteo del dinero, valida que esté el documento, si no está lo reporta en el campo de observaciones para que el asesor al cliente lo regularice antes del segundo depósito.	Detectivo	Manual	Permanente	2
RIESGO 3	Cliente no llena correctamente el formulario de licitud de fondos	Cliente	Previo efectuar el segundo depósito el cliente debe regularizar la licitud de fondos.	Preventivo	Manual	Permanente	3
RIESGO 4	Cliente no regulariza formulario de licitud de fondos antes del segundo depósito	Cliente	No se procesa el depósito.	Preventivo	Manual	Permanente	3
RIESGO 5	No se acredita segundo depósito hasta que el cliente entregue licitud de fondos del primer depósito	Cliente	Si es un cliente que en reiteradas ocasiones no ha regularizado el formulario se cancela el servicio.	Detectivo	Manual	Permanente	2
RIESGO 6	Cliente deposita billetes falsos	Cliente	Administrador de ATM identifica billetes falsos antes de registrar el depósito.	Preventivo	Manual	Permanente	3
RIESGO 7	Cliente no llena adecuadamente ficha de depósito	Cliente	No se procesa el depósito.	Preventivo	Manual	Permanente	3
RIESGO 8	Cliente digita monto a depositar en cheque distinto al realmente depositado	Canales de distribución	Especialista de procesos centralizados verifica el cheque y valor digitado, corrige el valor y procesa.	Correctivo	Manual	Permanente	3
RIESGO 9	Cliente frecuentemente registra faltantes o sobrantes en sus depósitos	Canales de distribución	Es una causa para cancelar el contrato.	Detectivo	Manual	Permanente	2
RIESGO 10	Contratos para depositar a través de ATM montos \geq USD5,000.00 sin firma del cliente	Empleado	Especialista de procesos centralizados valida que todos los documentos estén regularizados previo activar la tarjeta de seguridad.	Preventivo	Manual	Permanente	3
RIESGO 11	Acreditar monto señalado por el cliente sin comprobarlo, pues Administrador de ATM no alcanza a terminar el conteo en los cortes establecidos	Canales de distribución	Una vez concluido el conteo de valores se compara con lo acreditado y de no ser correcto el valor se realizan los ajustes correspondientes.	Detectivo	Manual	Permanente	2
RIESGO 12	Administrador de ATM omite reportar sobrantes o faltantes	Empleado	No existe control	No determinado	No determinado	No determinado	0
RIESGO 13	Administrador de ATM no firma la ficha de depósito como aceptación de los valores contados	Empleado	Especialista de procesos centralizados revisa la ficha y solicita la firma del responsable si no lo está.	Correctivo	Manual	Permanente	3
RIESGO 14	Formulario físico de licitud de fondos no se encuentra en la carpeta de la agencia	Empleado	Asesor senior revisa que los formularios estén en la carpeta.	Detectivo	Manual	Periodico	2

RIESGO 15	No se escanea el formulario de licitud de fondos	Empleado	Asesor senior revisa que los formularios estén escaneados.	Detectivo	Manual	Periodico	2
RIESGO 16	Especialista de procesos centralizados omite notificar sobrantes al cliente	Empleado	No existe control	No determinado	No determinado	No determinado	0
RIESGO 17	Entregar material para depósito en ATM montos \geq USD5,000.00 sin firma de acta entrega recepción	Empleado	Mientras no recibe el contrato, acta y todos los documentos habilitantes firmados por el cliente el EPC no habilita el servicio.	Preventivo	Manual	Permanente	3
RIESGO 18	No eliminar la exoneración anual del sistema cuando ya cumplió el año de vigencia	Empleado	No existe control	No determinado	No determinado	No determinado	0
RIESGO 19	Depósito en Ecuador e inmediato retiro de fondos en el exterior a través de tarjeta de débito sin que sea identificado	Productos/ Servicios	No existe control	No determinado	No determinado	No determinado	0
RIESGO 20	No disponer con la documentación de respaldo e información de las transacciones efectuadas por el cliente, cuando el organismo de control lo solicite	Cliente	No existe control	No determinado	No determinado	No determinado	0
RIESGO 21	Cliente con frecuente reporte de pérdidas, sustracción o deterioro de tarjeta de seguridad y material para depósito	Cliente	Se desactiva la tarjeta de seguridad cuando pide una nueva.	Preventivo	Manual	Permanente	3
RIESGO 22	Cliente con petición frecuente de material extra	Cliente	No existe control	No determinado	No determinado	No determinado	0
RIESGO 23	Cliente con varias tarjetas de débito activas.	Empleado	No existe control	No determinado	No determinado	No determinado	0
RIESGO 24	Cliente con varios códigos de depósito activos.	Empleado	Asesor al cliente previo a otorgar otro código, valida si el solicitante ya tiene uno.	Preventivo	Manual	Ocasional	3
RIESGO 25	NO clientes con más de un código de depósito activo	Empleado	Asesor al cliente previo a otorgar otro código, valida si el solicitante ya tiene uno.	Preventivo	Manual	Ocasional	3
RIESGO 26	Cientes con más de un código de depósito y una tarjeta activos.	Empleado	No existe control	No determinado	No determinado	No determinado	0
RIESGO 27	Manejo de un mismo código de depósito por diferentes personas	Productos/ Servicios	No existe control	No determinado	No determinado	No determinado	0
RIESGO 28	Cliente solicita varios códigos de retiro en varias agencias	Cliente	Asesor al cliente previo a otorgar otro código, valida si el solicitante ya tiene uno.	Preventivo	Manual	Ocasional	3

Fuente: Datos de la institución financiera
Elaboración propia