

**UNIVERSIDAD DE EL SALVADOR
FACULTAD DE CIENCIAS ECÓNICAS
ESCUELA DE CONTADURÍA PÚBLICA**



“MODELO DE GESTIÓN DE RIESGOS COMO HERRAMIENTA EN LA PREVENCIÓN DE LAVADO DE DINERO Y ACTIVOS, PARALAS SOCIEDADES PROVEEDORASDE DINERO ELECTRÓNICO EN EL SALVADOR”.

TRABAJO DE INVESTIGACION PRESENTADO POR:

CATOTA GARCÍA, ZULEYMA MARGARITA

CÓRTEZ HERNÁNDEZ, WILBER NAHUN

ESCOBAR JOYA, SULEYMA JANETH

PARA OPTAR AL GRADO DE:

LICENCIADO EN CONTADURÍA PÚBLICA

MAYO DE 2017

SAN SALVADOR

EL SALVADOR

CENTROAMÉRICA

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES UNIVERSITARIAS

Rector	:	Msc. Roger Armando Arias
Secretaria	:	Dra. Ana Leticia Zavaleta de Amaya
Decano de la Facultad de Ciencias Económicas	:	Lic. Nixon Rogelio Hernández Vázquez
Secretario de la Facultad de Ciencias Económicas	:	Licda. Vilma Marisol Mejía Trujillo
Directora de la Escuela de Contaduría Pública	:	Licda. María Margarita de Jesús Martínez Mendoza de Hernández
Coordinador general de Procesos de graduación facultad De ciencias económicas	:	Lic. Mauricio Ernesto Magaña Menéndez
Coordinador de Seminario	:	Lic. Daniel Nehemías Reyes López.
Docente Director	:	Msc. Morena Guadalupe Colorado De Hernández
Jurado Examinador	:	Msc. Morena Guadalupe Colorado De Hernández Lic. Henry Amílcar Marroquín Lic. Daniel Nehemías Reyes López

AGRADECIMIENTOS

Agradezco primeramente a Dios por todas las bendiciones que ha derramado a lo largo de mi carrera y que me han permitido culminar mis estudios universitarios, también agradezco a mis padres por su apoyo incondicional. A mí amado Samuel, por su constante motivación a lo largo de este trayecto. A mis compañeros de Tesis por compartir el esfuerzo de culminar este trabajo. A la Universidad de El Salvador por darme la oportunidad de formarme profesionalmente.

Zuleyma Margarita Catota García

Agradezco primeramente a Dios, por brindarme la sabiduría y las fuerzas necesarias para enfrentar los desafíos en la trayectoria de toda mi carrera y con ello lograr mis metas. A mis padres Herminio Cortez y Rosa Hernández, por su incondicional apoyo en mi carrera profesional. De manera muy especial agradezco a mi esposa Flor Ayala por su apoyo para salir adelante. A mis compañeras de tesis por su apoyo incondicional y por haber compartido esta etapa de mi vida. A todos los docentes que a lo largo de la carrera me prepararon para ser mejor profesional.

Wilber Nahun CortezHernández

Agradezco a Dios todopoderoso por su misericordia que siempre está conmigo, por ser mi guía y compañía a lo largo de mi carrera, por ser mi fuerza en los momentos de debilidad y por brindarme la sabiduría necesaria. A mis padres, Claudio Escobar y Emelida Joya, por sus sacrificios brindados hacia mí a lo largo de la vida, a mi hermana Vanesa Escobar por su apoyo incondicional. A mis compañeros de tesis, Zuleyma y Wilber por emprender juntos este viaje. A mis familiares y amigos por sus buenos deseos y a la Universidad de El Salvador por brindarme la oportunidad de formarme académicamente. A todos ellos infinitas gracias.

Suleyma Janeth Escobar Joya

ÍNDICE

RESUMEN EJECUTIVO	i
INTRODUCCIÓN	iii
CAPÍTULO I: MARCO TEÓRICO	1
1. ANTECEDENTES	1
1.1. Antecedentes internacionales del dinero electrónico	1
1.1.1. El dinero electrónico a nivel mundial.	2
1.1.2. Antecedentes locales del dinero electrónico.	4
1.2. Características del dinero electrónico	5
1.3. Antecedentes internacionales del lavado de dinero y activos.	7
1.3.1. Estados Unidos	7
1.3.2. Argentina	8
1.3.3. Europa	9
1.4. Antecedentes locales del lavado de dinero y activos.	10
1.5. Etapas del lavado de dinero y activos.	11
1.6. Técnicas utilizadas para el lavado de dinero y activos.	12
1.7. Financiamiento al terrorismo.	14
1.8. Modelo de gestión de riesgos	15
1.8.1. Etapa 1. Diagnóstico.	16
1.8.2. Etapa 2. Identificación de los riesgos.	17
1.8.3. Etapa 3. Medición o evaluación de los riesgos.	17
1.8.4. Etapa 4. Adopción de controles (Medidas Preventivas)	18
1.8.5. Etapa 5. Divulgación y documentación (Capacitación y Consulta).	19
1.8.6. Etapa 6. Seguimiento o monitoreo.	20

1.9. Marco normativo.	20
1.9.1. Marco Legal.	20
1.9.2. Marco Técnico.	27
CAPÍTULO II: METODOLOGÍA Y DIAGNÓSTICO DE LA INVESTIGACIÓN.	35
2.1. Procesamiento de la información.	35
2.2. Tipo de estudio.	35
2.3. Unidades de análisis.	35
2.4. Universo y muestra.	35
2.5. Instrumentos y técnicas utilizadas en la investigación.	35
2.6. Análisis e interpretación de la información.	36
2.7. Diagnóstico de la investigación.	36
CAPÍTULO III: MODELO DE GESTIÓN DE RIESGOS DE LAVADO DE DINERO Y ACTIVOS	39
3.1. Desarrollo del sistema de gestión de riesgos.	39
3.1.1. Introducción.	39
3.1.2. Objetivos	40
3.1.3. Estructura del sistema de gestión de riesgos de lavado de dinero y activos.	40
3.1.4. Caso práctico.	43
3.2. Etapa 1: Diagnóstico	45
3.2.1. Compromiso de dueños y directivos en la gestión de riesgos.	45
3.2.2. Determinación del contexto interno y externo.	46
3.2.3. Definición de la estructura organizativa.	49
3.2.4. Determinar factores de riesgo.	49
3.2.5. Diagnóstico general que refleje los factores de riesgo.	50
3.3. Etapa 2: Identificación de eventos.	52
3.3.1. Identificar los eventos de riesgo por cada factor de riesgo.	52

3.4. Etapa 3: Medición o evaluación de los riesgos.	61
3.4.1. Determinación de los criterios de medición de los riesgos.	61
3.5. Etapa 4. Adopción de controles.	77
3.5.1. Definir controles para mitigar cada uno de los riesgos identificados.	77
3.5.2. Definir los procedimientos para aplicar los controles.	87
3.6. Etapa 5: divulgación y documentación	89
3.6.1. Sistema de documentación y registro de los elementos del sistema de gestión del riesgo	89
3.6.2. Procedimientos para la realización de reportes internos y externos	90
3.6.3. Diseño de planes y programas de capacitación	90
3.7. Etapa 6: Seguimiento y Monitoreo	91
3.7.1. Definición de actividades de monitoreo	91
3.7.2. Procedimientos para la realización de actividades de monitoreo.	91
CAPÍTULO IV CONCLUSIONES Y RECOMENDACIONES	93
4.1. Conclusiones	93
4.2. Recomendaciones	94
BIBLIOGRAFÍA	95
ANEXOS	97

ÍNDICE DE FIGURAS

FIGURA N°1: Operatividad del dinero electrónico.	6
FIGURA N°2: Etapas del lavado de dinero y activos	12
FIGURA N° 3: Proceso de gestión de riesgo .	42
FIGURA N° 4: Esquema operativo, ElectroniCash, S.A.	47
FIGURA N° 5: Organigrama ElectroniCash, S.A.	49

ÍNDICE DE TABLAS

TABLA N° 1: Dinero electrónico a nivel mundial.	2
TABLA N° 2: Criterios para la medición de probabilidad e impacto.	17
TABLA N° 3: Legislación aplicable a las sociedades proveedoras de dinero electrónico.	20
TABLA N° 4: Normativa técnica aplicable a las sociedades proveedoras de dinero electrónico.	27
TABLA N° 5: Identificación de riesgos, causas y consecuencias.	52
TABLA N° 6: Niveles de medición para determinar la probabilidad e impacto de los riesgos.	64
TABLA N° 7: Obtención de los niveles de clasificación de riesgos.	64
TABLA N° 8: Mapa de calor para los diferentes niveles de riesgos.	65
TABLA N° 9: Clasificación de Riesgos.	66
TABLA N° 10: Escalas de valorización de la efectividad de los controles.	66
TABLA N° 11: Obtención del riesgo residual.	67
TABLA N° 12: Respuesta al riesgo.	77
TABLA N° 13: Controles para la mitigación de los riesgos.	78
TABLA N° 14: Procedimientos para la realización de actividades de monitoreo.	91

RESUMEN EJECUTIVO

El sistema financiero va cambiando a tal punto que el dinero electrónico se convirtió en una necesidad, no solo para hacer transacciones de una manera más rápida y cómoda sino también para incluir a la población que no tenía acceso a una entidad financiera. Es así como surgen las sociedades proveedoras de dinero electrónico.

La tecnología hace que todo se vuelva más fácil, pues solo se necesita de un Smartphone para tener acceso a este servicio, y hoy en día un 80% de la población cuenta con uno de estos teléfonos celulares, pero no todo puede ser tan bueno ya que por su práctico acceso, puede ser utilizado para fines ilícitos motivo por el cual la autoridades estatales vieron la necesidad de regularlo y las empresa de mejorar su controles y así salvaguardar su imagen y no verse involucrado en un problema legal.

Con la entrada en vigencia de la Ley para facilitar la inclusión financiera se da la paso para que las sociedades antes mencionadas se integren al sistema financiero del país, con lo cual es necesario la implementación de un modelo de gestión de riesgos el cual cumpla con las disposiciones contempladas es los diferentes normas y leyes aplicables al sistema financiero.

Para el desarrollo de dicha propuesta se consideró la bibliografía existente en temas relacionados al dinero electrónico y al lavado de dinero y activos y financiamiento al terrorismo, con la finalidad de crear una herramienta que sirva de apoyo a la sociedad proveedora de dinero electrónico.

El instrumento utilizado para la recolección de datos fue la guía de entrevista, la cual estuvo dirigida a miembros de la alta gerencia de Mobile Cash, S.A. de C.V. quien es la única empresa dedicada a proveer dinero electrónico en el país. Del análisis efectuado a cada una de las respuestas obtenidas, se procedió a la elaboración de un diagnóstico general que establece la necesidad de mejora en el sistema de gestión de riesgos que actualmente es aplicado.

En el desarrollo de la propuesta de un modelo de gestión de riesgos para los delitos de lavado de dinero y activos, se establecieron seis diferentes etapas basadas en estándares internacionales como las normas GAFI y normas locales como las emanadas por el BCR para la gestión de riesgos.

En la primera etapa se describe un diagnóstico sobre la situación actual de la entidad (ElectroniCash, S.A.), en su contexto interno y externo sobre la exposición a los riesgos de lavado de dinero, determinando el nivel de compromiso de los dueños, alta gerencia y miembros en general. Posteriormente

en la segunda etapa se realiza la identificación de los eventos de riesgo para cada factor establecido, determinando posibles causas que los originan. Para la medición y evaluación de los riesgos, etapa tres del modelo, se clasifica cada riesgo por su nivel de probabilidad e impacto, los cuales son trasladados a una matriz de riesgo para analizar que riesgos son considerados como no tolerables para la operatividad del negocio.

En la etapa número cuatro se definen los controles necesarios para mitigar cada uno de los riesgos identificados y los procedimientos a aplicar en el proceso de implementación de dichos controles. La etapa cinco comprende el sistema de divulgación y documentación de los elementos del sistema desarrollado. Por último, en la etapa seis se definen las actividades de monitoreo para verificar el fiel cumplimiento de las medidas definidas durante todo el proceso de la gestión de los riesgos.

Para finalizar se incluyen las conclusiones del trabajo realizado y las recomendaciones dirigidas a las sociedades proveedoras de dinero electrónico en El Salvador, para el logro de una eficaz gestión en materia de prevención de lavado de dinero y activos.

INTRODUCCIÓN

En el entorno tanto nacional como internacional el tema de lavado de dinero y activos y de financiamiento al terrorismo, ha tenido mucho auge, y a esto se le agrega que la tecnología avanza con mucha rapidez, lo que permite que los servicios ofrecidos por las empresas sean cada día más amplios y modernos. Las empresas que operan con dinero electrónico surgen por la necesidad de facilitar el acceso de las personas al sistema financiero nacional, por lo tanto el riesgo de lavado de dinero y financiamiento al terrorismo es mucho más evidente para este tipo de entidades. Esto llevó a los dirigentes del país a retomar las medidas necesarias para que se detecte y elimine a tiempo cualquier amenaza de lavado de dinero y financiamiento al terrorismo en todas las modalidades que se aplica actualmente en el sistema financiero.

En este sentido en El Salvador fue aprobada la Ley para facilitar la inclusión financiera que contempla a las sociedades proveedoras de dinero electrónico como las que proporcionaran servicios financieros de manera accesible a la población en general, no dejando de lado el aspecto de riesgo de lavado de dinero y financiamiento al terrorismo que las entidades proveedoras tienen inherentemente. Este es un delito que corrompe y altera todas las estructuras sociales y económicas de los países, las instituciones que integran el sistema financiero se muestran vulnerables a ser utilizadas para las actividades delictivas, por lo cual se vuelve necesario tener en las entidades proveedoras de dinero electrónico un Modelo de Gestión de riesgos como herramienta en la prevención del lavado de dinero y financiamiento al terrorismo.

En el documento se presenta la investigación denominada “MODELO DE GESTIÓN DE RIESGOS COMO HERRAMIENTA EN LA PREVENCIÓN DEL LAVADO DE DINERO Y DE ACTIVOS PARA LOS AGENTES AUTORIZADOS DE PROVEER DINERO ELECTRÓNICO EN EL SALVADOR”. Este está estructurado con cuatro capítulos en los que se plasman, de forma detallada, cada una de las etapas con las que cuenta el modelo así mismo los elementos que lo conforman.

El capítulo I, contiene los antecedentes internacionales y nacionales del dinero electrónico, las etapas del lavado de dinero, las técnicas utilizadas para el lavado de dinero y activos y financiamiento al terrorismo. Además se presentan los elementos básicos de un modelo de gestión de riesgos, conceptos básicos para la realización de la investigación, marco normativo y legal bajo el cual fue realizado este documento.

El capítulo II, corresponde a la metodología y diagnóstico de la investigación, procesamiento de la información, tipo de estudio, unidades de análisis, universo y muestra, instrumentos y técnicas utilizadas

en la investigación, el análisis e interpretación de la información y finalmente el diagnóstico de la investigación.

El capítulo III, contiene la elaboración completa de un sistema de gestión de riesgos, tomando como referencia un caso práctico que conlleva a la estructuración completa del mismo, esto con el objetivo que la entidad proveedora de dinero electrónico tenga un mejor control y disminuya su riesgo de lavado de dinero y activos y financiamiento al terrorismo, ya que el sistema de gestión de riesgos abarca todos los aspectos que la entidad debe aplicar para un mejor resultado.

El Capítulo IV, finalmente establece las conclusiones y recomendaciones que surgen como producto de los resultados obtenidos de la investigación, así como también la bibliografía y sus anexos.

CAPÍTULO I: MARCO TEÓRICO

1. ANTECEDENTES

1.1. Antecedentes internacionales del dinero electrónico

La evolución de los medios físicos de pago como lo son el cheque y el efectivo, sufrió un cambio durante la década de los 50's, surgió un nuevo mecanismo de pago, para el cual se aprovechó una infraestructura comercial suficientemente desarrollada para promover la aceptación del nuevo dinero plástico. En los primeros meses de 1950, un empresario llamado Frank McNamara, le proporcionó tarjetas a algunos cientos de personas en Manhattan, y se puso de acuerdo con varios de los principales restaurantes para que pagaran un 7% de la cuenta al recibir la nueva tarjeta 'Diners Club'. Ese fue el inicio de toda una industria, a su vez le siguieron a Diners Club las marcas de tarjetas de pago como Carte Blanche, American Express y BankAmericard durante esa misma década.

Desde entonces se ha mantenido un constante crecimiento de la industria de medios de pago alternativos. La tecnología ha facilitado enormemente esta expansión al lograr la interconexión inmediata de las entidades involucradas en cada una de esas transacciones electrónicas. Así MasterCard y Visa que nacieron en la década de los 60's han logrado en años recientes un crecimiento sorprendente en el volumen de transacciones electrónicas.

Y con el tiempo el siguiente paso del dinero plástico, es este que se está consolidado con el término de dinero electrónico, el cual está formado principalmente de dos tecnologías desarrolladas en años recientes:

- Tarjetas inteligentes o con Chip (Smart Cards).
- Los programas de Software que facilitan el intercambio de bienes y servicios en Internet.

Las tarjetas inteligentes o con chip, han sido de gran trascendencia en ciertas regiones del mundo, debido principalmente a dos características específicas que se presentan en esas zonas. Por un lado en los países o áreas en donde el costo de infraestructura de comunicaciones es relativamente alto, para lo cual la tecnología de chip ayuda a disminuir costos de telecomunicaciones al tener la posibilidad de funcionar con cierta independencia. También esta tecnología se ha adoptado en zonas

donde la incidencia de fraude tiene niveles especialmente altos y en donde se ha aprovechado la tecnología de tarjetas inteligentes.

El E-money presenta nuevas formas de pago facilitando la transferencia de fondos a velocidades y cierta manera eficiencia sin precedente, estableciendo a la vez las bases de la economía global y sus mecanismos de operación. Este desarrollo no está libre de riesgos y problemas que sobretodo tienen que ver con la regulación por parte de los gobiernos y autoridades financieras para las nuevas condiciones de funcionamiento, ya que el dinero electrónico abre la puerta a las transferencias masivas de capitales que fácilmente podrían plantear retos en el control del “circulante electrónico” para los gobiernos.

En la actualidad la mayoría de países carecen de una legislación clara en términos de la utilización del dinero electrónico, considerando por ejemplo el hecho de que actualmente hay instituciones en el mundo emitiendo dinero electrónico en la red que no son instituciones de crédito reguladas por autoridades de ningún tipo.

Con lo anterior, queda bastante claro que el dinero electrónico será solamente información contenida en bases de datos de computadoras con alcances mundiales, o al mismo tiempo en microchips de dispositivos como las tarjetas inteligentes que actualmente conocemos.(Endeavor, 2010)

1.1.1. El dinero electrónico a nivel mundial.

Tabla 1. Dinero electrónico a nivel mundial.

Países	Empresas involucradas	Información
Perú	Movistar y MasterCard	Brindan el servicio “tu dinero móvil” mediante el cual se puede enviar y recibir dinero desde su celular, además de realizar compras en establecimientos afiliados a MasterCard.
Ecuador	CNT, Claro y Movistar y Banco Central de Reserva de Ecuador	Estas empresas telefónicas en conjunto con el Banco Central de Reserva de Ecuador, crearon “efectivo”. Ecuador es el único país donde el gobierno administra esta forma de pago.

Países	Empresas involucradas	Información
Uruguay	QOOLLET	Funciona como emisora de dinero electrónico permitiendo pagar servicios básicos desde una aplicación móvil. QOOLLET no necesita una compañía de teléfono en específica ya que trabaja con una cuenta de Banco.
Paraguay	TIGO y Personal	<p>La operadora Tigo cuenta con “tigomoney” con la cual puede realizar transferencias y pagos desde un móvil Tigo.</p> <p>La operadora Personal cuenta con “billetera personal”, la cual necesita una cuenta corriente o de ahorro para poder funcionar.</p>
México	BBVA Bancomer y Banorte	Con Bancomer móvil se puede transferir dinero a través de un teléfono móvil, quien lo recibe puede ir a un cajero automático ingresar la clave de retiro y código de seguridad para retirar su dinero.
Kenia	Safaricom	M-pesa es la plataforma lanzada por Safaricom, en la cual se puede transferir dinero, pagar facturas y recibir salarios. Al momento de recibir el dinero puedo hacerlo efectivo a través de un agente autorizado o un cajero automático sin necesidad de una tarjeta de crédito o débito.
España	Vodafone	Vodafone Wallet, es una aplicación que permite ingresar tarjetas de crédito o débito de VISA y MASTERCAR a un teléfono móvil, y así pagar con ellas en muchos de los establecimientos de España, solo se necesita acercar el celular al post e ingresar el PIN de seguridad, siempre que la cantidad a pagar sea mayor a 20€.

Países	Empresas involucradas	Información
Japón	Domoco y Mizuho	<p>Las tarjetas IC se usan como un monedero electrónico con el cual se realiza el pago en el transporte público, tiendas 24 horas y máquinas de bebidas.</p> <p>Los nuevos teléfonos móviles traen incorporado la tecnología IC con la cual además de realizar pago se puede transferir dinero electrónico.</p>

1.1.2. Antecedentes locales del dinero electrónico.

Fue en junio del año 2011 cuando la empresa MOBILE CASH, SOCIEDAD ANONIMA DE CAPITAL VARIABLE, que puede abreviarse MOBILE CASH, S.A. DE C.V., adjunta a la compañía de telefonía TELEMÓVIL (Tigo), lanzaron al mercado una nueva modalidad del uso del dinero en El Salvador, se trataba de TigoMoney que opera bajo el sistema de dinero electrónico.

Ya en muchos países del mundo el dinero electrónico se había convertido en un sustituto parcial del efectivo, y porque no decirlo como un reemplazo total de este, en países con las mejores economías hasta el más pequeño de los pagos por bienes y servicios se hacía con el uso del dinero contenido en un teléfono móvil, en nuestro país debido a la creciente demanda en el sistema de telefonía móvil y el fenómeno de violencia que se vive en la actualidad, fueron los factores claves para que estas empresas fusionaran sus estrategias de negocio y operaran con un novedoso sistema, por un lado, se aprovechaba la cartera de clientes existentes y se motivaba a la población a utilizar un sistema que les permitiría en gran medida no ser objeto de robos y asaltos debido a que ya no se maneja efectivo en los bolsillos.

El sistema de dinero electrónico presenta varias ventajas en cuanto a la economía del país, en tanto que permite que muchas personas tengan acceso al sistema financiero, se sabe que hoy en día muchas personas del área rural en el país no cuentan con una cuenta bancaria pero si con un teléfono celular, lo que permite que mediante el uso del dinero electrónico tengan la facultad de mejorar su situación económica.

Son muchos los comentarios respecto al tema de operación de Tigo Money, ya que fue hasta el mes de septiembre del año 2015, que el Banco Central de Reserva y la Superintendencia del Sistema Financiero, decidieron tomar el control de sus operaciones con la entrada en vigencia de la Ley para facilitar la inclusión financiera, uno de los principales motivos de la creación de esta ley, fue la de regular el establecimiento legal de instituciones que operaban bajo la modalidad de sociedades proveedoras de dinero electrónico y que no cumplían con requisitos formales ante el Sistema Financiero y que propiciaban el cometimiento de acciones ilícitas como el lavado de dinero y financiamiento al terrorismo.

Dicha Ley, establece mecanismos novedosos de prestación de servicios financieros, a través de medios electrónicos, los cuales facilitan a los salvadoreños la inserción a la actividad económica; además favorece la competencia en la prestación de servicios de pagos minoristas. Esta normativa apoya el bienestar de las familias salvadoreñas, a través de la reducción de costos de transacción, mediante la utilización de tecnología en los servicios financieros que se realizan por medio de celulares, entre otros.

Un punto importante dentro de este triángulo de mercado (TigoMoney-Intermediario-Cliente), son las empresas intermediarias del sistema conocidas como agentes autorizados, según datos publicados son más de 2,500 puntos de atención en todo el país de TigoMoney, entre ellas podemos mencionar Farmacias, Tiendas, Supermercados, etc.(El Diario de Hoy, 2015, pág. 34)

Entre los servicios que presta esta empresa se encuentran envíos de dinero, recargas de saldo, pago de recibos de servicios básicos, etc. Según la publicación antes citada TigoMoney pretende incrementar su mercado por lo que ha establecido alianzas con diferentes sectores de comercio privado, para que en un futuro el dinero electrónico pueda utilizarse como sistema de pago de planillas de salarios a sus empleados y la prestación de otros servicios.

1.2. Características del dinero electrónico

- El dinero electrónico es ampliamente aceptado por las masas y por eso se debe diferenciar de los otros instrumentos de prepago que utilizan dispositivos técnicos similares.
- Está diseñado para transacciones de poca cuantía, sin embargo, puede adecuarse a grandes pagos.
- Su uso requiere una infraestructura específica para el comprador y el vendedor.

- Cuenta con mayores niveles de seguridad en comparación con el dinero físico, tanto para el usuario como para los comerciantes.(Duarte, 2012)
- Los usuarios podrán acceder a servicios financieros, desde cualquier lugar ya cualquier hora.

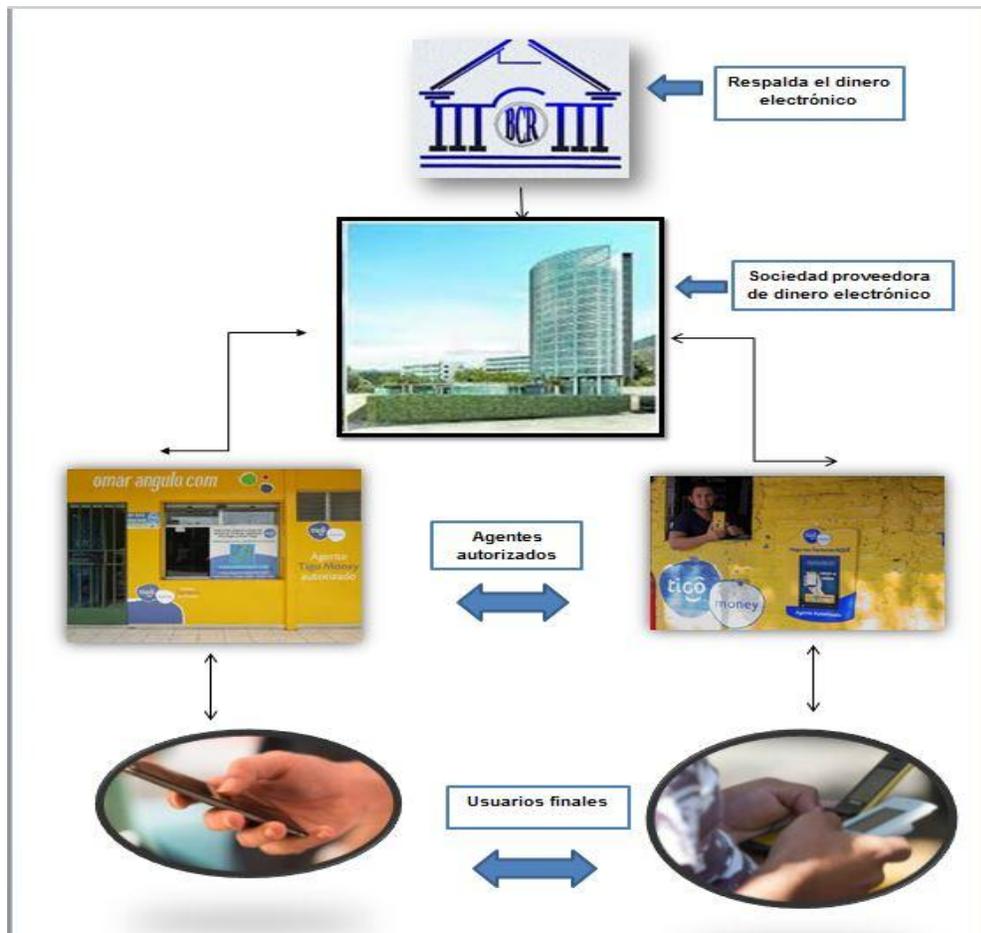


Figura 1. Operatividad del dinero electrónico. **Fuente:** creación propia.

En el esquema anterior muestra cómo funcionan las operaciones de dinero electrónico definidas a continuación:

- **Banco Central de Reserva:** ejerce control diario y continuo sobre la masa de dinero electrónico, que deberá ser un monto fijo para garantizar que el dinero electrónico no exceda al depósito de respaldo correspondiente en el BCR. Esto con el fin de asegurarse que la sociedad proveedora de dinero tenga liquidez con la cual responder a sus clientes ante cualquier contingencia.

- **Sociedad proveedora de dinero electrónico:** es la que autoriza y controla las cuentas de los usuarios de este servicio, cuenta con una plataforma tecnológica en la cual se resguarda el dinero electrónico. Además de formar alianzas con micro empresas que sirvan de intermediadoras en el proceso a las cuales se denomina agentes autorizados, dichas sociedades proveen todo lo necesario a estos agentes para que puedan operar.
- **Agentes autorizados:** son los que generan los registros de cada usuario, reciben pagos de dinero electrónico, y convierten estos pagos a dinero en efectivo mediante un pin de seguridad que es proporcionada al usuario cuando se registra en el sistema o plataforma tecnológica. Poseen un contacto directo con los usuarios finales.
- **Usuarios finales:** estos al crear su usuario en la plataforma tecnológica pueden convertir dinero físico en electrónico mediante los agentes autorizados, una vez hecho esto el cliente puede usarlo mediante su aplicación móvil, ya sea para realizar una remesa, pagar recibos, recargar su teléfono móvil o convertirlo nuevamente en efectivo.

1.3. Antecedentes internacionales del lavado de dinero y activos.

1.3.1. Estados Unidos

El fenómeno del lavado de dinero, tiene sus orígenes en el país de los Estados Unidos de Norteamérica, con el surgimiento de las grandes mafias en Chicago y Nueva York en el año de 1899, provenientes de la inmigración de familias de diferentes países, especialmente de Europa.

Al Capone fue uno de los más representativos personajes de la mafia, se unió a una pandilla callejera, liderada por Jhonny Torrio e integrada por otros mafiosos como Lucky Luciano y Meyer Lansky, quien luego pasó a ser el cerebro financiero del grupo de Capone. Cerca de los años de 1920, Al Capone se unió a Torrio en la ciudad de Chicago, lo que se conoció como la familia Colosito.

La situación relacionada con la prohibición del alcohol o Ley Volstead en los Estados Unidos ocasionó el surgimiento de las industrias criminales de mayor crecimiento, se creó una red de lavanderías para esconder la procedencia ilícita del dinero que se alcanzaban con la venta callejera de drogas y la preparación y distribución de licor de forma ilegal.

El mecanismo que se utilizaba era el de presentar las ganancias obtenidas de forma ilícita en el negocio de las lavanderías, la mayoría de los pagos del negocio se realizaban en efectivo y eran reportadas al Internal Revenue Service de los Estados Unidos, pero se realizaba una combinación de ingresos, por una parte se encontraban las ganancias por el lavado de textiles y por otra las ganancias obtenidas por la venta ilegal de drogas, armas y prostitución, de esta forma la mafia pudo burlar por muchos años a las autoridades.

El 16 de junio de 1931, Al Capone se declaró culpable por los cargos de evasión fiscal y la venta ilícita de alcohol. El 18 de octubre de 1931, Capone fue declarado culpable después de un juicio y el 24 de noviembre fue sentenciado a once años de cárcel en una prisión federal, multado con \$50.000.00, fue recluido en el Penal de Atlanta y en Alcatraz. (R24N NOTICIAS, 2016)

La recaudación del dinero ilícito en Estados Unidos era depositada en los bancos sin ningún control que permitiera establecer la procedencia lícita de los fondos obtenidos, así era como estos se introducían fácilmente al sistema formal de la banca estadounidense, fue en la década de los 60, que se introdujo el concepto del blanqueo de capitales.

Fue hasta el año de 1970 que las autoridades norteamericanas establecieron los primeros controles para la prevención del narcotráfico, con la entrada en vigencia de la Ley de secreto bancario. El enfoque de esta ley era el uso del efectivo, se establecieron una serie de requisitos que se aplicaban a las transacciones en efectivo.

En el año de 1982 se reconoce judicialmente la expresión del lavado de dinero, al ser confiscado el dinero procedente de la venta de droga colombiana.

1.3.2. Argentina

Entre los países que más destacan en Latinoamérica, por el trabajo arduo que se realiza en materia de prevención de lavado de dinero, encontramos a Argentina, país que ha promulgado leyes orientadas a la prevención de delitos de esta naturaleza, tal es el caso de la Ley penal sobre estupefacientes. En el año de 1990, se creó la Comisión Mixta de Control de las operaciones relacionadas con el lavado de dinero del narcotráfico.

Hasta el año 2000, sólo se castigaba el blanqueo de dinero proveniente del narcotráfico, pues el lavado de dinero no estaba tipificado en el Código Penal. En Abril de ese año se sancionó la primera Ley contra el lavado de dinero (25.246). Sin embargo, la ley exigía que el lavador no fuera al mismo tiempo el autor del

delito previo porque en ese caso el lavado era considerado parte del mismo ilícito y sancionarlo equivalía a aplicar una doble sanción. El Gobierno se propuso terminar con esta situación y logró que en el año 2011 el Congreso de Argentina aprobara una ley que considera al lavado de dinero como un delito autónomo. Esta ley es la 26.683, la ley incorporó la posibilidad de extender la sanción por el delito de lavado de activos al autor del delito precedente y además prevé la responsabilidad penal de las personas jurídicas involucradas. Otras leyes que se aprobaron en esta fecha fueron la 26.733, 26.734, 26.831 y el Decreto N° 918/2012.

Todas estas disposiciones contenidas en las Leyes fueron gracias al apoyo internacional de países como Estados Unidos y a la Comunidad Económica Europea.

1.3.3. Europa

En los países europeos como Gran Bretaña, se promulgaron diferentes leyes para tratar los casos de lavado de dinero y activos, entre ellas se pueden mencionar la Ley de delitos vinculados al narcotráfico en el año de 1986 y la Ley de justicia criminal aprobada en el año de 1993, esta última buscaba incorporar conceptos relativos al lavado de dinero, como por ejemplo, se penalizaba el hecho de recibir ganancias del narcotráfico con conocimiento de su origen y el no informar sobre cualquier sospecha de delitos de lavado a las autoridades correspondientes.

En Francia, se aprobó en el año de 1990, la Ley 90-614, que establecía entre otros aspectos, la obligación de informar sobre cualquier operación realizada con evidencias relacionadas al crimen organizado. Enmarcaba, además, la participación de organismos financieros en la lucha contra el lavado de dinero.

Italia, aprobó la Ley 55, en el año 1990, en esta normativa legal tipificaba como delito el lavado de dinero y activos, provenientes de la actividad ilícita como robos, extorsiones, secuestros y el tráfico de drogas. Un año después, en 1991, se promulgo la Ley 197, que establecía como requisito esencial la identificación total de las partes involucradas en transacciones con fuertes sumas de dinero.

Por último en España, se creó en el año de 1990 la Ley 19/1993, en esta ley se establecían conceptos sobre el tema del blanqueo de capitales y una lista de actividades consideradas como parte del delito de lavado de dinero, así como una serie de requerimientos a cumplir por parte de las entidades financieras de este país. En el año de 1995, se aprobó el Real Decreto 925/95, que contenía un reglamento contra el delito de lavado de dinero, en ese mismo año se establece la Ley Orgánica 10/95 del Código Penal, que tipifico el blanqueo de capitales como un delito grave.

En los últimos años la legislación española ha tratado de promulgar leyes que prevengan el delito de lavado de dinero, tal es el caso de la entrada en vigencia, en abril del año 2010, de la Ley de prevención del blanqueo de capitales y del financiamiento al terrorismo. Su objetivo es erradicar las llamadas “tapaderas” y vehículos financieros donde se esconden activos ilícitos.

1.4. Antecedentes locales del lavado de dinero y activos.

En El Salvador, se promulgo la Ley contra el lavado de dinero y activos, por Decreto Legislativo N° 498, publicada en el Diario Oficial N° 240, Tomo N° 341 de fecha 23 de diciembre del año 1998. Con esta Ley se pretende dar cumplimiento al Convenio centroamericano para la prevención y represión de los delitos de lavado de dinero y de activos relacionado con el tráfico ilícito de drogas y delitos conexos. Según el artículo 1 de la Ley, su objeto principal es prevenir, detectar, sancionar y erradicar el delito de lavado de dinero y de activos, así como su encubrimiento. (Financiero, Superintendencia del Sistema, 2011). El Reglamento derivado de esta Ley, se creó por Decreto Legislativo N° 2, publicado en el Diario Oficial N° 21, de fecha 31 de enero del año 2000.

Se resalta el hecho que pese a la normativa legal establecida en el país, las entidades reguladas por la Ley enfocan su atención más a la relación legal-penal que pueda traer consigo los delitos de lavado de dinero, y no la aplicación de técnicas y procedimientos que permitan prevenir y detectar a tiempo los casos de blanqueo de capitales.

La Superintendencia del Sistema Financiero desarrolla un papel importante en materia de lavado de dinero en el país, entres sus responsabilidades se encuentra la supervisión de la actividad individual y consolidada de los integrantes del Sistema Financiero y demás personas, operaciones o entidades que mandan las leyes. (Superintendencia del Sistema Financiero, 2012).

Por otra parte, se emitió el acuerdo N° 356 de la Fiscalía General de la República, denominado instructivo de la Unidad de Investigación Financiera para la prevención del lavado de dinero y activos en las instituciones de intermediación financiera, este documento tiene por objetivo emitir normas específicas de prevención, detección y reporte de operaciones relacionadas con el lavado de dinero y de activos para las instituciones de intermediación financiera.

Siguiendo la historia de los casos de lavado de dinero en El Salvador, la Fiscalía General de la República ha asegurado en varias ocasiones que casos como el de FINSEPRO-INSEPRO, Lafise, S.A. de C.V. y Banco de Fomento Agropecuario, son claros ejemplos de lavado de dinero, pero que no fueron judicializados por no existir, en esa época, una ley que permitiría tomar acciones penales contra los

implicados, ya que estos hechos ocurrieron antes de la entrada en vigencia de la Ley el lavado de dinero y de activos en el año 1999.

Otro de los casos confirmados de lavado de dinero en El Salvador, fue en el año 2003 cuando se llevó un juicio contra el locutor Riley Serrano, quien estaba acusado de secuestro, fue además la primer suma de dinero llevada al fondo especial contra el lavado de dinero obtenida por la confiscación de cuentas bancarias del implicado (La Prensa Gráfica, 2004). Este fondo especial se enmarca en la disposición contenida en el artículo 23 de la Ley contra el lavado de dinero y de activos, que establece la creación de un patrimonio especial al que se le asignaran recursos provenientes de la liquidación de los bienes comisados de ilegítima procedencia y que serán destinados a financiar actividades como la de protección de víctimas y testigos, programas de rehabilitación de personas víctimas de la drogadicción, etc.

En el año 2011, la Fiscalía General de la República a través de la Unidad de Investigación Financiera tenía unas 75 investigaciones activas por lavado de dinero. Sin embargo, no todas son llevadas a los tribunales, ya que algunas dependen de información internacional. Según datos son más de 200 denuncias mensuales las que recibía en el año 2011 la FGR, de reportes de operaciones sospechosas o ROS. (La Prensa Gráfica, 2011).

1.5. Etapas del lavado de dinero y activos.

Un aspecto importante en la operación del lavado de dinero, es que este no se consume en un instante, sino que se efectúa por etapas. La persona que comete delitos de lavado de dinero, busca que los fondos provenientes de actividades ilícitas se vaya poco a poco mezclando con los fondos lícitos, de manera que las autoridades no detecten ninguna sospecha, se utilizan empresas fachadas para proceder a ocultar los ilícitos, o los fondos son depositados en las instituciones financieras en pequeñas cuantías o utilizando documentos de identidad de otras personas, a quienes se utilizan pagándoles un poco de dinero, a cambio de que trabajen colocando los fondos ilícitos en sus cuentas bancarias, luego que procedan a realizar transferencias a otras cuentas, cuyo usuario final son jefes de bandas dedicadas al narcotráfico o la prostitución.

Entre las etapas del lavado de capitales se destacan las descritas en la siguiente figura:

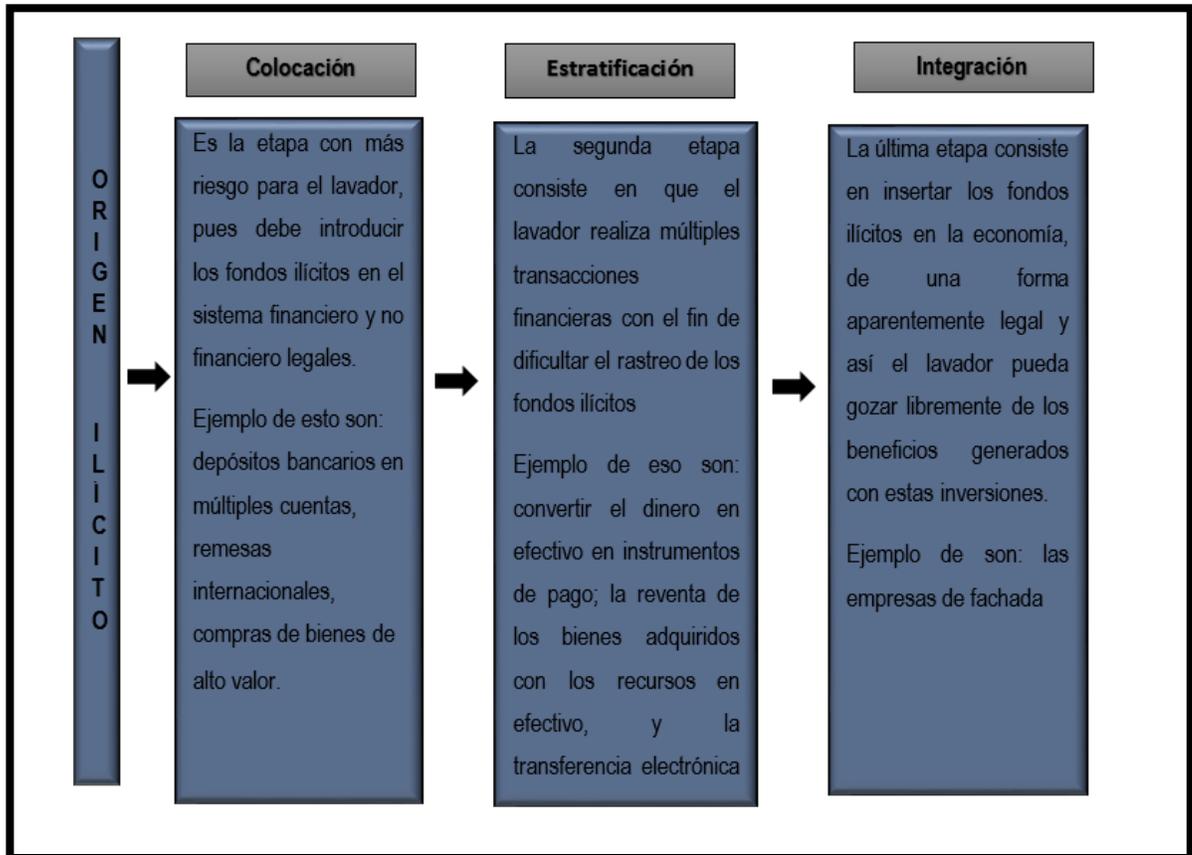


Figura 2: Etapas del lavado de dinero y activos. Fuente: Creación propia.

1.6. Técnicas utilizadas para el lavado de dinero y activos.

Entre las formas más comunes para dar paso a la realización del blanqueo de capitales se pueden mencionar las siguientes:

- **Estructurar, trabajo de hormiga o “pitufeo”:** División o reordenación de las grandes sumas de dinero adquiridas por ilícitos, reduciéndolas a un monto que haga que las transacciones no sean registradas o no resulten sospechosas. Estas transacciones se realizan por un período limitado en distintas entidades financieras.
- **Complicidad de un funcionario u organización:** Uno o varios empleados de las instituciones financieras pueden colaborar con el lavado de dinero omitiendo informar a las autoridades sobre

las grandes transacciones de fondos, generalmente su complicidad es causada por una extorsión y, a veces, obtendrá una comisión por ella.

- **Complicidad de la banca:** Hay casos en que las organizaciones de lavado de dinero gozan de la colaboración de las instituciones financieras (a sabiendas o por ignorancia), dentro o que están fuera del mismo país, las cuales dan una justificación a los fondos objeto del lavado de dinero.
- **Mezclar:** Las organizaciones suman el dinero recaudado de las transacciones ilícitas al capital de una empresa legal, para luego presentar todos los fondos como rentas de la empresa. Esta es una forma legal para no explicar las altas sumas de dinero.
- **Empresas fantasmas (*shell company*):** También conocidas como compañías de fachada o *de portafolio*. Son empresas legales, las cuales se utilizan como cortina de humo para enmascarar el lavado de dinero. Esto puede suceder de múltiples formas, en general, la compañía de fachada desarrollará pocas o ninguna de las actividades que oficialmente debería realizar, siendo su principal función aparentar que las desarrolla y que obtiene de las mismas el dinero que se está lavando. Lo habitual es que de dicha empresa sólo existan los documentos que acrediten su existencia y actividades, no teniendo presencia física ni funcionamiento alguno más que sobre el papel.
- **Compraventa de bienes o instrumentos monetarios:** Inversión en bienes como vehículos, inmuebles, etc. (los que a menudo son usados para cometer más ilícitos) para obtener beneficios monetarios de forma legal. En muchos casos el vendedor tiene conocimiento de la procedencia del dinero negro que recibe, e incluso puede ser parte de la organización de lavado de dinero. En esos casos, la compra de bienes se produce a un precio muy por debajo de su coste real, quedando la diferencia como comisión para el vendedor. Posteriormente el blanqueador vende todo o parte de lo que ha adquirido a su precio de mercado para obtener dinero lícito. Este proceso puede repetirse, de tal modo que los productos originalmente ilícitos son pasados de una forma a otra sucesivamente para así enmascarar el verdadero origen del dinero que permitió adquirir los bienes. Además, con cada transformación se suele disminuir el valor de los bienes para que las transacciones no resulten tan evidentes.
- **Contrabando de efectivo:** Es el transporte del dinero objeto del lavado hacia el exterior. Existen algunas ocasiones en las cuales los blanqueadores de activos mezclan el efectivo con fondos transportados de otras empresas, para así no dejar rastro del ilícito.

- **Transferencias bancarias o electrónicas:** Uso de Internet para mover fondos ilícitos de una entidad bancaria a otra u otras, sobre todo entre distintos países, para así no dar cuenta de las altas sumas de dinero ingresado. Para hacer más difícil detectar el origen de los fondos, es habitual dividirlos en entidades de distintos países, y realizar transferencias sucesivas.
- **Transferencias inalámbricas o entre corresponsales:** Las organizaciones de lavado de dinero pueden tener ramificaciones en distintos países, por lo tanto la transferencia de dinero de una a otra organización no tiene por qué resultar sospechosa. En muchos casos, dos o más empresas aparentemente sin relación resultan tener detrás a la misma organización, que transfiere a voluntad fondos de una a otra para así enmascarar el dinero negro.
- **Falsas facturas de importación/exportación o “doble facturación”:** Aumentar los montos declarados de exportaciones e importaciones aparentemente legales, de modo que el dinero negro pueda ser colocado como la diferencia entre la factura falsa y el valor real.
- **Garantías de préstamos:** Adquisición de préstamos legalmente, con los cuales el blanqueador puede obtener bienes que aparentan haber sido obtenidos de forma lícita. El pago de dichos préstamos hace efectivo el blanqueo.
- **Acogerse a ciertos tipos de amnistías fiscales:** Por ejemplo, aquellas que permiten que el defraudador regularice dinero en efectivo.

1.7. Financiamiento al terrorismo.

El financiamiento del terrorismo (FT) es 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 fondos para llevar a cabo sus actividades, cuyo origen puede provenir de fuentes legítimas, actividades delictivas, o ambas. (Gobierno de Chile, 2016)

Las técnicas utilizadas para el financiamiento al terrorismo son las mismas que se usan para cometer el blanqueo de capitales, en estas técnicas se trata de encubrir las fuentes y los fines del financiamiento del terrorismo. No obstante, sin importar si el origen de los recursos es legítimo o no, para los grupos terroristas es importante ocultar la fuente y su uso, a fin de que la actividad de financiamiento pase inadvertida.

El Grupo de Acción Financiera Internacional (GAFI), recomienda que cada país tipifique como delito el financiamiento del terrorismo, los actos terroristas y las organizaciones terroristas y que los clasifique como delitos que dan origen al lavado de activos. Asimismo, sugiere que las nueve recomendaciones especiales diseñadas por el organismo para combatir el financiamiento del terrorismo sumadas a las 40 recomendaciones sobre lavado de activos sean el marco para prevenir, detectar y eliminar ambos delitos.

1.8. Modelo de gestión de riesgos

La gestión de riesgos es una parte fundamental de las buenas prácticas de la administración de cualquier entidad y un elemento esencial de las buenas prácticas en la dirección corporativa. Las medidas preventivas adoptadas durante los procesos de gestión de riesgos, son controles mínimos sugeridos para la prevención de estos eventos en los procesos de los negocios, y son el punto de partida para realizar una debida diligencia.

Existen varias razones para que los negocios incorporen medidas preventivas contra los riesgos, una de ellas es que los negocios, cada vez más, se desarrollan en escenarios internacionales, y por tanto, se requieren mercados sanos y sostenibles, así como oportunidades equitativas (competencias leales). A su vez, las actividades criminales como el narcotráfico, la corrupción y el terrorismo, entre otras, son fenómenos mundiales que representan una amenaza no sólo para el país, sino también para la región o el mundo entero. Otra de las razones es que cada vez los riesgos asociados a conductas delictivas como el lavado de activos, la financiación del terrorismo y la corrupción son objeto de recomendaciones (internacionales o locales), de regulación por organismos o autoridades, que buscan la protección de los sistemas económicos y de los mercados. Por tanto, estas recomendaciones internacionales imponen obligaciones no sólo al Estado y las instituciones que lo integran, sino también a todos los sectores que conforman la sociedad. Esto no excluye al sector empresarial. Además, garantiza mayor organización en los negocios porque implica una revisión detallada de prácticas y procedimientos comerciales y financieros. Implica mayor transparencia porque involucra a todos los actores que se relacionan de manera directa con su negocio, o a quienes participan o se deben enterar de las medidas incorporadas para evitar los riesgos y fortalecer la cultura de legalidad de los negocios.

Un modelo de gestión de riesgos comprende las siguientes seis etapas:

1.8.1. Etapa 1. Diagnóstico.

Esta etapa comprende el compromiso de los dueños y directivos del negocio en la prevención de los riesgos, conocer el entorno de la entidad, elaborar el diagnóstico de los riesgos y definir cuáles serán las metodologías, técnicas, herramientas y las fuentes de información para el diseño y adopción del sistema.

Consta de los siguientes pasos:

1. **Compromiso de los dueños y directivos del negocio:** Es esencial el compromiso de los dueños y directivos de los negocios para adoptar medidas, programas, estrategias, manuales, políticas, procesos, procedimientos, cultura institucional, herramientas, buenas prácticas, reportes y ejemplos que demuestren un verdadero rechazo a prácticas que faciliten la realización de actividades ilícitas o sospechosas de dicha condición.(Cámara de Comercio de Bogotá, pág. 18).
2. **Determinar el contexto interno y externo en el que se desarrolla la empresa:** se enfoca en tres ejes principales, establecer el contexto externo, interno y de administración o gestión de los riesgos.

En el contexto externo es necesario que la empresa identifique cuales son aquellas fortalezas, oportunidades, debilidades y amenazas de la organización frente al ambiente en el que opera. Es necesario, además, que la empresa realice una evaluación de los aspectos normativos que le aplican y las partes externas interesadas en el proceso de gestión de riesgos. En cuanto al contexto interno, se evalúan las relaciones entre los objetivos, metas y estrategias del negocio, los costos-beneficios y el entorno interno del negocio como lo son sus productos, clientes, canales de distribución, etc. Por último, es necesario definir cuáles son los objetivos, políticas, estructura organizativa y el control interno de la administración de riesgos.
3. **Determinar los factores de riesgo:**se determinan los factores de riesgo que deben ser objeto de administración y control.
4. **Elaboración del diagnóstico de riesgo:** se elabora un diagnostico general del riesgo que reflejan cada factor de riesgo identificado en las etapas anteriores, y se realiza una aproximación de lo que es el riesgo inherente de la empresa.
5. **Definición de las metodologías y herramientas para la gestión de riesgos:**En esta etapa es necesario definir las metodologías, técnicas, herramientas y fuentes de información para el diseño y adopción del sistema de gestión del riesgo.

1.8.2. Etapa 2. Identificación de los riesgos.

Tiene como principal objetivo, identificar cuáles son aquellos riesgos inherentes al desarrollo de la actividad de la empresa. Se trata de la identificación de eventos de riesgos para cada uno de los factores de riesgo y sus causas del diagnóstico realizado.

En esta etapa se hace uso de las matrices de riesgos, clasificando los riesgos, generalmente, en riesgo alto, medio y bajo. Se debe entender que puede suceder, cómo y por qué puede suceder, cuáles son esas causas principales que pueden materializar los eventos de riesgos identificados.

1.8.3. Etapa 3. Medición o evaluación de los riesgos.

La medición o evaluación de riesgos implica medir la probabilidad o posibilidad de ocurrencia del riesgo inherente de cada uno de los eventos de riesgo en cada una de las matrices de riesgos diseñadas para cada factor de riesgo, así como el impacto en caso de materializarse mediante los riesgos asociados. Las consecuencias y probabilidades se combinan para producir el nivel de riesgo.

Para el desarrollo de esta etapa se pueden describir dos pasos, primero, determinar los criterios para la medición de los riesgos y segundo, establecer los procedimientos para la medición de los riesgos.

Generalmente, se pueden utilizar los siguientes criterios de medición:

Tabla 2. Criterios para la medición de probabilidad e impacto.

PROBABILIDAD	IMPACTO
Muy Alta	Muy Alto
Alta	Alto
Media	Medio
Baja	Bajo
Muy Baja	Muy Bajo

Esta clasificación responde al nivel de pérdida o daño que podría resultar en caso de materializarse el riesgo y su consecuencia en los objetivos del sistema.

Para establecer los procedimientos de medición de los riesgos, los riesgos inherentes deben ser evaluados de acuerdo con la magnitud del impacto y la probabilidad de ocurrencia. Se deben priorizar aquellos riesgos que más afectan la operatividad de la empresa y clasificar los riesgos aceptables.

1.8.4. Etapa 4. Adopción de controles (Medidas Preventivas)

Esta etapa se caracteriza por establecer las medidas necesarias para controlar los riesgos y detectar actividades inusuales.

Los controles serán aquellas políticas, actividades y procedimientos que se desarrollan a través de toda la organización para eliminar o mitigar los riesgos adversos, y garantizar que las directrices de la dirección de la empresa se lleven a cabo y los riesgos se administren de manera que se cumplan los objetivos. El control se debe traducir en una disminución de la posibilidad de ocurrencia o del impacto del riesgo, en caso de materializarse. Estos se pueden clasificar de acuerdo con los tipos, formas, implementación, valoración y opciones de tratamiento tal como sigue:

- **Tipos de Controles**

Controles Preventivos: se aplica sobre la causa del riesgo y su agente generador, con el fin de disminuir la posibilidad de ocurrencia. Es el control que por excelencia debe aplicarse para prevenir el riesgo. Permite prevenir y resolver los problemas. (Cámara de Comercio de Bogotá, pág. 39).

Controles Detectivos: son los que pretenden detectar operaciones realizadas por las contrapartes (clientes, empleados, etc.) que puedan ser una alerta y constituirse en operaciones inusuales o sospechosas que deban ser reportadas a las autoridades.

- **Formas de Controles**

Controles Manuales: son todas aquellas acciones de las personas responsables que participan en el proceso de la gestión de riesgos.

Controles Automáticos: son procedimientos aplicados desde una computadora en un software de soporte; diseñados para prevenir, detectar o corregir errores o deficiencias, sin que tenga que intervenir el hombre en el proceso.

- **Clasificación de los controles sobre su implementación**

Implementado: los controles que se requieren ya han sido implementados y funcionan adecuadamente.

En desarrollo: en este caso los controles ya existen, pero por alguna razón aún no se han obtenido los resultados favorables que se esperan.

No existe: los controles aún no se implementan porque no han sido creados.

- **Valorización de los controles:**

Fuerte: los controles que se han implementado funcionan de manera adecuada.

Moderado: en los controles existentes se presentan algunas debilidades pero con un mejor diseño e implementación se pueden mejorar.

Débil: los controles existentes no son aceptables. Presentan fallas en su diseño e implementación que no permiten obtener los resultados esperados.

- **Tipos de controles por sus opciones de tratamiento:**

Evitar el riesgo: la empresa puede evitar los riesgos con mejores controles y evitar mayores costos en trabajos que permitan tener un riesgo aceptable.

Reducir la probabilidad de ocurrencia de los riesgos: se implementaran controles que permitan la minimización de los eventos de riesgos y se enfoca la atención en aquellos que sean más probables que se materialicen.

Aceptar los riesgos: se realizará un análisis de riesgos en donde se pueda concluir cuales son aquellos riesgos identificados que se encuentran dentro de los límites aceptables para el negocio, es decir eventos que a materializarse no afectaran drásticamente las operaciones realizadas.

Transferir riesgos: se pueden implementar controles como contratos con terceros, seguros, etc. De manera que exista un soporte que responda ante cualquier suceso.

1.8.5. Etapa 5. Divulgación y documentación (Capacitación y Consulta).

El principal objetivo de esta etapa es la de proveer un sistema de documentos y registro de las etapas y elementos de todo el modelo de gestión de riesgos, de manera que se garantice la integridad, oportunidad, confiabilidad y disponibilidad de la información contenida en el mismo.

Durante esta etapa se realiza una divulgación, tanto interna como externa, de todos los elementos contenidos en el modelo de gestión de riesgos, lo que permite el buen funcionamiento de los procesos y el logro de todos los objetivos establecidos. El componente principal en este punto, es el de brindar capacitaciones a todo el personal encargado, para que trabajen juntos en el logro de metas. Se tienen claras cuáles son cada una de las responsabilidades y obligaciones que tendrá cada persona y se entenderán las bases sobre las cuales se toman las decisiones y en todo caso, cuáles son las acciones a tomar en situaciones particulares.

Para esta etapa se determina cuáles serán los reportes incluidos en el sistema de divulgación de la información, los que pueden ser:

1. **Reportes internos**

- Transacciones inusuales.

- Operaciones sospechosas.
- Reportes en la etapa de seguimiento o monitoreo.

2. Reportes externos

- Reporte de operaciones sospechosas (ROS).
- Reporte de transacciones en efectivo, el cual se compone: i) de reporte de transacciones individuales en efectivo, y ii) de reporte de transacciones múltiples en efectivo.
- Otros reportes exigidos por las autoridades competentes.

1.8.6. Etapa 6. Seguimiento o monitoreo.

Se basa en realizar un seguimiento general del sistema, el cual deberá ser efectivo, que permita la detección temprana y la pronta solución a cualquier falla que se presente. Se debe asegurar que los controles sean comprensivos de todos los riesgos y que estos estén funcionando de forma oportuna y efectiva.

La principal herramienta del monitoreo o seguimiento, es la autoevaluación de riesgos y controles, con el fin de establecer un enfoque que examine y evalúe la efectividad del modelo. Una vez que se termina la implementación del sistema de gestión del riesgo, los gestores de riesgo deben realizar una labor de revisión y evaluación del mismo para verificar la pertinencia y suficiencia del proceso de administración de riesgos y de los controles implementados y corregir las posibles deficiencias detectadas.

1.9. Marco normativo.

1.9.1. Marco Legal.

TABLA N° 3: Legislación aplicable a las sociedades proveedoras de dinero electrónico.

NORMATIVA	REFERENCIA	DESCRIPCIÓN
Ley para facilitar la inclusión financiera. DECRETO N° 72, D.O. N° 160, Tomo N° 408.	TÍTULO PRIMERO Sociedades proveedoras de dinero electrónico. Art. 2.	Su finalidad se limitará a la de proveer dinero electrónico y también administrar u operar sistemas de pagos móviles con la autorización del Banco Central de Reserva.

NORMATIVA	REFERENCIA	DESCRIPCIÓN
<p>Fecha: 3 de septiembre de 2015.</p> <p>Esta ley establece los requisitos para la constitución y la operación de las empresas proveedoras de dinero electrónico, asimismo da la pauta para que los bancos, cooperativas y sociedades de ahorro y crédito puedan implementar esta modalidad.</p> <p>Define que es el dinero electrónico y sus principales características.</p>		<p>Las sociedades proveedoras se considerarán integrantes del sistema financiero (Asamblea Legislativa de la Republica de El Salvador, 2015)</p>
	<p>Dinero electrónico Art.5.</p>	<p>Es el valor monetario registrado a favor de un titular o cliente, que constituye una obligación de pago exigible a su proveedor, el cual es aceptado por los demás actores que hayan convenido recibir o prestar este servicio, como un medio de pago en un monto equivalente al dinero efectivo entregado, y se almacena en un soporte electrónico. Su titular podrá utilizarlo para hacer transferencias locales, pagos y conversión a dinero en efectivo al valor nominal.</p>
	<p>Art. 7.</p>	<p>Los proveedores de dinero electrónico deben contar con políticas internas en materia de gestión de riesgos, códigos de conducta y otro tipo de requisitos que les son exigidos por ser integrantes del sistema financiero.</p>
<p>Ley de supervisión y regulación del Sistema Financiero.</p>	<p>Art.3.</p>	<p>La Superintendencia es responsable de supervisar la actividad individual y consolidada de los integrantes del sistema financiero.</p>

NORMATIVA	REFERENCIA	DESCRIPCIÓN
<p>DECRETO No. 592, D.L. No. 64, 12 de julio de 2012.</p> <p>Establece las instituciones que conforman el sistema financiero así como las facultades que posee la Superintendencia para poder supervisar o intervenir si es que lo estima conveniente.</p>	<p>Supervisados. Art. 7 literal t)</p> <hr/> <p>Obligaciones de los supervisados. Art.35 literal d)</p>	<p>Las personas jurídicas que realizan operaciones de envío o recepción de dinero sistemática o sustantivamente, por cualquier medio, a nivel nacional e internacional.</p> <hr/> <p>d) adopción y actualización de políticas para la gestión de riesgos, debiendo identificarlos, evaluarlos, mitigarlos y revelarlos acordes a las mejores prácticas internacionales. En dichas políticas se deberán incluir las medidas que se adoptarán para prevenir posibles incumplimientos a requerimientos regulatorios y las que adoptarán en el evento de que haya incurrido en ellos, debiendo definir en ambas situaciones los parámetros que orientarán la actuación y los responsables de implementarlas. (Asamblea Legislativa de la Republica de El Salvador, 2012)</p>
<p>Ley contra el lavado de dinero y de activos.</p>	<p>Sujetos obligados. Art. 2 numeral 1</p>	<p>Toda sociedad, empresa o entidad de cualquier tipo, supervisado y regulado por la Superintendencia del Sistema Financiero.</p>

NORMATIVA	REFERENCIA	DESCRIPCIÓN
<p>DECRETO NO. 498Diario Oficial No. 240. Tomo No. 341, del 23 de diciembre de 1998.</p> <p>Establece todas las entidades obligadas a la aplicación de la ley así como los parámetros para identificar el delito de lavado de dinero y de activos, además de medidas preventivas que deben de tomar para prevenirlo, y las directrices a seguir en caso de operacionessospechosas.</p>	<p>Lavado de dinero y activos.</p> <p>Art.4.</p>	<p>El que depositare, retirare, convirtiere o transfiriere fondos, bienes o derechos relacionados que procedan directa o indirectamente de actividades delictivas, para ocultar o encubrir su origen ilícito.</p> <p>Se entenderá también por lavado de dinero y de activos, cualquier operación, transacción, acción u omisión encaminada a ocultar el origen ilícito y a legalizar bienes y valores provenientes de actividades delictivas cometidas dentro o fuera del país.</p>
	<p>Obligaciones de las instituciones sometidas al control de esta ley.</p> <p>Art.9.</p>	<p>Los sujetos obligados deberán informar a la UIF, por escrito o cualquier medio electrónico y en el plazo máximo de cinco días hábiles, cualquier operación o transacción de efectivo, fuere individual o múltiple, independientemente que se considere sospechosa o no, realizada por cada usuario o cliente que en un mismo día o en el término de un mes exceda los diez mil dólares.</p>
	<p>Art.9B.</p>	<p>Los sujetos obligados de esta ley, deberán establecer una política interna de debida diligencia para la identificación de sus usuarios o clientes.</p>

NORMATIVA	REFERENCIA	DESCRIPCIÓN
	Oficial de cumplimiento. Art. 14.	Los sujetos obligados deben establecer una oficialía de cumplimiento, a cargo de un oficial nombrado por la junta directiva u órgano competente.
<p>Reglamento de la ley contra el lavado de dinero y de activos.</p> <p>Facilita el entendimiento y lamejor aplicación de la Ley.</p>	<p>Obligaciones de las instituciones.</p> <p>Art.14.</p>	<p>Adoptar una política que garantice el conocimiento de sus clientes.</p> <p>Establecer procedimientos para asegurar un alto nivel de integridad del personal y un sistema de auditoría interna.</p> <p>Prestar la asistencia técnica que les sea requerida por la UIF, cuando se trate de investigaciones relacionadas con el delito de lavado de dinero y de activo.</p>
	<p>Transacciones irregulares o sospechosas.</p> <p>Art.12.</p>	<p>Operaciones poco usuales, las que se encuentran fuera de los patrones de transacción habituales y las que no sean significativas pero sí periódicas, y todas aquellas operaciones inconsistentes o que no guardan relación con el tipo de actividad económica del cliente.</p>
<p>Ley especial contra actos de terrorismo.</p> <p>DECRETO No. 108 D.O: 193, Tomo: 373,</p>	<p>Financiación de actos de terrorismo.</p> <p>Art. 29.</p>	<p>El que por cualquier medio, directa o indirectamente, proporcione, recolecte, transporte o tuviere en su poder fondos, ayudare o tratare de favorecer servicios financieros u otros servicios con la</p>

NORMATIVA	REFERENCIA	DESCRIPCIÓN
Publicación DO: 10/17/2006.		<p>intención de que se utilicen, total o parcialmente para cometer cualquiera actos de terrorismo, será sancionado con prisión de veinte a treinta años, y multa de cien mil a quinientos mil dólares.</p> <p>Así mismo incurrirá en la misma sanción el que, directa o indirectamente, pusiere fondos, recursos financieros o servicios financieros, a disposición de personas o en entidades que los destine a la comisión de alguno de los delitos previstos en esta Ley. (Asamblea Legislativa de la Republica de El Salvador, 2006)</p>
Normas técnicas para el inicio de operaciones y funcionamiento de los proveedores de dinero electrónico.	CAPÍTULO VIII Control interno. Art.32 y 33.	<p>Los proveedores por medio de sus distribuidores y puntos de atención, cumplirán con el marco legal y regulatorio en materia de prevención de lavado de dinero y de activos y financiamiento al terrorismo, debiendo contar con un manual en dicha materia.</p> <p>Los proveedores deberán establecer un sistema de gestión integral de riesgos, en el cual identifiquen, midan, controlen y monitoreen los distintos tipos de riesgos a que se encuentran expuestos. deberá contar con medidas para mitigar o cubrir los riesgos asociados a la</p>

NORMATIVA	REFERENCIA	DESCRIPCIÓN
		realización de la prestación del servicio, incluyendo aquellas relacionadas con la prevención de lavado de dinero y de activos y financiamiento al terrorismo, deberán incluir, entre otros, el establecimiento de límites para la prestación de servicios, como monto por operación y número de transacciones. (Comité de Normas del Banco Central de Reserva de El Salvador, 2016)
<p>Convenio Centroamericano para la prevención y la represión de los delitos de lavado de dinero y de activos, relacionados con el tráfico ilícito de drogas y delitos conexos.</p>	Art. 10 literal c)	Las entidades de intermediación financiera y las que realicen actividades financieras, serán objeto de control por las autoridades competentes de los estados parte. Asimismo, las personas que realicen las siguientes actividades: c) Transferencias sistemáticas o sustanciales de fondos, realizadas por cualquier medio.(Organización de las Naciones Unidas , 1997)
	Art. 14.	Las entidades de intermediación financiera y las que realicen actividades financieras, prestarán atención especial a las transacciones, efectuadas en forma sospechosa. Esas entidades deberán comunicar, de inmediato, a las autoridades competentes la sospecha de que las transacciones puedan constituir

NORMATIVA	REFERENCIA	DESCRIPCIÓN
		actividades ilícitas o estar relacionadas con ellas. (Organización de las Naciones Unidas , 1997)

1.9.2. Marco Técnico.

TABLA N° 4: Normativa técnica aplicable a las sociedades proveedoras de dinero electrónico.

NORMATIVA TÉCNICA	APLICACIÓN	DESCRIPCIÓN
Cuarenta recomendaciones del Grupo de Acción Financiera Internacional (GAFI).	A. Políticas y coordinación ALA/CFT.	1. Evaluación de riesgos y aplicación de un enfoque basado en riesgo. 2. Cooperación y coordinación nacional.
	B. Lavado de activos y decomiso.	3. Delito de lavado de activos. 4. Decomiso y medidas provisionales.
	C. Financiamiento del terrorismo y financiamiento de la proliferación.	5. Delito de financiamiento al terrorismo. 6. Sanciones financieras dirigidas relacionadas al terrorismo y al financiamiento al terrorismo. 7. Sanciones financieras dirigidas relacionadas con la proliferación. 8. Organizaciones sin fines de lucro.
	D. Medidas preventivas.	9. Leyes sobre el secreto de las instituciones financieras. Debida diligencia del cliente y mantenimiento de registros: 10. Debida diligencia del cliente. 11. Mantenimiento de registros. Medidas adicionales para clientes y actividades específicas: 12. Personas expuestas políticamente.

NORMATIVA TÉCNICA	APLICACIÓN	DESCRIPCIÓN
		<p>13. Banca corresponsal.</p> <p>14. Servicios de transferencia de dinero o valores.</p> <p>15. Nuevas tecnologías.</p> <p>16. Transferencias electrónicas.</p> <hr/> <p>Dependencia, controles y grupos financieros:</p> <p>17. Dependencia en terceros.</p> <p>18. Controles internos y sucursales y filiales extranjeras.</p> <p>19. Países de mayor riesgo.</p> <hr/> <p>Reporte de operaciones sospechosas:</p> <p>20. Reporte de operaciones sospechosas.</p> <p>21. Revelación (tipping-Off) y confidencialidad.</p> <hr/> <p>Actividades y profesiones no financieras designadas (APNFD):</p> <p>22. APNFD: Debida diligencia del cliente.</p> <p>23. APNFD: Otras medidas.</p>
	E. Transparencia y beneficiario final de las personas jurídicas y otras estructuras jurídicas.	<p>24. Transparencia y beneficiario final de las personas jurídicas.</p> <p>25. Transparencia y beneficiario final de las estructuras jurídicas.</p>
	F. Facultades y responsabilidades de las autoridades competentes y otras medidas institucionales.	<p>Regulación y supervisión:</p> <p>26. Regulación y supervisión de instituciones financieras.</p> <p>27. Facultades de los supervisores.</p> <p>28. Regulación y supervisión de las</p>

NORMATIVA TÉCNICA	APLICACIÓN	DESCRIPCIÓN
		<p>APNFD.</p> <p>Operativo y orden público:</p> <p>29. Unidades de Inteligencia Financiera.</p> <p>30. Responsabilidades de las autoridades del orden público e investigativas.</p> <p>31. Facultades de las autoridades del orden público e investigativas.</p> <p>32. Transporte de efectivo.</p> <p>Requisitos generales:</p> <p>33. Estadísticas.</p> <p>34. Guía y retroalimentación.</p> <p>Sanciones:</p> <p>35. Sanciones.</p>
	G. Cooperación internacional.	<p>36. Instrumentos internacionales.</p> <p>37. Asistencia legal mutua.</p> <p>38. Asistencia legal mutua: congelamiento y decomiso.</p> <p>39. Extradición.</p> <p>40. Otras formas de cooperación internacional.</p>
<p>ISO 31000:2009.</p> <p>Gestión de riesgos</p> <p>Principios y directrices.</p>	Principios para la gestión de riesgos.	<p>1. Crear valor.</p> <p>2. Está integrada en los procesos de una organización.</p> <p>3. Forma parte de la toma de decisiones.</p> <p>4. Trata explícitamente la incertidumbre.</p> <p>5. Es sistemática, estructurada y adecuada.</p>

NORMATIVA TÉCNICA	APLICACIÓN	DESCRIPCIÓN
		<ol style="list-style-type: none"> 6. Está basada en la mejor información disponible. 7. Está hecha a medida. 8. Tiene en cuenta factores humanos y culturales. 9. Es transparente e inclusiva. 10. Es dinámica, interactiva y sensible al cambio. 11. Facilita la mejora continua de la organización.
	Estructura de soporte.	<ol style="list-style-type: none"> 1. Compromiso de la dirección. 2. Diseño de la estructura de soporte. 3. Implantación de la gestión del riesgo. 4. Seguimiento y revisión de la estructura. 5. Mejora continua de la estructura
	Proceso de gestión de riesgos.	<ol style="list-style-type: none"> 1. Establecer el contexto. 2. Evaluación de riesgos: <ul style="list-style-type: none"> • Identificar los riesgos. • Analizar los riesgos. • Evaluar los riesgos. • Tratar los riesgos. 3. Comunicación y consulta. 4. Seguimiento y revisión.
Instructivo de la Unidad de Investigación Financiera para la prevención del lavado de dinero y de activos.	CAPÍTULO I. Objeto y Sujetos obligados. Art. 1 y 2.	El instructivo tiene por objeto desarrollar las obligaciones de los sujetos obligados establecidas en la Ley contra el lavado de dinero y de activos, y su Reglamento, relacionadas a la prevención y reporte de

NORMATIVA TÉCNICA	APLICACIÓN	DESCRIPCIÓN
<p>Acuerdo No. 085. Fiscalía General de la República. D. O. Tomo No. 400 de fecha 01 de julio de 2013.</p>		operaciones, las acciones de prevención y reporte de aquellas operaciones relacionadas con el lavado de dinero y de activos.
	<p>CAPÍTULO III Debida diligencia en la identificación y conocimiento del cliente. Art. 6.</p>	La forma más importante para evitar el riesgo de que se involucre y utilice a las instituciones, como intermediarias en operaciones ilícitas, es precisamente la correcta aplicación del “Conocimiento del cliente”.
	<p>CAPÍTULO IV Operaciones sospechosas o irregulares. Art. 9.</p>	Las instituciones, deberán elaborar manuales de operación, los cuales deberán ser aprobados por su administración superior, mismos que contendrán los criterios y bases para considerar las operaciones como sospechosas, así como desarrollar sistemas manuales o de computo, que les permitan documentar los procesos.
	<p>CAPÍTULO V Procedimientos. Art. 11.</p>	Los manuales de las instituciones, deberán contener las bases y procedimientos para la prevención de lavado de dinero y activos. Estos manuales deberán ser aprobados por el órgano de administración superior u órgano equivalente, necesariamente debe ser de conocimiento de todo el personal de la institución y tenerse a disposición de la UIF y los auditores externos.

NORMATIVA TÉCNICA	APLICACIÓN	DESCRIPCIÓN
	CAPÍTULO VI Archivo y conservación de documentos. Art. 13.	Las copias de los formularios y reportes, así como de los documentos relativos a la identificación de los clientes, se conservaran por un periodo no menor a cinco años.
	CAPÍTULO VII Capacitación y difusión. Art. 14.	Las instituciones estarán obligadas a desarrollar programas de capacitación y difusión al personal responsable de la aplicación de las disposiciones, al directorio y gerentes según sus cargos y funciones, expidiendo las constancias correspondientes.
	CAPÍTULO VIII Oficial de Cumplimiento. Art. 15.	Las instituciones instituirán una oficina de cumplimiento, la cual será dirigida por un oficial de cumplimiento, aprobado por el órgano superior de administración, el nombrado debe ostentar como mínimo, un cargo gerencial con facultad para la toma de decisiones, las cuales deben ser vinculantes para toda la institución.
Norma técnica para gestión de los riesgos de lavado de dinero y de activos y financiamiento al terrorismo. (NRP-08).	CAPÍTULO I Objeto, sujetos y términos. Art. 1. Art. 2 literal s)	El objeto de estas normas es proporcionar los lineamientos mínimos para la adecuada gestión del riesgo de lavado de dinero y de activos, a fin de que las entidades integrantes del sistema financiero prevengan y detecten operaciones irregulares relacionadas con el referido riesgo, de forma oportuna. Los sujetos obligados al cumplimiento de

NORMATIVA TÉCNICA	APLICACIÓN	DESCRIPCIÓN
		<p>las presentes normas son:</p> <p>s) Cualquier otra sociedad o institución que en razón de su giro o actividad pase a formar parte integrante en el futuro del sistema financiero.</p>
	<p>CAPÍTULO II</p> <p>Entorno para la gestión de los riesgos de LD/FT.</p> <p>Programas de capacitación.</p> <p>Art. 8.</p>	<p>Las entidades deben desarrollar e implementar programas de inducción al personal de nuevo ingreso, en materia de prevención de lavado de dinero y financiamiento al terrorismo, así mismo desarrollar e implementar un programa anual de capacitación al personal responsable de la aplicación de la regulación sobre prevención de lavado de dinero y financiamiento al terrorismo, según sus funciones, así como a sus directivos, miembros de comités y gerentes según sus cargos y funciones.</p>
	<p>Auditoría interna.</p> <p>Art. 9.</p>	<p>Auditoría interna deberá evaluar la gestión de la Oficialía de Cumplimiento e informar a Junta Directiva tanto de los hallazgos de auditoría en la materia como de los resultados de la evaluación de la gestión de la Oficialía.</p>
	<p>CAPÍTULO III</p> <p>Gestión de los riesgos de LD/FT.</p>	<p>Etapas del proceso de gestión. Art. 11:</p> <ul style="list-style-type: none"> • Identificación. Art. 12. • Medición. Art. 13. • Control y mitigación. Art. 14. • Monitoreo y comunicación. Art. 15.

NORMATIVA TÉCNICA	APLICACIÓN	DESCRIPCIÓN
	Factores de riesgo. Art. 16.	Las entidades deben establecer las metodologías para segmentar los factores de riesgo e identificar las formas y tipologías a través de las cuales se puede presentar este riesgo, siendo los principales agentes generadores del riesgo de LD/FT, entre otros: clientes, productos, servicios, canales de distribución, y ubicación o localización geográfica.
	CAPÍTULO IV Debida diligencia. Art. 17.	Las entidades deberán aplicar la debida diligencia, lo cual implicará que estas implementen los procedimientos y controles para valorar, identificar y verificar la identidad de sus clientes y beneficiarios finales, monitorear sus operaciones, a efecto de gestionar adecuadamente el riesgo de LD/FT.
	CAPÍTULO V Monitoreo de transacciones y herramientas informáticas. Análisis de alertas. Art. 26.	La Oficialía de Cumplimiento y otras áreas responsables de la entidad deben realizar una revisión de las alertas de acuerdo con el nivel de riesgo identificado, con el objetivo de identificar las transacciones inusuales o sospechosas a las que debe realizarse seguimiento.

CAPÍTULO II: METODOLOGÍA Y DIAGNÓSTICO DE LA INVESTIGACIÓN.

2.1. Procesamiento de la información.

La información obtenida a través de la técnica de la entrevista con el personal responsable de la empresa TigoMoney, fue consolidada y analizada según la guía de preguntas, de manera que se pudo concluir sobre la situación actual de la problemática. Se presentan los datos de forma resumida en pocos puntos, entre ellos se encuentran las fallas en el sistema y las medidas que se toman en cuenta para mitigarlas. Para esto se hizo uso de equipos de grabación y programas de procesamiento de textos y bases de datos como Microsoft Word, entre otros.

2.2. Tipo de estudio.

El estudio que se realizó fue de naturaleza descriptiva, ya que con él se identificaron los diferentes riesgos a los que están expuestos las sociedades autorizadas de proveer dinero electrónico en El Salvador, al momento en que se realizan operaciones con el sistema de dinero electrónico y no contar con un modelo de gestión de riesgos, que les permita detectar a tiempo alguna deficiencia o cometimiento de delitos por parte de los clientes, para esto se hizo uso de diversos instrumentos y técnicas de recolección de datos, lo que permitió realizar un análisis para comprobar las hipótesis planteadas, por lo que el estudio llevado a cabo, se realizó por medio del método hipotético deductivo.

2.3. Unidades de análisis.

La principal unidad de análisis para la realización de esta investigación fue la Sociedad Mobile Cash, S.A. de C.V., conocida como TigoMoney, quien funciona como única empresa autorizada de proveer dinero electrónico actualmente en el país.

2.4. Universo y muestra.

La unidad de análisis para el desarrollo de esta investigación contó con un solo elemento debido a que hasta la fecha solo Mobile Cash, S.A. de C.V. funciona como sociedad autorizada para trabajar con el sistema de dinero electrónico en el país, si bien cuenta con más de 2,500 agentes autorizados a nivel nacional bajo el nombre comercial de TigoMoney, estos operan bajo las mismas políticas de la empresa.

2.5. Instrumentos y técnicas utilizadas en la investigación.

- **Recopilación bibliográfica.**

Esta se efectuó por medio de la obtención de información teórica que sustenta el marco técnico y legal, esto a través del uso de fuentes bibliográficas como libros, revistas, periódicos, páginas web, boletines, etc.

- **La entrevista**

Con esta técnica se obtuvo información relacionada con la problemática, por medio de las experiencias de Mobile Cash, S.A. de C.V., respecto al tratamiento en la mitigación de riesgos en la operatividad del sistema de dinero electrónico. Esta técnica se desarrolló a través de una guía de preguntas como herramienta de recopilación de datos.

2.6. Análisis e interpretación de la información.

Se realizó un análisis de todas las respuestas obtenidas para cada una de las interrogantes planteadas en la guía de preguntas, de tal forma que se pueda realizar un diagnóstico preciso de los riesgos existentes y plantear posibles soluciones a la problemática, esto permitirá una mejor comprensión de los datos y el desarrollo de un modelo eficaz para la gestión de riesgos contra el lavado de dinero y activos, mediante el uso del actual sistema de dinero electrónico en nuestro país. (ANEXO 1)

2.7. Diagnóstico de la investigación.

Planteamiento del diagnóstico de la problemática

De acuerdo a la investigación realizada, actualmente la empresa TigoMoney, dedicada a proveer dinero electrónico en el país, trabaja en la gestión de riesgos relacionados con los delitos de lavado de dinero, esta gestión ha sido más efectiva desde la entrada en vigencia de la Ley para facilitar la inclusión financiera, la cual establece en su artículo uno, literales b y d, los requisitos que se deben cumplir para la constitución de las sociedades antes mencionadas, así como las consecuencias penales y legales de incumplirlos, y el control que están deben tener sobre los montos de dinero que se deben admitir en la plataforma electrónica, justo en ello la empresa ha establecido nuevos límites para transferencias, paso de ser \$ 5,000.00 a \$ 750.00 mensuales, lo que permite que los clientes no realicen transferencias con grandes montos, lo que evita el cometimiento de delitos. Sin embargo, pese a que existe un manual de políticas y procedimientos para esta gestión, se necesitan herramientas más completas, que engloben cada área de operación, como ejemplo: manuales para oficiales de cumplimiento, manuales para el comité de riesgos, planes de trabajo y planes de capacitación al personal.

La empresa realiza prácticas de debida diligencia, como las contempladas en la norma para la gestión de riesgos de lavado de dinero y activos y financiamiento al terrorismo NRP-08, en su artículo 17, que establece procedimientos que se deben implementar para la verificación de la identidad de sus clientes. No obstante, se deben realizar nuevos requerimientos de identificación para el caso de las Personas Políticamente Expuestas (PEP's), ya que la misma norma nos indica la aplicación de medidas adicionales para clientes como estos, de manera; que se pueda tener todo un perfil de identidad adecuado, actualmente la entidad registra de la misma forma, cualquier tipo de persona como cliente, sean estos clientes normales o PEP's, dejando de lado el cumplimiento el marco normativo.

La gestión de riesgos en la entidad, implica la elaboración de herramientas que permitan medir la posibilidad de ocurrencia de cualquier evento, para que a partir de estos resultados, se puedan tomar las mejores decisiones ya sea para mitigar, reducir, aceptar o transferir dicho riesgo. La empresa trabaja en la elaboración de planes de contingencia que le permite tomar acciones de prevención de delitos; pero necesita incluir en estos planes la elaboración de matrices que midan los riesgos por su probabilidad e impacto, sacando conclusiones de que riesgos son tolerables y aquellos que necesitan especial atención para mitigarlos.

Por el tipo de servicio que se brinda, es necesario contar con un software adecuado, que permita dar cobertura en todo el país y emitir a tiempo alertas sobre sospechas. Los reportes elaborados para informar a la UIF sobre cualquier operación sospechosa, son elaborados únicamente si existe un cliente que sobrepasa los parámetros de dinero establecidos. Dichos reportes necesitan ser más completos y automatizados para que las alertas puedan llegar más rápido a las autoridades pertinentes y se pueda comenzar una investigación; también se deben realizar no solo en estos casos, sino en muchos otros eventos que dan indicio que se está frente a un posible delito, como realizar operaciones más recurrentes, por ejemplo. Además, para que esta medida sea realmente eficaz, se debe realizar una actualización constante de la información de los clientes y proveerla a la UIF; además de seguir el rastro de la investigación que se le da a estos reportes, que servirá de base para tomar la decisión de mantener inactivas las cuentas reportadas por cuestión de seguridad. Un factor importante que se debe trabajar para la prevención de delitos, es la creación de planes de capacitación al personal, que permita transmitir los conocimientos necesarios en materia de lavado de dinero, tanto en el aspecto legal como normativo. Se debe realizar capacitaciones principalmente a los agentes autorizados, ya que ellos son los que realizan la función de aplicar la debida diligencia del cliente. Estas capacitaciones al personal deben ir acompañados, de una programación constante de evaluaciones, para que se pueda medir el grado de

conocimiento de cada empleado. Porque si bien estas evaluaciones ya se llevan a cabo, es necesario que se realicen con más frecuencia.

En cuanto al establecimiento de una nueva unidad, dentro de la entidad, que coordine el trabajo de la gestión de riesgo, aun no se ha establecido una estructura organizacional clara; si bien, existe un Comité de Aseguramiento de Ingresos, este está encargado de todas las áreas de negocios de TigoMoney, y este trabajo es realmente arduo, se necesita realizar una división especial para los negocios con dinero electrónico, que es la más expuesta a los eventos de riesgos de blanqueo de capitales, contar con una Oficialía de Cumplimiento permitirá que se trabaje con mayor énfasis en la prevención de estos.

Las deficiencias que más se destacan en la entidad, para llevar a cabo una eficaz gestión de riesgos, son la falta de políticas y procedimientos relacionados con los límites de fondos mantenidos en cada cuenta, se debe poner en practica la debida diligencia para los clientes de destino y aplicar medidas adicionales de identificación cuando sea una PEP's quien apertura la cuenta. Además, se debe establecer una estructura organizativa con líneas de trabajo más definidas y crear los planes de trabajo necesarios, para cada unidad encargada de la gestión de eventos y para el personal encargado del registro de los clientes.

Actualmente, la empresa TigoMoney trabaja constantemente en la gestión de riesgos de lavado de dinero; sin embargo, se destaca la importancia de la existencia de un modelo como herramienta para prevenir estos eventos, se necesita de un orden lógico, que permita a la entidad trabajar paso a paso y construir una base fuerte (basado en leyes y normas aplicables), para asegurar que no está siendo objeto de actividades ilícitas. Un modelo de gestión de riesgos permitirá tener un enfoque más amplio de lo que se quiere lograr, es por ello que junto con el trabajo realizado por la empresa y la propuesta de este tema de investigación, se pretende obtener una herramienta eficaz para prevenir delitos de este tipo, que ayude tanto a la entidad actual como a futuras sociedades de este giro, en el país.

CAPÍTULO III: MODELO DE GESTIÓN DE RIESGOS DE LAVADO DE DINERO Y ACTIVOS

3.1. Desarrollo del sistema de gestión de riesgos.

3.1.1. Introducción.

Hasta hace no mucho tiempo, la prevención de delitos de lavado de dinero y activos y financiamiento al terrorismo, se consideraba más un asunto de instituciones bancarias; sin embargo, la dinámica actual de diversos modelos de blanqueo de capitales demuestra que el lavado de dinero no es sólo un problema de bancos. Cualquier institución o empresa que maneja dinero en efectivo o crédito, puede ser víctima de este delito con el riesgo e impacto que implica en su reputación y competitividad en el mercado.

Tal es el caso de las sociedades proveedoras de dinero electrónico, cuyo servicios ofrecidos son blanco fácil para el cometimiento de delitos de lavado de dinero. Primeramente, por tratarse de una nueva tecnología que acerca a más personas a ser parte integrante del sistema financiero y segundo porque solo con el hecho de que una persona tenga a su alcance un teléfono móvil puede solicitar una cuenta de dinero electrónico y con ella realizar diferentes operaciones, desde la comodidad de su casa o en un lugar cercano a su residencia donde se encuentre un punto de atención de agentes autorizados.

Los riesgos de lavado de dinero a los que puede estar expuesto una sociedad proveedora de dinero electrónico, son tanto internos como externos, y pueden tener su origen debido a la ausencia de controles y políticas claramente definidas para poder prevenirlos.

Se sabe que uno de los bienes más preciados para las empresas es el buen nombre y la reputación, por lo que la implementación de un sistema de gestión de riesgos de lavado de dinero se convierte en una necesidad real, el cual se logra con mayores esfuerzos para implementar los controles necesarios para reducir los riesgos ya que, entre otras cosas, el incumplimiento con los requerimientos legales podría implicar sanciones y multas millonarias, deterioro de la relación con los clientes y otras entidades relacionadas, prisión y no solo el daño reputacional latente.

La aplicación de un sistema de gestión de riesgos de lavado de dinero definido en diferentes etapas complementarias, permitirá que la entidad pueda obtener resultados más favorables en este trabajo de gestión que realiza, con esta metodología se identifican los principales riesgos por factor, determinando

cuales de estos son aceptables y los que significan un impacto negativo para las operaciones normales del negocio.

3.1.2. Objetivos

Objetivo General:

Proporcionar los elementos claves para que las sociedades proveedoras de dinero electrónico, desarrollen un sistema efectivo para la gestión de los riesgos de lavado de dinero y activos y financiamiento al terrorismo, basado en la legislación y normativa local e internacional aplicable, que permita la correcta identificación, evaluación, control y monitoreo de estos eventos.

Objetivos Específicos:

- a) Dar a conocer a los miembros de la empresa los riesgos de lavado de dinero y activos a los que se tiene mayor exposición en el curso normal de las operaciones efectuadas.
- b) Presentar las medidas o controles que se pueden implementar para prevenir dichos riesgos.
- c) Sugerir una metodología sencilla de implementación y mantenimiento de dichas medidas.

3.1.3. Estructura del sistema de gestión de riesgos de lavado de dinero y activos.

Este sistema está diseñado para ayudar a la empresa a fortalecer e implementar medidas preventivas o controles, con el fin de garantizar su permanencia, transparencia y reputación al verse involucrada en actividades ilícitas. Estas medidas se convertirán en una buena práctica y formarán parte de la cultura empresarial de la entidad. Es un sistema definido mediante una metodología paso a paso, para integrar las medidas de mitigación de riesgos sugeridas, a las estrategias, políticas, procesos y procedimientos existentes en el negocio.

En la elaboración de este modelo, se ha tomado en cuenta la aplicación de estándares internacionales, como las Normas del Grupo de Acción Financiera Internacional (GAFI) y Normas ISO 31000; además de normas locales, como las emanadas por el Banco Central de Reserva de El Salvador para la gestión de riesgos (Normas técnicas para la gestión de los riesgos de lavado de dinero y de activos y de financiamiento al terrorismo-NRP-08). Así mismo el cumplimiento de leyes, como la Ley para facilitar la inclusión financiera y la Ley contra el lavado de dinero y activos, en conjunto con información complementaria, como el instructivo de la Unidad de Investigación Financiera de la Fiscalía General de la República.

El sistema se compone de seis etapas principales, cada una con diversos puntos desarrollados para una mejor comprensión, por parte de los usuarios. Primeramente se describe un diagnóstico sobre la situación actual de la entidad en su contexto interno y externo sobre la exposición a los riesgos de lavado de dinero, en esta etapa se conoce cuál es el compromiso que los dueños, alta gerencia y directivos tienen con la entidad, para trabajar sobre la gestión de riesgos, herramientas como cartas de compromiso, códigos de ética, normas internas, son las utilizadas para medir dicho compromiso.

En la etapa número dos, denominada identificación de eventos, se muestra una lista de eventos de riesgos detectados para cada uno de los factores establecidos en el diagnóstico y se determinan cuáles son las posibles causas que los originan.

Para la medición o evaluación de los riesgos, etapa tres del sistema, se realiza una clasificación de riesgos por probabilidad e impacto, se plasman sobre una matriz de riesgo, realizando un análisis, sobre qué riesgos serán considerados de alto impacto y cuáles serán aquellos riesgos tolerables para el negocio, este análisis servirá de base para establecer los procedimientos necesarios a aplicar para la minimización de ocurrencia de estos eventos de riesgo.

La etapa número cuatro, trata sobre qué controles se adoptarán para mitigar cada uno de los riesgos identificados, para ello se hará uso de controles detectivos y preventivos, tales como manuales, reportes de operaciones inusuales, programas de trabajo, etc.

La etapa cinco, divulgación y documentación, desarrolla un mecanismo de registro de cada una de las etapas y elementos que conforman el sistema de gestión de riesgos, y define los procedimientos para la realización de reportes, la ejecución de programas de capacitación y planes de divulgación para cada miembro de la organización.

Por último, se definen las actividades de monitoreo que se llevarán a cabo, para verificar el cumplimiento de todo el ciclo de vida del sistema creado, y se establecen las medidas correctivas que se han de utilizar, en caso de ocurrir fallas.

De manera ilustrativa el proceso de gestión de riesgos definido en el sistema se puede presentar como sigue:

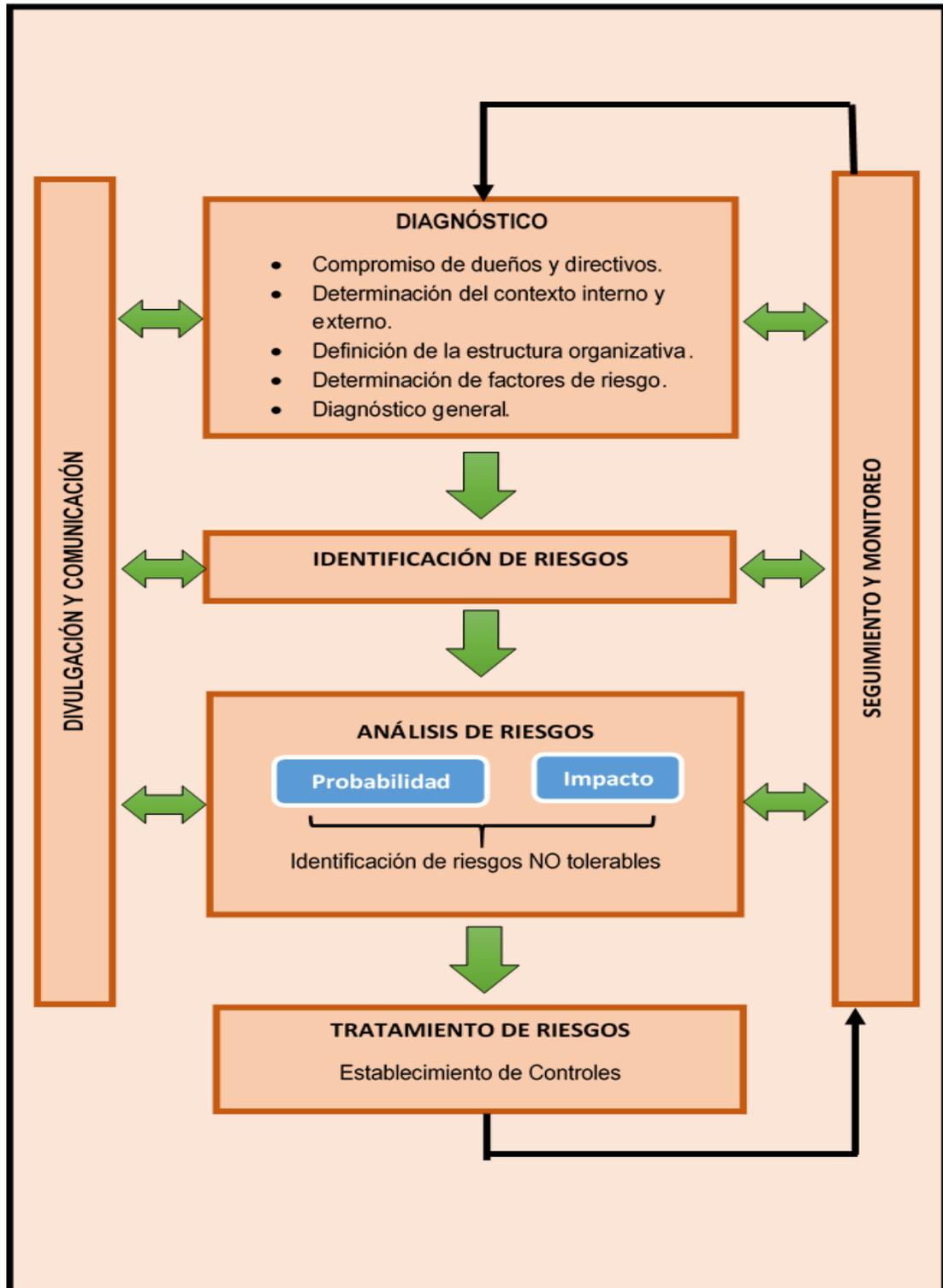


Figura 3:Proceso de gestión de riesgo.**Fuente:** ISO 39000-2009.

3.1.4. Caso práctico.

Información general de la sociedad.

La empresa ElectroniCash, es una Sociedad Anónima de Capital fijo, proveedora de dinero electrónico en El Salvador. Con oficinas centrales en la Colonia Escalón, Pasaje Maracaibo N° 521-A, San Salvador. Fue constituida en el año 2011, como parte de una alianza con la compañía telefónica TELECEL, quien es el mayor operador de telefonía móvil en el país, contando con más de 2.1 millones de usuarios en todo el país.

ElectroniCash, inició operaciones con un número promedio de doscientos setenta y cinco empleados, y con setenta y cinco puntos de atención en la zona metropolitana de San Salvador. Su giro empresarial es la de proveer dinero electrónico a través de plataformas virtuales, que son utilizadas en teléfonos celulares. Según los últimos informes financieros, son alrededor de 1.1 millones de dólares en transacciones realizadas en un mes. De las cuales un 45% corresponde a transferencias de dinero locales, 20% al pago de facturas de servicios básicos, 20% a recargas a teléfonos móviles, 7% pago de cuentas en restaurantes y un 8% a compras en supermercado.

Cuenta con un total de nueve socios, quienes enfocaron sus esfuerzos en la generación de un servicio novedoso que permita a todos los salvadoreños ser parte del sistema financiero, mediante la inclusión financiera. Su estrategia de negocios fue la utilizar la tecnología actual de la telefonía celular, a la que tienen acceso casi todos los habitantes de este país, para que realicen transacciones de una manera más segura y rápida.

Misión, visión y valores.

La misión bajo la cual opera la sociedad es:

“Brindar el mejor servicio de dinero electrónico a nuestros clientes, con el cual podrán hacer sus transacciones de dinero de una manera más cómoda y práctica, mejorando así el estilo de vida de clientes, proveedores y colaboradores y fomentando una cultura de inclusión financiera en nuestro país”.

La visión de la empresa es:

“Convertirnos en la empresa número uno en proveer dinero electrónico en el país y en la región centroamericana, estandarizando nuestros procesos de servicios y mejorando la calidad de atención a nuestros clientes”.

Los valores en la organización son:

“Somos una empresa novedosa que mantiene el respeto tanto con nuestros clientes como con los compañeros de trabajo, proveedores y sociedad en general. Somos honestos y responsables en todas las labores de la empresa y también personales; desarrollando todo nuestro potencial dentro de la empresa con constancia y disciplina”.

Información sobre los agentes autorizados.

Actualmente la empresa ElectroniCash, cuenta con setecientos treinta y cinco puntos de atención en doscientos municipios de todo el país, estos puntos de atención son alianzas que se han realizado con pequeños y microempresarios para que ellos sirvan como intermediarios en los servicios ofrecidos, de manera que todos los clientes, en todo el país tengan fácil acceso al sistema. Ejemplos de estos puntos de atención son farmacias, tiendas y supermercados.

Para ser parte del negocio, los pequeños o microempresarios deben realizar y cumplir con ciertos requisitos, que los convierte en agentes autorizados en prestar los servicios, entre los que podemos mencionar los siguientes:

- Formulario de inscripción de agentes autorizados debidamente llenado y firmado por la persona responsable del negocio.
- Fotocopia legible de los documentos personales.
- Declaración Jurada sobre el compromiso de realizar operaciones de manera lícita.

Necesidad de un modelo.

Actualmente, ElectroniCash no cuenta con una estructura organizativa clara, ya que no se tiene la formación de un comité establecido para la gestión de eventos. Además, con lo que respecta al trabajo de un Oficial de Cumplimiento dentro de la entidad, por el momento solamente una persona es la encargada de la supervisión en la prevención de riesgos para toda la gama de servicios prestados, y no se cuenta con un plan o programa de trabajo específico para realizar esta acción.

Para la divulgación de las políticas y procedimientos establecidos para prevenir delitos de lavado de dinero, por el momento no se tiene un plan definido, que permita transmitir la información a todos los miembros de la entidad, cuyos cargos tienen relación directa con los clientes. De igual manera, las capacitaciones impartidas al personal, no se realizan de forma regular, lo que indica una deficiencia en

cuanto a la actualización en materia de prevención de delitos; esta deficiente actividad, surge debido a que no se cuenta con los planes de capacitación necesarios, que proporcionen una guía y programación, para mantener al personal debidamente capacitado para realizar sus operaciones.

En la actividad económica habitual de la empresa, los riesgos provenientes de factores internos, como la falta o debilidad de los controles, insuficiencia de políticas y procedimientos o la ausencia de valores institucionales fuertes que prevengan la complicidad con actividades ilegales, son los que más amenazan a la entidad. Por otra parte, factores externos como los clientes y zonas geográficas donde se ubican los puntos de atención, requieren de atención especial, ya que son un canal que puede involucrar al negocio, directa o indirectamente, en actividades ilegales.

Estas amenazas latentes en el entorno, son las que han levantado la sospecha que los servicios prestados por la empresa, estén siendo objeto de actividades ilícitas relacionadas con los delitos de lavado de dinero y activos, que han afectado su imagen y su situación financiera. Por estas deficiencias descritas anteriormente, los dueños han tomado la decisión de establecer un sistema de gestión de riesgos como herramienta en la prevención de delitos de lavado de dinero y activos y financiamiento al terrorismo.

3.2. Etapa 1: Diagnóstico

3.2.1. Compromiso de dueños y directivos en la gestión de riesgos.

Al evaluar, mediante una serie de entrevistas directas y con la documentación de respaldo existente, el nivel de compromiso que los dueños y directivos de ElectroniCash tienen en el trabajo de prevención de riesgos de lavado de dinero y activos, se detectó que estos no cuentan con un código de ética, que establezca las normas básicas del comportamiento ético y moral que todos los miembros de la organización deben tener para llevar a cabo sus funciones y/o actividades.

Además, en la información presentada por la oficialía de cumplimiento, se constató que no existe un documento que ampare o garantice la lealtad de sus empleados en el desarrollo de sus cargos. Para esto es necesario, que la entidad celebre actas de compromiso, por cada nueva relación laboral entre patrono y empleado, que sirva de salvaguarda para la empresa, en caso de que un empleado se vea implicado con delitos de lavado de dinero y activos.

En cuanto a la comunicación que se lleva a cabo, entre los miembros de la alta gerencia y el resto del personal, no se cumplen con líneas de información definidas, ya que no cuentan con un programa que

permita transmitir a todos los involucrados de la gestión de riesgos, las medidas y controles implementados para esta actividad.

Tampoco, se han establecido planes de capacitación para que los funcionarios de la entidad, mantengan un conocimiento actual en materia de lavado de dinero, de las medidas que se pueden aplicar para mitigar esta problemática y cuál es el ámbito legal y normativo aplicable a las operaciones con dinero electrónico.

La empresa ha establecido algunas sanciones administrativas para el personal, dictadas por la Junta Directiva en coordinación con la oficialía de cumplimiento, en caso de faltas a las políticas existentes para la prevención y detección de lavado de dinero y de activos. No obstante, estas sanciones no se encuentran establecidas dentro de un manual de riesgos, que sea transmitido a todos los miembros de la organización, solo constan en volantes elaborados por el departamento de recursos humanos.

Otro aspecto a resaltar es la carga laboral asigna al oficial de cumplimiento, que es el encargado de toda la supervisión de gestión de riesgo de lavado de dinero y activos en la entidad, y de la elaboración de informes para los dueños y miembros de Junta Directiva. Sin embargo, carece de planes y programas de trabajo específicos para el desarrollo de estas funciones.

3.2.2. Determinación del contexto interno y externo.

- **Contexto interno.**

En cuanto al entorno interno de la empresa, se cuenta con las condiciones necesarias para el desarrollo de sus operaciones, con un avanzado recurso tecnológico que permite tener a la mano la información requerida y un servicio ágil para cumplir con la demanda de los clientes; es importante mencionar que los clientes de este tipo de negocios requieren que el servicio prestado por la empresa sea de alto nivel, tanto en la calidad de atención al cliente como en la seguridad de las operaciones que se realizan, para esto se ha definido un departamento de informática que tiene el soporte técnico de las operaciones que se realizan, el recurso humano está capacitado técnicamente para brindar los mejores resultados.

Sobre la función operativa de los servicios que se ofrecen, resalta la falta de controles sobre los clientes finales que reciben transferencias de dinero, el agente autorizado realiza debida diligencia solamente con el cliente inicial, y se deja un lado el conocimiento de quien es la persona que recibe el dinero y que lo hace efectivo. Este aspecto implica un riesgo latente para la empresa porque puede ser el origen del delito. De igual forma, no se aplican políticas adicionales de debida diligencia, cuando se trata de clientes clasificados como personas políticas expuestas.

Actualmente, la empresa no cuenta con un sistema de registro de las políticas y procedimientos destinados a la prevención de riesgos; ni se ha definido quien será el responsable de mantener y actualizar la información proveniente de reportes de operaciones sospechosas.

Entre los servicios ofrecidos se encuentran los siguientes:

- ✓ Pagos de facturas de servicios básicos.
- ✓ Transferencias de dinero.
- ✓ Recarga de saldo a teléfonos móviles.
- ✓ Pago de compras en supermercados.
- ✓ Pago de consumo en restaurantes.

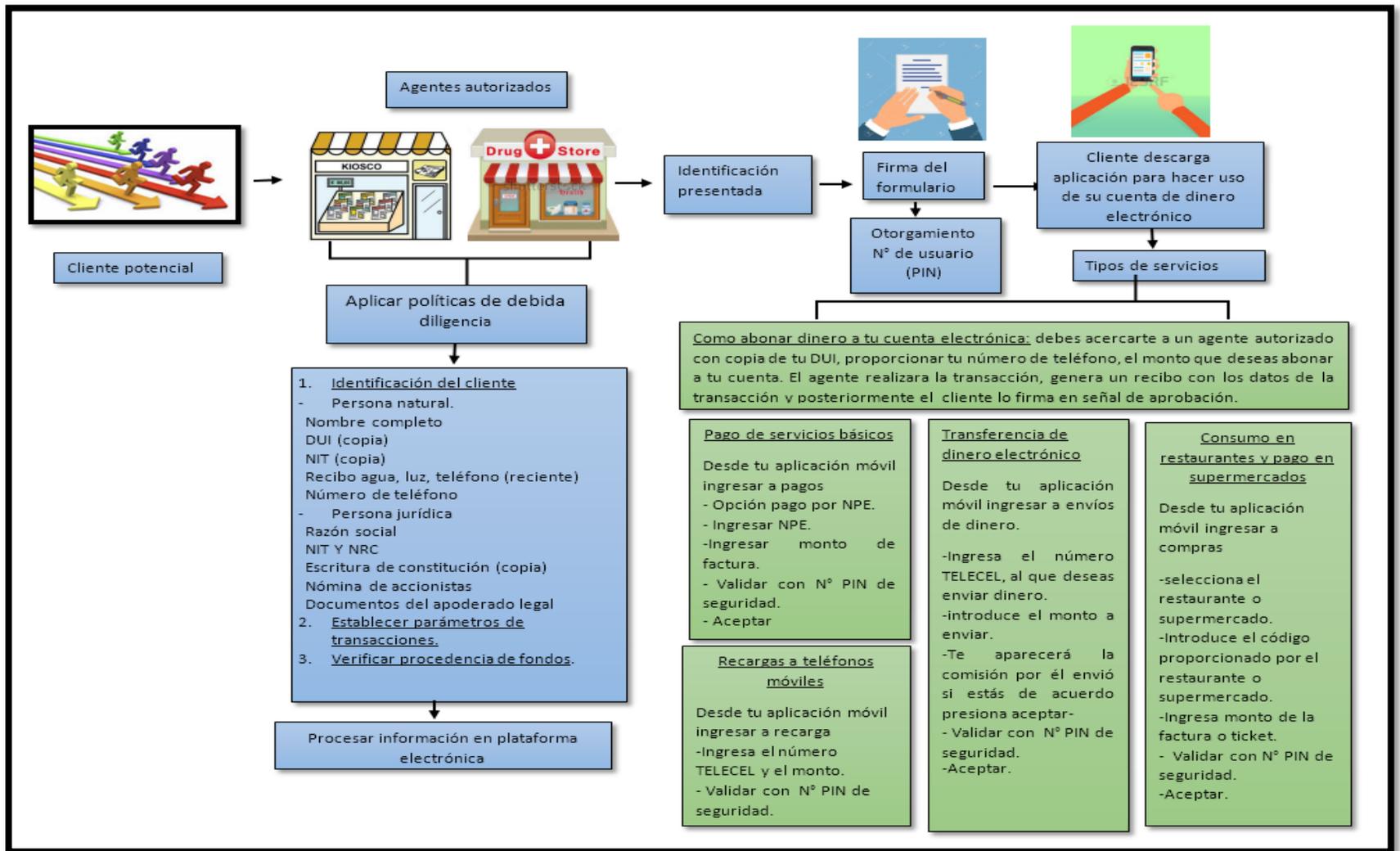


Figura 4: Esquema operativo, ElectroniCash, S.A. Fuente: Creación propia.

- **Contexto externo.**

En el entorno legal y normativo, se opera bajo la supervisión de la Superintendencia del Sistema Financiero y con las normas técnicas emitidas por el Banco Central de Reserva de El Salvador, leyes emitidas por el órgano legislativo y normas y convenios internacionales tales como:

- ✚ Ley para facilitar la inclusión financiera.
- ✚ Ley de supervisión y regulación del sistema financiero.
- ✚ Ley contra el lavado de dinero y activos y su Reglamento.
- ✚ Ley especial contra actos de terrorismo.
- ✚ Normas técnicas para el inicio de operaciones y funcionamiento de los proveedores de dinero electrónico.
- ✚ Normas técnicas para la gestión de los riesgos de lavado de dinero y de activos y financiamiento al terrorismo.
- ✚ Instructivo de la Unidad de Investigación Financiera para la prevención del lavado de dinero y de activos.
- ✚ Convenio Centroamericano para la prevención y la represión de los delitos de lavado de dinero y activos, relacionado con el tráfico ilícito de drogas y delitos conexos.
- ✚ Recomendaciones GAFI.
- ✚ ISO 31000-2009, gestión de riesgos.

En lo referente a la gestión de riesgos. Además, se encuentra a disposición de la Fiscalía General de la Republica, mediante la Unidad de Investigación Financiera, en lo que concierne a las investigaciones llevadas a cabo para los delitos relacionados con lavado de dinero, para que se pueda proporcionar cualquier información que se requiera durante el proceso investigativo.

3.2.3. Definición de la estructura organizativa.

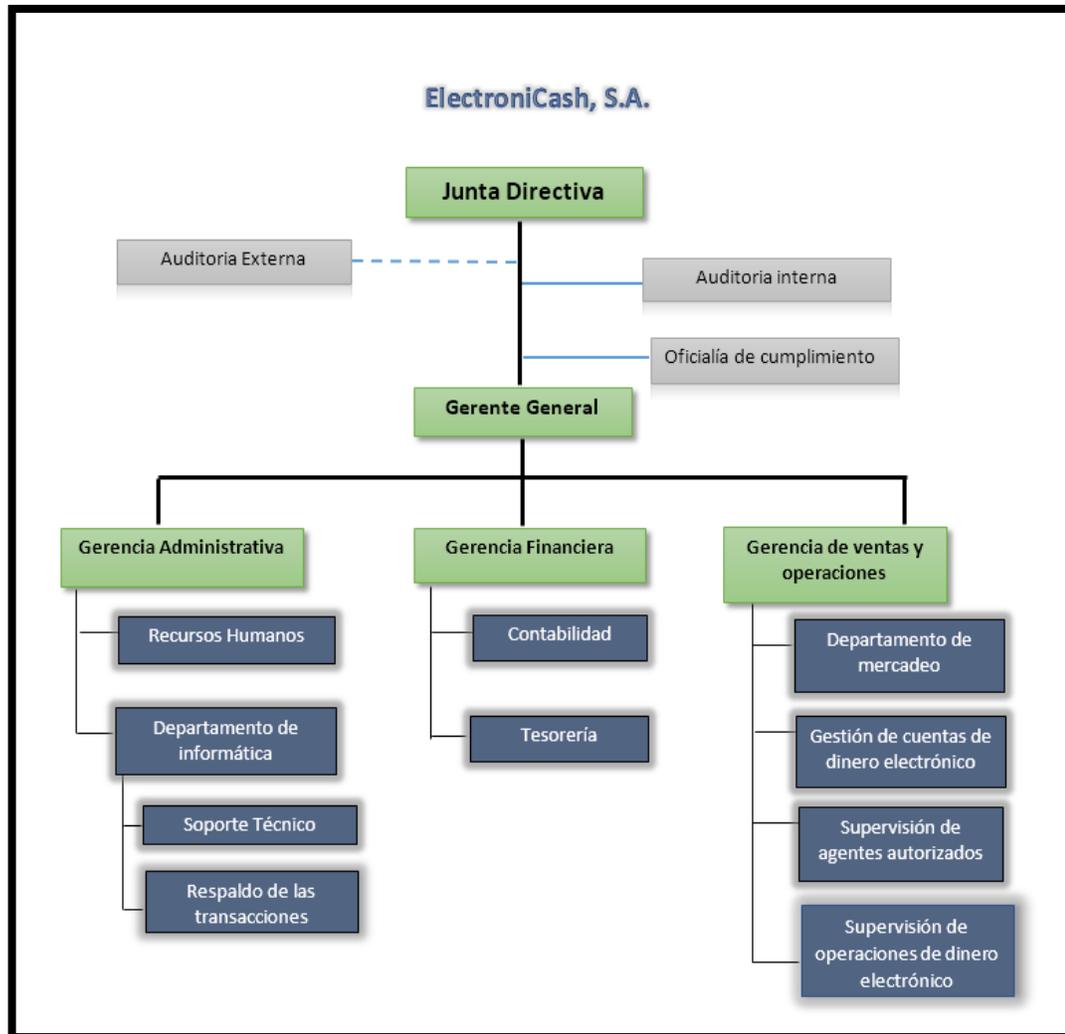


Figura 5: organigrama ElectroniCash, S.A. **Fuente:** Creación propia.

3.2.4. Determinar factores de riesgo.

Las contrapartes: se refiere a todas aquellas partes que tiene relación directa o indirectamente con la sociedad proveedora de dinero electrónico en relación a su giro principal, dentro de estas se encuentran las siguientes:

- Agentes autorizados.
- Oficial de cumplimiento.
- Los empleados.

- d) Cliente origen.
- e) Cliente destino.
- f) Las instituciones afiliadas a la entidad en las que se pueden realizar operaciones de dinero electrónico.

Los servicios: dentro de los servicios que ofrece la sociedad en mención se encuentra: transferencias electrónicas de un teléfono celular a otro, pago de servicios, recargas telefónicas y consumo en restaurantes. Algunas de estas operaciones con dinero electrónico son propensas a ser utilizadas de manera inadecuada por sus clientes.

Los canales de distribución: Es el medio que utiliza la empresa para la distribución de sus servicios. En el caso de ElectroniCash se cuenta con una plataforma virtual, en la cual los clientes por medio de un teléfono móvil pueden interactuar con su dinero electrónico.

Las áreas geográficas o jurisdicciones: ElectroniCash cuenta con agentes autorizados en todos los departamentos del país, de los cuales 290 se encuentran en el área metropolitana, 150 en la zona occidental, 200 en la zona oriental y 95 en la zona Paracentral de El Salvador, por lo que se puede decir que tiene cobertura a nivel nacional.

La empresa debe realizar un estudio de las zonas en las que pretende operar con el fin de establecer mecanismos específicos que minimicen la probabilidad de tener clientes que puedan incorporar dinero ilícito al sistema de dinero electrónico que la empresa tiene como servicio principal.

3.2.5. Diagnóstico general que refleje los factores de riesgo.

Luego de realizar un análisis completo de toda la información proporcionada, por las autoridades de la entidad, mediante la aplicación de técnicas como encuestas, entrevistas y con la observación directa sobre la situación actual de la entidad, se concluye que el trabajo en materia de prevención de riesgos de lavado de dinero, aplicado a la operatividad de los servicios prestados, presenta deficiencias por cada factor de riesgo como se describe en los siguientes apartados:

Con el factor de las contrapartes, quienes se relacionan directa o indirectamente con la sociedad, empezando por los agentes autorizados quienes realizan la debida diligencia, al momento no se encuentran debidamente capacitados para ejercer tan importante función, pues la empresa no tiene definido un proceso adecuado que deban seguir al momento de la creación de nuevas cuentas. Dentro de ElectroniCash existen supervisores que están a cargo de los agentes autorizados, los cuales no tienen

una adecuada comunicación con la gerencia, que les permita reportar cualquier anomalía, ya que no se cuenta con un protocolo de comunicación que permita, por una parte que la gerencia comunique las medidas a tomar en cuenta para mitigar los riesgos, y por otro lado, que los supervisores reporten cualquier incidente que se considere como una operación sospechosa.

Los clientes quienes juegan un papel muy importante en toda sociedad no son monitoreados constantemente, ya que no se realizan actualizaciones en sus datos, lo que mejoraría las alertas de operaciones sospechosas. Con los clientes finales, quienes reciben el dinero, no se cuenta con un límite regulado, lo que facilita la técnica del pitufeo en el delito de lavado de dinero y activos.

Por la naturaleza de la empresa, es necesario contar con excelente tecnología que sea capaz de darle cobertura a todo el país, la empresa cuenta con una plataforma virtual en buenas condiciones, sin embargo, se observó que no se realiza una auditoria de sistemas, que verifique que ningún intruso ha burlado la seguridad de la misma, al igual que no se realiza un back-up de las transacciones diarias, siendo esta información sensible y exigida su resguardo según las nuevas reformas de ley.

Para dar cobertura a todo el país, es necesario contar con agentes autorizados en todos los departamentos, pero debido a la situación social que enfrenta nuestro país, es necesario realizar un estudio de las zonas en las que se pretende operar, con el fin de establecer mecanismos específicos que minimicen la probabilidad de tener clientes que puedan incorporar dinero que no es lícito al sistema de dinero electrónico que la empresa tiene como servicio principal. Actualmente se cuenta con puntos de atención en zonas catalogadas como de alto riesgo los que representa una amenaza para la sociedad en cuestión.

3.3. Etapa 2: Identificación de eventos.

3.3.1. Identificar los eventos de riesgo por cada factor de riesgo.

Los riesgos identificados para cada factor de riesgo definido en la etapa uno del diagnóstico, se detallan de la siguiente manera:

TABLA N° 5: Identificación de riesgos, causas y consecuencias.

FACTOR DE RIESGO	EVENTO O RIESGO	CAUSA	CONSECUENCIAS
Las Contrapartes			
Agentes Autorizados	Vínculos con grupos delictivos, lo que permite el otorgamiento de cuentas a clientes de dudosa reputación y la realización de transacciones con fondos provenientes de actividades ilícitas.	El agente autorizado puede estar siendo objeto de extorsiones y amenazas por parte de estructuras criminales para que sirva como un medio en la colocación de dinero ilícito al sistema financiero del país.	Pérdidas económicas para la entidad, debido a fraude y atentados cometidos por los agentes autorizados.
Agentes Autorizados	Comunicación inadecuada entre el agente autorizado y el personal encargado de la gestión de riesgos de la entidad, al momento de informar sobre la aprobación de cuentas a clientes de dudosa reputación y sobre cualquier operación sospechosa realizada.	No se cuenta con las líneas o canales de información adecuados entre los diferentes agentes autorizados y los miembros de la entidad, para transmitir la información necesaria en el tiempo requerido.	Pérdida de información importante, falsificación de información y documentación atrasada.
Agentes Autorizados	Deficiencia en la prestación de servicios ofrecidos por la entidad, lo que conlleva	El agente no cuenta con la formación adecuada para el cargo. No cumple con	Servicios deficientes prestados al cliente, sanciones por el incumplimiento a las

FACTOR DE RIESGO	EVENTO O RIESGO	CAUSA	CONSECUENCIAS
	a una mala o nula aplicación de políticas de debida diligencia, que permitan detectar cualquier caso sospechoso de lavado de dinero por parte de los clientes.	<p>los requerimientos mínimos para saber qué acciones tomar en caso que no existan políticas de gestión de riesgos claras.</p> <p>Falta de liderazgo por parte de los miembros de la entidad para con los agentes, de manera que se pueda ofrecer un servicio eficiente.</p>	normas que establecen la correcta aplicación de debida diligencia y daño a la imagen de la entidad por la deficiencia en los procesos realizados.
Agentes Autorizados	Políticas y procedimientos de debida diligencia inadecuados al momento de la aprobación de cuentas y de la realización de operaciones mediante los servicios ofrecidos	El agente no es capaz de aplicar la debida diligencia debido a la debilidad de las políticas establecidas por los encargados de la gestión de riesgos en la entidad.	Sanciones por el incumplimiento en la aplicación de la normativa legal relacionada con la debida diligencia y pérdida de recursos destinados en la capacitación del personal.
Oficial de Cumplimiento	Mala distribución de las labores encomendadas al Oficial de Cumplimiento, este realiza labores fuera del área de la gestión de riesgos, lo que desvía la atención a los casos de lavado de dinero presentados, los cuales deben solucionarse en el menor tiempo posible.	No existen planes de trabajo definidos para cada puesto de la entidad, las labores deben ser enfocadas a cada área y estar redactadas en forma sencilla para una mejor comprensión por parte del empleado.	<p>Desigualdad laboral, personal desmotivado, ineficiencia en el cumplimiento de los objetivos y metas relacionados con el desarrollo de las funciones y actividades comerciales de la entidad.</p> <p>Pérdida de recursos destinados a la</p>

FACTOR DE RIESGO	EVENTO O RIESGO	CAUSA	CONSECUENCIAS
			capacitación del personal.
Oficial de Cumplimiento	El oficial de Cumplimiento no cuenta con las habilidades necesarias para el puesto, en cuanto a la gestión de riesgos y la operatividad del dinero electrónico y los casos de lavado de capitales que se pueden presentar mediante este sistema.	El Oficial ha sido contratado por vínculos de afinidad de algún miembro de la entidad, anteponiendo el interés personal a los requerimientos mínimos para el puesto. No se cuenta con un plan de capacitación para el personal en materia de lavado de dinero y en el modo de operación del dinero electrónico.	Pérdida de recursos económicos utilizados en capacitación al personal en materia de lavado de dinero. Pérdidas económicas derivadas de fraudes o atentados por parte de los empleados de la entidad. Personal ineficiente, lo que se traduce a una mala prestación de los servicios ofrecidos.
Los Empleados (supervisores)	Encubrimiento de casos sospechosos entre los supervisores y los agentes autorizados, de manera que no se gire una alerta que indique que el cliente está haciendo mal uso de los servicios ofrecidos por la entidad, evitando además el inicio de las investigaciones necesarias para determinar cualquier culpabilidad de delito de lavado de dinero.	Tanto el Supervisor de zona como el Agente autorizado pueden estar siendo objeto de amenazas o extorsiones por parte de delincuentes, para que exista una alianza que beneficie la fácil colación de dinero ilícito al sistema.	Pérdidas económicas derivadas de robo y fraude por parte de los empleados de la entidad, provenientes de operaciones ilícitas con ocultamiento del empleado.

FACTOR DE RIESGO	EVENTO O RIESGO	CAUSA	CONSECUENCIAS
Los empleados (Supervisores)	Los casos de operaciones sospechosas no son reportados de forma oportuna al oficial de cumplimiento, para que se investigue el origen de la operación realizada por el cliente, o en su caso realizar el reporte que será evaluado por los miembros de la alta gerencia, para tomar la decisión si el caso procede hacer investigado por la UIF.	El supervisor no cuenta con los canales de información necesarios o simplemente no cuenta con las habilidades para su cargo, que permita la acción oportuna para los casos de operaciones sospechosas que han sido girados como alertas por parte de los agentes autorizados.	Información fraudulenta en los reportes de operaciones sospechosas, lo que no brinda una fuente confiable para realizar las investigaciones correspondientes.
Cliente Origen	Proporcionar información falsa al momento de abrir una cuenta, de manera que no se pueda detectar vínculos con estructuras delictivas.	La documentación presentada por el cliente es fraudulenta, intentando engañar al agente autorizado, para que este le otorgue una cuenta.	Registros de clientes con información fraudulenta. Posibles pérdidas económicas y daños en la imagen comercial de la entidad.
Agente Autorizado	No se aplican políticas de debida diligencia ampliada para los clientes considerados como personas políticamente expuestas.	No se cuenta con políticas de debida diligencia ampliada para clientes considerados como PEP's. El agente no practica la debida diligencia ampliada como lo establece la normativa y regulaciones legales aplicadas a la entidad.	Sanciones legales por incumplimiento a las disposiciones legales referentes a la aplicación de una debida diligencia ampliada para personas políticamente expuestas. Pérdida económica por el uso indebido de los servicios prestados.

FACTOR DE RIESGO	EVENTO O RIESGO	CAUSA	CONSECUENCIAS
<p>Cliente Destino</p>	<p>Ausencia de un límite en la cantidad de dinero recibida por el cliente destino, que cumpla con las disposiciones fijadas por la normativa legal aplicable actualmente al cliente de origen, dichos límites deben ser cumplidos, tanto por el cliente que recibe, como el que coloca los fondos dentro de la plataforma electrónica.</p>	<p>Las políticas establecidas por la entidad para la prestación de los diferentes servicios con dinero electrónico, fijan límites de dinero solamente para el cliente de origen, no así para la persona que recibe los fondos, permitiendo claramente que fuertes cantidades de dinero sean enviadas a un mismo cliente destino, facilitando los casos de financiamiento al terrorismo.</p>	<p>Sanciones legales por incumplimiento a la normativa legal. Implicaciones en actos de financiamiento al terrorismo. Pérdidas económicas por robo o atentados de grupos delictivos.</p>
<p>Los empleados</p>	<p>Las actividades realizadas por el personal de la entidad, no sean llevadas a cabo de conformidad con las leyes, normas y estándares éticos.</p>	<p>No se cuenta con un Código de Conducta que defina claramente, los diferentes valores y normas éticas que se deben cumplir en el desempeño de labores de trabajo. Falta de liderazgo por parte de los miembros de alta gerencia de la entidad, que transmita valores éticos a sus subalternos.</p>	<p>Personal ineficiente, conflictos internos de trabajo. Incumplimiento de los objetivos y metas trazados por la entidad.</p>

FACTOR DE RIESGO	EVENTO O RIESGO	CAUSA	CONSECUENCIAS
Servicios			
	Fraude interno y externo, los servicios son utilizados para mover cantidades de dinero ilícito de un lugar a otro dentro del país sin ser detectados por las autoridades.	Falta de controles para detectar oportunamente factores de riesgos en el entorno interno y externo del sistema, que pueda alterar la información contenida en cada operación.	Pérdidas económicas para la entidad, daños en la imagen comercial por el involucramiento inconsciente en actividades ilícitas.
	Fallas en los procesos al momento de efectuar las transacciones, lo que puede ocasionar alteración en los datos de las operaciones realizadas por los clientes, pasando por alto cualquier actividad ilícita.	Falta de políticas y planes de contingencia para el desarrollo de procesos en la prestación de los servicios ofrecidos.	Sanciones por incumplimiento de las normas legales establecidas, además de las pérdidas en recursos por las operaciones realizadas erróneamente.
	Diseños inapropiados para la prestación de servicios.	Carencia de un proceso lógico para la prestación de los servicios, lo que ocasiona alteración de la información proporcionada por el cliente, llevando a un caso de operación ilícita sin ser detectada por el agente autorizado. Inexistencia de un manual de servicio al cliente.	Deterioro de la imagen comercial de la entidad y alteración de la información contenida en los registros de operaciones de los clientes.

FACTOR DE RIESGO	EVENTO O RIESGO	CAUSA	CONSECUENCIAS
	Manipulación inadecuada de los registros de las operaciones efectuadas por cada cliente.	Manipulación y alteración de la información contenida en los expedientes a favor de algún cliente, afectando de manera favorable o desfavorable su historial de operaciones.	Información errónea de expedientes para cada cliente, obstaculizando el trabajo de investigación para casos de operaciones sospechosas.
Canales de Distribución			
	Fallas en el procesamiento de la información de las operaciones efectuadas por los clientes.	Problemas en la plataforma electrónica que impiden el registro de las transacciones en los tiempo requeridos.	Información fraudulenta. Daños al equipo tecnológico de la entidad.
	Manipulación de los servidores por personas externas a la entidad, que ocasionen alteración a los registros de las operaciones.	Que el equipo informático no cuente con las medidas de seguridad apropiadas para combatir ataques cibernéticos.	Alteración de la información contenida en los registros efectuados por la entidad. Daños a la infraestructura que contiene los respaldos necesarios, por cada operación realizada.
	Los límites de dinero establecidos por la ley para las transacciones realizadas con dinero electrónico, no sean verificados por los empleados al momento de que el cliente realice una operación, ya sea esto por negligencia o dolo.	Falta de controles que eviten que los empleados hagan mal uso del sistema, favoreciendo operaciones de clientes que realicen transacciones fuera de los límites establecidos.	Pérdidas financieras por robo y fraude de los empleados. Sanciones legales.

FACTOR DE RIESGO	EVENTO O RIESGO	CAUSA	CONSECUENCIAS
	Falta de copias de seguridad de la información de los clientes y de las transacciones realizadas por estos.	Falta de políticas de aseguramiento de la información, que exijan resguardar diariamente las transacciones, mediante los medios adecuados y en el espacio físico idóneo, al cual tenga acceso solo el personal autorizado.	Alteración de la información contenida en los resguardos, preparados por la entidad. Sanciones por incumplimiento a las disposiciones legales.
	Existencia de clientes que posean más de una cuenta, mediante el mecanismo de prestanombres.	Inexistencia de alertas en el sistema de la sociedad que impidan la creación de más de una cuenta. Los agentes autorizados no aplican la debida diligencia para asegurarse que los documentos presentados pertenecen a una sola persona, quien será el titular y que no realizara ninguna operación a cuenta de terceros.	Pérdidas económicas, sanciones legales y daño a la imagen comercial de la entidad. Información fraudulenta contenida en el registro de los clientes y sus operaciones.
Áreas Geográficas			
	Ubicación de agentes autorizados en zonas geográficas catalogadas como de alto índice delincriminal.	No realizar estudios de zona de riesgo donde se encuentran ubicados los agentes autorizados.	Extorsiones constantes a los agentes autorizados, amenazas a la integridad física de los empleados y pérdidas financieras para la entidad.

FACTOR DE RIESGO	EVENTO O RIESGO	CAUSA	CONSECUENCIAS
	Entorno de trabajo inadecuado, que no cumpla con los requerimientos mínimos de seguridad para que los empleados puedan cumplir con sus respectivas funciones.	Las condiciones laborales para los empleados no cumplen con los requerimientos legales establecidos para garantizar la estabilidad del personal.	Trabajos deficientes, los objetivos de la entidad se ven amenazados, debido a que el personal no se encuentra motivado a trabajar en equipo.
	Transacciones recurrentes desde zonas consideradas de alto riesgo, por la presencia de estructuras criminales.	Falta de sistemas de alertas que permitan detectar operaciones recurrentes desde una misma zona geográfica.	Daño en la imagen comercial de la entidad, al verse involucrada en actos delictivos, por consiguiente sanciones legales, que pueden llevar al cierre total del negocio.
	Pérdida de información debido a desastres naturales.	Los equipos informáticos, documentación y resguardos de la información registrada, no se encuentran en el espacio físico que impida que cualquier evento natural pueda acabar con dichos registros.	Pérdidas financieras por el daño a la infraestructura y documentación resguardada.

3.4. Etapa 3: Medición o evaluación de los riesgos.

3.4.1. Determinación de los criterios de medición de los riesgos.

Una vez, identificados los riesgos por cada factor, se procede al análisis de estos, para establecer la probabilidad de ocurrencia de los mismos y sus consecuencias en la operación del negocio; este último aspecto orienta la clasificación del riesgo, con el objetivo de obtener información para establecer el nivel de riesgo y las acciones que se deberán implementar para aquellos considerados como no tolerables para la entidad.

Para el análisis llevado a cabo, se siguió los siguientes pasos claves:

1. Determinar probabilidad
2. Determinar impacto
3. Clasificación del riesgo
4. Estimar el nivel del riesgo
5. Análisis de efectividad de los controles

Se establecieron dos aspectos a tener en cuenta en el análisis de los riesgos identificados los cuales son: **probabilidad e impacto.**

La probabilidad, en este caso se entiende como la periodicidad de ocurrencia de un riesgo identificado; esta periodicidad que existe, fue medida con criterios de frecuencia, para aquellos eventos ya materializados y de factibilidad, para aquellos que aún no se hayan materializado, teniendo en cuenta la presencia de factores internos y externos los cuales proporcionan el riesgo.

Para el impacto se tomó como base, las derivaciones que ocasionan a la organización una consecuencia negativa, una vez se ha materializado el riesgo. Estas derivaciones a su vez modifican el grado de alcance de los objetivos establecidos para la mitigación de los eventos.

- **Identificación y clasificación del nivel de riesgo.**

Para establecer el nivel de riesgo fue necesario tipificar, de acuerdo a la escala, el tipo de probabilidad de ocurrencia para que el evento ocurra, al igual que el nivel de impacto que el riesgo pueda tener sobre el plan de trabajo que la empresa ha establecido. Dicha valoración es inicial y se realizó sin considerar los controles que ya existen en la empresa y las acciones que se hayan implementado para su monitoreo, los

cuales comprenden una serie de materiales que se han elaborado para medir los avances y regresiones de los objetivos de la organización.

Las escalas consideran una puntuación que van del uno al cinco, en donde el cinco es el número de puntuación mayor, esto quiere decir que esta calificación indica un nivel de ocurrencia y un impacto mayor.

- **Medición de la probabilidad de riesgo.**

La medición se evaluó en función de la frecuencia en la que un evento de riesgo ocurre, por cada factor determinado y su calificación depende de la incidencia que estos tienen.

La evaluación esta desde el nivel uno al cinco y se clasifica en un nivel por cada uno de ponderación como a continuación se muestra:

- a) **Muy baja:** está incluida en la ponderación 1. Representa una probabilidad muy baja de ocurrencia que pueda suceder un evento.
- b) **Baja:** está incluida en la ponderación 2. Representa una probabilidad media en la aparición de un evento identificado.
- c) **Media:** está incluida en la ponderación 3. Representa una probabilidad media en la aparición de un evento, lo que significa que se considera que la posibilidad que existe es del 50%, las decisiones que están relacionadas a este nivel de riesgo están consensuadas, para que se eviten daños de importancia bajo la visión de que existe la misma oportunidad de ocurrencia de que el evento de riesgo ocurra o de que no.
- d) **Alta:** está integrado en el nivel 4. Representa una probabilidad alta de ocurrencia de un evento, en esta categoría se toma la decisión de tener un enfoque dirigido a la prevención y estrategias de estabilización de la situación ante una crisis, la posición que deben tener la toma de decisiones es de que el evento va a ocurrir y el que no ocurra es un escenario más improbable.
- e) **Muy alta:** incluye el parámetro 5 de ponderación. En este nivel se toman las decisiones de que la entidad está colocada firmemente en la restauración del daño y altos niveles de control que eviten la presencia del evento de riesgo.

- **Medición del impacto de riesgo.**

Esta medición se llevó a cabo, según una evaluación en función del grado de magnitud de los efectos identificados y registrados sobre las medidas o programas que la empresa tiene para la prevención de riesgos de lavado de dinero.

Las consecuencias que el impacto tiene sobre los riesgos que han sido identificados, son a corto, mediano, y largo plazo, y se derivan del incumplimiento de las metas que la empresa se ha proyectado. Por lo tanto la medición del impacto, ha servido como un factor esencial para la toma de decisiones, con respecto a las acciones a tomar en torno al riesgo, ya sea para su aceptación, compartirlos o mitigación.

Las categorías asignadas al impacto son:

- a) Muy bajo:** está incluido en la ponderación 1. Representa aquellos riesgos que pueden tener un pequeño o nulo efecto en la entidad.
- b) Bajo:** está incluido en la ponderación 2. Representa aquellos daños en el patrimonio o imagen de la entidad, y que se pueden corregir en el corto plazo, y que no afectan el cumplimiento de los objetivos estratégicos de la organización.
- c) Medio:** está incluido en la ponderación 3. Representa aquellos riesgos que causarían, ya sea una pérdida importante en el patrimonio de la sociedad, incumplimientos normativos, problemas operativos o un deterioro significativo de la imagen. Además, se necesita una cantidad importante de tiempo de la alta gerencia en investigar y corregir estos daños.
- d) Alto:** su ponderación es 4. Representa un daño significativo en el patrimonio, incumplimientos del marco normativo, problemas en el curso normal de las operaciones, deterioro de la imagen y cumplimiento de los objetivos de la organización. Se necesita de medidas y tiempo adicional por parte de la alta gerencia, en mitigar estos daños.
- e) Muy Alto:** se pondera con un valor de 5. Representa un daño directamente en el cumplimiento de la misión de la entidad, así como pérdida patrimonial, incumplimiento a la normativa establecida, fallas en la operación, deterioro de imagen comercial, con la posibilidad de dejar sin funcionar totalmente o por un periodo importante de tiempo los servicios que presta la empresa.

Tabla N° 6: Niveles de medición para determinar la probabilidad e impacto de los riesgos.

Probabilidad		Impacto		Parámetros	Nivel de Riesgo
Categoría	Ponderación	Categoría	Ponderación		
Muy Alta	5	Muy Alto	5	15-25	Muy grave
Alta	4	Alto	4	9-14	Importante
Media	3	Medio	3	5-8	Apreciable
Baja	2	Bajo	2	3-4	Marginal
Muy Baja	1	Muy Bajo	1	1-2	Insignificante

La correcta evaluación de los riesgos permitió comparar los resultados que se le asignaron a la calificación del riesgo, con los criterios definidos para establecer el grado de exposición de la entidad; de esta manera se hizo la distinción entre riesgos que se deben aceptar, evitar, compartir o transferir, y así fijar las prioridades de las acciones que se requieren para su tratamiento.

La elaboración de matrices se compone de dos partes, la primera es la obtención de los niveles de riesgos, en donde se debe realizar la operación matemática entre las ponderaciones de probabilidad e impacto. Al efectuar el producto de ambas variables, se obtiene los parámetros que permiten determinar el nivel de riesgo por cada evento, agrupados en cinco niveles con diferente color, lo que permite una mejor apreciación de los resultados.

Tabla N° 7: Obtención de los niveles de clasificación de riesgos.

MATRIZ DE RIESGOS				
FACTOR DE RIESGO:				
RIESGO	PROBABILIDAD	IMPACTO	VALOR DEL RIESGO	NIVEL DE RIESGO
Riesgo 1	Nivel de probabilidad traducido a ponderación de 1-5.	Nivel de impacto traducido a ponderación de 1-5.	Resultado obtenido al efectuar la multiplicación de las ponderaciones de los niveles de Probabilidad e Impacto.	Clasificación del riesgo en nivel insignificante, marginal, apreciable, importante y muy grave. Identificación de riesgos NO tolerables para la entidad.

La segunda parte se compone de un diagrama de calor, en el eje vertical se encuentran los niveles de probabilidad y en el eje horizontal los niveles de impacto. Según esta gráfica, separada por cinco colores principales, aquellos riesgos que se encuentran en color blanco y verde, son los que la entidad puede asumir y mitigar solo con la correcta aplicación de las medidas de prevención ya existentes. Por el contrario, los riesgos situados en las zonas de color amarillo, naranja y rojo, son los que requieren de principal atención, ya que son riesgos no tolerables para la entidad, y necesitan de la implementación de controles inmediatos para prevenir su probabilidad de ocurrencia; si estos eventos no son tratados con la debida atención que merecen, los impactos que puede sufrir el negocio son muy graves.

Tabla N° 8: Mapa de calor para los diferentes niveles de riesgos.

			FACTOR DE RIESGO:				
			IMPACTO				
			Muy Bajo	Bajo	Medio	Alto	Muy Alto
			1	2	3	4	5
PROBABILIDAD	Muy Alta	5	5	10	15	20	25
	Alta	4	4	8	12	16	20
	Media	3	3	6	9	12	15
	Baja	2	2	4	6	8	10
	Muy Baja	1	1	2	3	4	5

	Riesgo muy grave. Requiere medidas preventivas urgentes. No se debe seguir con la operación sin la aplicación de medidas preventivas urgentes y sin acotar sólidamente el riesgo. Reducir, Compartir o transferir el riesgo.
	Riesgo importante. Medidas preventivas obligatorias. Se deben controlar fuertemente las variables de riesgo durante la operación. Reducir o Compartir el riesgo.
	Riesgo apreciable. Realizar un análisis de costo-beneficio si es posible introducir medidas preventivas para reducir el nivel de riesgo. Si no fuera posible, mantener las variables controladas. Evitar o Reducir el riesgo.
	Riesgo marginal. Se vigilará aunque no requiere medidas preventivas de partida. Aceptar o Evitar el riesgo.
	Riesgo insignificante. Se vigilará aunque no requiere medidas preventivas de partida, pero si se analizara su frecuencia de ocurrencia. Aceptar el riesgo.

A continuación se presenta en resumen de la clasificación de riesgos, identificando cuales son los riesgos que pueden ser tolerables para la entidad.

Tabla N° 9: Clasificación de riesgos.

ZONA DE RIESGO	NIVEL DE RIESGO	RESPUESTA AL RIESGO	CLASIFICACIÓN
Muy Alto	Riesgo Muy Grave	Reducir/Compartir/Transferir	NO TOLERABLES
Alto	Riesgo Importante	Reducir/Compartir	
Medio	Riesgo Apreciable	Evitar/Reducir	
Bajo	Riesgo Marginal	Aceptar/Evitar	TOLERABLES
Muy Bajo	Riesgo Insignificante	Aceptar	

- **Análisis de efectividad de los controles.**

Una vez que los riesgos han sido valorizados se procede a evaluar la calidad de la gestión, a fin de determinar cuán eficaces son los controles establecidos por la empresa para mitigar los riesgos identificados. En la medida que los controles sean más eficientes y la gestión de riesgos pro-activa, el indicador de riesgo inherente neto tiende a disminuir. La escala de valoración de efectividad de los controles se ajusta al rango siguiente:

Tabla N° 10: Escalas de valoración de la efectividad de los controles.

CONTROL	EFFECTIVIDAD
Ninguno	1
Bajo	2
Medio	3
Alto	4
Destacado	5

Luego se calcula el riesgo neto o residual, que resulta de la relación entre el grado de manifestación de los riesgos inherentes y la gestión de mitigación de riesgos establecida por la entidad, la operación matemática a realizar es la división del valor del riesgo entre el grado de efectividad de los controles establecidos. En el siguiente cuadro se muestra el riesgo neto o residual utilizando escalas numéricas de posición de riesgo para cada evento identificado:

Tabla Nº 11: Obtención de Riesgo Residual.

Nº	FACTOR DE RIESGO	EVENTO O RIESGO	PROBABILIDAD	IMPACTO	VALOR DEL RIESGO	NIVEL DEL RIESGO	EFFECTIVIDAD	RIESGO RESIDUAL
Las Contrapartes								
R1	Agentes Autorizados	Vínculos con grupos delictivos, lo que permite el otorgamiento de cuentas a clientes de dudosa reputación y la realización de transacciones con fondos provenientes de actividades ilícitas.	4	5	20	Muy Grave	5	4.0
R2	Agentes Autorizados	Comunicación inadecuada entre el agente autorizado y el personal encargado de la gestión de riesgos de la entidad, al momento de informar sobre la aprobación de cuentas a clientes de dudosa reputación y sobre cualquier operación	3	4	12	Importante	3	4.0

N°	FACTOR DE RIESGO	EVENTO O RIESGO	PROBABILIDAD	IMPACTO	VALOR DEL RIESGO	NIVEL DEL RIESGO	EFFECTIVIDAD	RIESGO RESIDUAL
		sospechosa realizada.						
R3	Agentes Autorizados	Deficiencia en la prestación de servicios ofrecidos por la entidad, lo que conlleva a una mala o nula aplicación de políticas de debida diligencia, que permitan detectar cualquier caso sospechoso de lavado de dinero por parte de los clientes.	2	4	8	Apreciable	4	2.0
R4	Agentes Autorizados	Políticas y procedimientos de debida diligencia inadecuados al momento de la aprobación de cuentas y de la realización de operaciones mediante los servicios ofrecidos	3	5	15	Muy Grave	4	3.75
R5	Oficial de Cumplimiento	Mala distribución de las labores encomendadas al	4	5	20	Muy Grave	4	5.0

N°	FACTOR DE RIESGO	EVENTO O RIESGO	PROBABILIDAD	IMPACTO	VALOR DEL RIESGO	NIVEL DEL RIESGO	EFFECTIVIDAD	RIESGO RESIDUAL
		Oficial de Cumplimiento, este realiza labores fuera del área de la gestión de riesgos, lo que desvía la atención a los casos de lavado de dinero presentados, los cuales deben solucionarse en el menor tiempo posible.						
R6	Oficial de Cumplimiento	El oficial de Cumplimiento no cuenta con las habilidades necesarias para el puesto, en cuanto a la gestión de riesgos y la operatividad del dinero electrónico y los casos de lavado de capitales que se pueden presentar mediante este sistema.	2	5	10	Importante	3	3.33
R7	Los Empleados	Encubrimiento de casos	4	5	20	Muy Grave	5	4.0

N°	FACTOR DE RIESGO	EVENTO O RIESGO	PROBABILIDAD	IMPACTO	VALOR DEL RIESGO	NIVEL DEL RIESGO	EFFECTIVIDAD	RIESGO RESIDUAL
	(supervisores)	sospechosos entre los supervisores y los agentes autorizados, de manera que no se gire una alerta que indique que el cliente está haciendo mal uso de los servicios ofrecidos por la entidad, evitando además el inicio de las investigaciones necesarias para determinar cualquier culpabilidad de delito de lavado de dinero.						
R8	Los empleados (Supervisores)	Los casos de operaciones sospechosas no son reportados de forma oportuna al oficial de cumplimiento, para que se investigue el origen de la operación realizada por el cliente, o en su caso realizar	4	5	20	Muy Grave	4	5.0

N°	FACTOR DE RIESGO	EVENTO O RIESGO	PROBABILIDAD	IMPACTO	VALOR DEL RIESGO	NIVEL DEL RIESGO	EFFECTIVIDAD	RIESGO RESIDUAL
		el reporte que será evaluado por los miembros de la alta gerencia, para tomar la decisión si el caso procede hacer investigado por la UIF.						
R9	Cliente Origen	Proporcionar información falsa al momento de abrir una cuenta, de manera que no se pueda detectar vínculos con estructuras delictivas.	4	5	20	Muy Grave	5	4.0
R10	Agente Autorizado	No se aplican políticas de debida diligencia ampliada para los clientes considerados como personas políticamente expuestas.	2	4	8	Apreciable	4	2.0
R11	Cliente Destino	Ausencia de un límite en la cantidad de dinero recibida por el cliente destino, que	5	5	25	Muy Grave	5	5.0

N°	FACTOR DE RIESGO	EVENTO O RIESGO	PROBABILIDAD	IMPACTO	VALOR DEL RIESGO	NIVEL DEL RIESGO	EFFECTIVIDAD	RIESGO RESIDUAL
		cumpla con las disposiciones fijadas por la normativa legal aplicable actualmente al cliente de origen, dichos limites deben ser cumplidos, tanto por el cliente que recibe, como el que coloca los fondos dentro de la plataforma electrónica.						
R12	Los empleados	Las actividades realizadas por el personal de la entidad, no sean llevadas a cabo de conformidad con las leyes, normas y estándares éticos.	2	3	6	Apreciable	2	3.0
Servicios								
R13		Fraude interno y externo, los servicios son utilizados para mover cantidades de dinero ilícito de un lugar a otro del	4	5	20	Muy Grave	4	5.0

N°	FACTOR DE RIESGO	EVENTO O RIESGO	PROBABILIDAD	IMPACTO	VALOR DEL RIESGO	NIVEL DEL RIESGO	EFFECTIVIDAD	RIESGO RESIDUAL
		país sin ser detectados por las autoridades.						
R14		Fallas en los procesos al momento de efectuar las transacciones, lo que puede ocasionar alteración en los datos de las operaciones realizadas por los clientes, pasando por alto cualquier actividad ilícita.	2	5	10	Importante	4	2.5
R15		Diseños inapropiados para la prestación de servicios.	2	3	6	Apreciable	3	2.0
R16		Manipulación inadecuada de los registros de las operaciones efectuadas por cada cliente.	2	4	8	Apreciable	4	2.0
Canales de Distribución								
R17		Fallas en el procesamiento de la información de las	2	5	10	Importante	4	2.5

N°	FACTOR DE RIESGO	EVENTO O RIESGO	PROBABILIDAD	IMPACTO	VALOR DEL RIESGO	NIVEL DEL RIESGO	EFFECTIVIDAD	RIESGO RESIDUAL
		operaciones efectuadas por los clientes.						
R18		Manipulación de los servidores por personas externas a la entidad, que ocasionen alteración a los registros de las operaciones.	3	5	15	Muy Grave	5	3.0
R19		Los límites de dinero establecidos por la ley para las transacciones realizadas con dinero electrónico, no sean verificados por los empleados al momento de que el cliente realice una operación, ya sea esto por negligencia o dolo.	2	5	10	Importante	4	2.5
R20		Falta de copias de seguridad de la información de los clientes y de las transacciones realizadas por	2	5	10	Importante	5	2.0

N°	FACTOR DE RIESGO	EVENTO O RIESGO	PROBABILIDAD	IMPACTO	VALOR DEL RIESGO	NIVEL DEL RIESGO	EFFECTIVIDAD	RIESGO RESIDUAL
		estos.						
R21		Existencia de clientes que posean más de una cuenta, mediante el mecanismo de prestanombres.	3	3	9	Importante	4	2.25
Áreas Geográficas o Jurisdicciones								
R22		Ubicación de agentes autorizados en zonas geográficas catalogadas como de alto índice delincencial.	4	5	20	Muy Grave	4	5.0
R23		Entorno de trabajo inadecuado, que no cumpla con los requerimientos mínimos de seguridad para que los empleados puedan cumplir con sus respectivas funciones.	3	3	9	Importante	3	3.0
R24		Transacciones recurrentes	4	4	16	Muy Grave	3	5.33

N°	FACTOR DE RIESGO	EVENTO O RIESGO	PROBABILIDAD	IMPACTO	VALOR DEL RIESGO	NIVEL DEL RIESGO	EFFECTIVIDAD	RIESGO RESIDUAL
		desde zonas consideradas de alto riesgo, por la presencia de estructuras criminales.						
R25		Pérdida de información debido a desastres naturales.	2	5	10	Importante	2	5.0

3.5. Etapa 4. Adopción de controles.

3.5.1. Definir controles para mitigar cada uno de los riesgos identificados.

Una vez que ElectroniCash ha identificado los riesgos por cada factor, se deben tomar las medidas necesarias para controlar dichos riesgos, para ello se requiere que la entidad evalúe los controles ya existentes y analice la efectividad de los nuevos controles que se implantarán. Si los controles existentes muestran un comportamiento eficiente contra los riesgos, la entidad los fortalecerá y en caso que no existieren, inmediatamente se tomaran las medidas necesarias, de manera que se evite en primer lugar la probabilidad de ocurrencia de cada evento de riesgo.

En cuanto al tratamiento del riesgo, la entidad puede optar por aceptar, evitar, reducir, compartir o transferir el riesgo, este tratamiento se resume en la siguiente tabla:

Tabla N° 12: Respuesta al riesgo.

NIVEL DEL RIESGO	VALOR	RESPUESTA AL RIESGO	DESCRIPCIÓN
Insignificante	1	Aceptar	Cuando se cuenta con riesgos insignificantes y poco habituales la entidad los aceptara.
	2		
Marginal	3	Aceptar/Evitar	Si los riesgos marginales son aislados se aceptara, cuando se muestre un patrón más recurrente deberá ajustar las medidas para evitarlo.
	4		
Apreciable	5	Evitar/Reducir	Ante un riesgo apreciable se deberán tomar acciones para discontinuar las actividades que lo generan. En caso de no poder evitarlo se tomaran medidas para reducir su impacto
	8		
Importante	9	Reducir/Compartir	Cuando se cuente con un riesgo importante se buscaran las medidas necesarias para compartir y en última instancia reducir el impacto
	11		
	14		

NIVEL DEL RIESGO	VALOR	RESPUESTA AL RIESGO	DESCRIPCIÓN
Muy Grave	15	Reducir/Compartir/Transferir	Siempre que se esté ante un posible riesgo muy grave se tomaran acciones para transferirlo, en caso de ser inevitable la transferencia se buscara reducirlo o compartirlo
	19		
	25		

A continuación se presentan los controles a seguir para cada riesgo identificado, se describen el factor de riesgo, el evento y el control o medidas a implementar.

TABLA N° 13: Controles para la mitigación de los riesgos.

FACTOR DE RIESGO	EVENTO O RIESGO	NIVEL DEL RIESGO	RESPUESTA AL RIESGO	CONTROLES
Las Contrapartes.				
Agentes Autorizados	Vínculos con grupos delictivos, lo que permite el otorgamiento de cuentas a clientes de dudosa reputación y la realización de transacciones con fondos provenientes de actividades ilícitas.	Muy Grave	Reducir/Compartir /Transferir	Realizar una evaluación del negocio al que se le otorgará la calidad de agentes autorizados que incluya: DUI y NIT del propietario, comprobantes de ingresos mensuales del negocio, y declaración jurada donde se desligue de cualquier vínculo con grupos delictivos y a la vez se comprometa a informar cualquier anomalía presentada al momento de brindar el servicio.

FACTOR DE RIESGO	EVENTO O RIESGO	NIVEL DEL RIESGO	RESPUESTA AL RIESGO	CONTROLES
Agentes Autorizados	Comunicación inadecuada entre el agente autorizado y el personal encargado de la gestión de riesgos de la entidad, al momento de informar sobre la aprobación de cuentas a clientes de dudosa reputación y sobre cualquier operación sospechosa realizada.	Importante	Reducir/Compartir	La sociedad proveedora de dinero electrónico, proporcionará una línea telefónica de apoyo a los agentes autorizados, donde personal capacitado ayudará a resolver cualquier duda o conflicto al momento de otorgar una cuenta de dinero sospechosa.
Agentes Autorizados	Deficiencia en la prestación de servicios ofrecidos por la entidad, lo que conlleva a una mala o nula aplicación de políticas de debida diligencia, que permitan detectar cualquier caso sospechoso de lavado de dinero por parte de los clientes.	Apreciable	Evitar/Reducir	El oficial de cumplimiento programará por lo menos dos veces al año, visitas encubiertas de supervisores a los agentes autorizados con un historial numeroso de transacciones efectuadas, donde se verifique si el agente cumple con las políticas de debida diligencia. Y posteriormente se realizará una evaluación efectiva de la continuidad del negocio como agente autorizado.
Agentes Autorizados	Políticas y procedimientos de debida diligencia	Muy Grave	Reducir/Compartir /Transferir	Elaboración de una bitácora donde quede

FACTOR DE RIESGO	EVENTO O RIESGO	NIVEL DEL RIESGO	RESPUESTA AL RIESGO	CONTROLES
	inadecuados al momento de la aprobación de cuentas y de la realización de operaciones mediante los servicios ofrecidos			registrado, los documentos solicitados al momento de la creación de una cuenta, dicha información debe ser solicitada mensualmente por el supervisor, y llevada a un expediente, el cual se analizará, para verificar que la documentación se encuentra en orden o si se necesitase investigada más a fondo.
Oficial de Cumplimiento	Mala distribución de las labores encomendadas al Oficial de Cumplimiento, este realiza labores fuera del área de la gestión de riesgos, lo que desvía la atención a los casos de lavado de dinero presentados, los cuales deben solucionarse en el menor tiempo posible.	Muy Grave	Reducir/Compartir /Transferir	El departamento de recursos humanos y la oficialía de cumplimiento es la encargada de evaluar la gestión del oficial de cumplimiento, desarrollando los perfiles necesarios para el puesto. Además, se realizaran evaluaciones continuas para verificar el cumplimiento de las funciones establecidas para el cargo.
Oficial de Cumplimiento	El oficial de Cumplimiento no cuenta con las habilidades necesarias	Importante	Reducir/Compartir	Establecer los requerimientos mínimos para el puesto de Oficial

FACTOR DE RIESGO	EVENTO O RIESGO	NIVEL DEL RIESGO	RESPUESTA AL RIESGO	CONTROLES
	para el puesto, en cuanto a la gestión de riesgos y la operatividad del dinero electrónico y los casos de lavado de capitales que se pueden presentar mediante este sistema.			de Cumplimiento, de manera que cumpla con el perfil idóneo para realizar el trabajo de supervisión y comunicación del sistema de gestión de riesgos.
Los Empleados (supervisores)	Encubrimiento de casos sospechosos entre los supervisores y los agentes autorizados, de manera que no se gire una alerta que indique que el cliente está haciendo mal uso de los servicios ofrecidos por la entidad, evitando además el inicio de las investigaciones necesarias para determinar cualquier culpabilidad de delito de lavado de dinero.	Muy Grave	Reducir/Compartir /Transferir	Rotación de los supervisores de zonas, para evitar la complicidad con los agentes autorizados.
Los empleados (Supervisores)	Los casos de operaciones sospechosas no son reportados de forma oportuna al oficial de cumplimiento, para que se investigue el origen de la operación realizada por el cliente, o en su caso	Muy Grave	Reducir/Compartir /Transferir	Capacitaciones y evaluaciones constantes a los empleados, de manera que se pueda determinar si están preparados o no para detectar casos de operaciones sospechosas. Sanciones a los

FACTOR DE RIESGO	EVENTO O RIESGO	NIVEL DEL RIESGO	RESPUESTA AL RIESGO	CONTROLES
	realizar el reporte que será evaluado por los miembros de la alta gerencia, para tomar la decisión si el caso procede hacer investigado por la UIF.			supervisores en caso de no notificar a tiempo cualquier operación sospechosa.
Cliente Origen	Proporcionar información falsa al momento de abrir una cuenta, de manera que no se pueda detectar vínculos con estructuras delictivas.	Muy Grave	Reducir/Compartir /Transferir	Actualizar la información de los clientes cada dos meses o cuando se detecte una operación sospechosa, con el fin de validar si la información es verídica.
Agente Autorizado	No se aplican políticas de debida diligencia ampliada para los clientes considerados como personas políticamente expuestas.	Apreciable	Evitar/Reducir	Realización de capacitaciones y evaluaciones a los agentes autorizados para determinar si pueden reconocer e implementar la debida diligencia a clientes políticamente expuestos.
Cliente Destino	Ausencia de un límite en la cantidad de dinero recibida por el cliente destino, que cumpla con las disposiciones fijadas por la normativa legal aplicable actualmente al cliente de origen, dichos límites	Muy Grave	Reducir/Compartir /Transferir	Los clientes destinos que reciban grandes cantidades de dinero electrónico serán investigados por el oficial de cumplimiento, quien en caso de ser necesario realizará los reportes para

FACTOR DE RIESGO	EVENTO O RIESGO	NIVEL DEL RIESGO	RESPUESTA AL RIESGO	CONTROLES
	deben ser cumplidos, tanto por el cliente que recibe, como el que coloca los fondos dentro de la plataforma electrónica.			que sean analizados por Junta Directiva, para tomar las acciones pertinentes, de manera que se pueda descartar cualquier caso de operación sospechosa.
Los empleados	Las actividades realizadas por el personal de la entidad, no sean llevadas a cabo de conformidad con las leyes, normas y estándares éticos.	Apreciable	Evitar/Reducir	Evaluaciones periódicas a todos los empleados involucrados en las operaciones de dinero electrónico, midiendo su capacidad de resolver situaciones que involucren un posible lavado de dinero, además de su compromiso en el logro de los objetivos y metas de la entidad.
Servicios.				
	Fraude interno y externo, los servicios son utilizados para mover cantidades de dinero ilícito de un lugar a otro del país, sin ser detectados por las autoridades.	Muy Grave	Reducir/Compartir /Transferir	Implementar políticas que verifiquen cada operación realizada por los clientes, de manera que se pueda detectar oportunamente cualquier operación ilícita.
	Fallas en los procesos al momento de efectuar las transacciones, lo que	Importante	Reducir/Compartir	Realizar planes de contingencia que permitan actuar de forma eficiente

FACTOR DE RIESGO	EVENTO O RIESGO	NIVEL DEL RIESGO	RESPUESTA AL RIESGO	CONTROLES
	puede ocasionar alteración en los datos de las operaciones realizadas por los clientes, pasando por alto cualquier actividad ilícita.			en caso de fallas en los procesos. Además, de capacitar al personal para que conozca las medidas a utilizar en cualquier caso de fallas.
	Diseños inapropiados para la prestación de servicios.	Apreciable	Evitar/Reducir	Implementación de un protocolo que muestre paso a paso el proceso que se debe seguir al momento de atender a un cliente. El supervisor evaluará si el agente sigue apropiadamente el proceso.
	Manipulación inadecuada de los registros de las operaciones efectuadas por cada cliente.	Apreciable	Evitar/Reducir	El oficial de cumplimiento programará dos veces al año al equipo de apoyo telefónico, para que realice llamadas a los clientes corroborando la información proporcionada por el agente autorizado, de manera que se pueda comprobar si las políticas de debida diligencia establecidas son realizadas correctamente.

FACTOR DE RIESGO	EVENTO O RIESGO	NIVEL DEL RIESGO	RESPUESTA AL RIESGO	CONTROLES
Canales de Distribución.				
	Fallas en el procesamiento de la información de las operaciones efectuadas por los clientes.	Importante	Reducir/Compartir	Mantenimiento periódico a la plataforma electrónica evitando fallas en las transacciones.
	Manipulación de los servidores por personas externas a la entidad, que ocasionen alteración a los registros de las operaciones.	Muy Grave	Reducir/Compartir /Transferir	El gerente de informática elaborará un reporte donde se evalúen los niveles de seguridad con los que la entidad cuenta, para protegerse de ataques cibernéticos. Este reporte deberá ser presentado a la unidad de auditoría interna y a la oficina de cumplimiento, para su análisis y en caso de encontrar alguna vulnerabilidad en el sistema, se procederá a dar una pronta solución.
	Los límites de dinero establecidos por la ley para las transacciones realizadas con dinero electrónico, no sean verificados por los empleados al momento de que el cliente realice una	Importante	Reducir/Compartir	Revisar los permisos de ingreso a los empleados con acceso a la plataforma virtual, para descartar que estén colaborando en actividades de lavado de dinero y activos.

FACTOR DE RIESGO	EVENTO O RIESGO	NIVEL DEL RIESGO	RESPUESTA AL RIESGO	CONTROLES
	operación, ya sea esto por negligencia o dolo.			
	Falta de copias de seguridad de la información de los clientes y de las transacciones realizadas por estos.	Importante	Reducir/Compartir	El gerente de informática realizará copias de seguridad diarias de las transacciones de dinero electrónico.
	Existencia de clientes que posean más de una cuenta, mediante el mecanismo de prestanombres.	Importante	Reducir/Compartir	Inversión en el sistema que gire alertas cuando se realizan transacciones de diferentes cuentas en una misma ubicación y estas ser investigadas por la oficialía de cumplimiento.
Áreas Geográficas o Jurisdicciones.				
	Ubicación de agentes autorizados en zonas geográficas catalogadas como de alto índice delincuencia.	Muy Grave	Reducir/Compartir /Transferir	Realización de estudios de zonas geográficas donde se encuentren ubicados los agentes autorizados, para analizar los diferentes factores de riesgos a los que están expuestos. Al encontrar un agente autorizado en zona de alto riesgo se procederá a cancelar el contrato con el negocio.
	Entorno de trabajo inadecuado, que no	Importante	Reducir/Compartir	Desarrollar planes de trabajo adecuados para

FACTOR DE RIESGO	EVENTO O RIESGO	NIVEL DEL RIESGO	RESPUESTA AL RIESGO	CONTROLES
	cumpla con los requerimientos mínimos de seguridad para que los empleados puedan cumplir con sus respectivas funciones.			cada uno de los puestos de trabajo, incluyendo las funciones específicas en materia de prevención de delitos de lavado de dinero.
	Transacciones recurrentes desde zonas consideradas de alto riesgo, por la presencia de estructuras criminales.	Muy Grave	Reducir/Compartir /Transferir	Se realizará una investigación a operaciones sospechosas en zonas con presencia criminales, y ante cualquier indicio de mal utilización de las cuentas de dinero electrónico, se procederá a la cancelación de la cuenta.
	Pérdida de información debido a desastres naturales.	Importante	Reducir/Compartir	Establecer planes de prevención y mitigación de riesgos, por causa de desastres naturales.

3.5.2. Definir los procedimientos para aplicar los controles.

- **Procedimientos para el control de los riesgos.**

Para llevar a cabo los controles definidos anteriormente, la entidad debe implementar los siguientes procedimientos:

- Los informes de la gestión de riesgos serán elaborados mensualmente por los encargados de la Oficialía de Cumplimiento y transmitidos a Junta Directiva para que estos puedan evaluar el desempeño y efectividad de las medidas adoptadas. El Oficial de Cumplimiento anexará al

informe correspondiente una serie de recomendaciones o sugerencias que él crea conveniente aplicar, para un mejor tratamiento de los riesgos.

- El encargado del control global de las operaciones realizadas será el Oficial de Cumplimiento, quien identificará cualquier desviación de los controles existentes; en caso de encontrar fallas en el sistema, se deben plantear las posibles acciones de corrección, las que en coordinación con Junta Directiva serán aplicadas.
- Para el control de las actividades externas de la entidad, se delega la función de monitoreo a los supervisores de zonas, quienes tienen la obligación de detectar e informar sobre cualquier anomalía presentada en el curso normal de las operaciones. Los supervisores son los encargados directos de transmitir cualquier información entre la entidad y los agentes autorizados.
- Semanalmente, los supervisores deben elaborar un informe que contenga los casos de operaciones sospechosas y los perfiles de clientes a quienes se les han otorgado nuevas cuentas. Este documento será presentado a la Oficialía de Cumplimiento para su evaluación y registro.
- En cuanto al estudio de los factores externos de la ubicación geográfica de cada agente autorizado, la entidad realiza una evaluación mensual de las condiciones sociales que pueden afectar la actividad del negocio, estableciendo una calificación de la factibilidad para operar en cada zona, o por el contrario, determinar si es mejor dejar de operar.

- **Medidas de mitigación de riesgos.**

La mitigación de los riesgos se realiza mediante la aplicación de una gestión preventiva, teniendo en consideración la influencia que tienen los diferentes factores de riesgos sobre las operaciones realizadas por la entidad. Las medidas de mitigación comprenden lo siguiente:

- Identificación del grado de compromiso adquirido por parte de dueños y directivos de la entidad. A través de Cartas Compromisos y aplicación de un Código de Conducta. (Anexo N° 4 y 5).
- Manual para la prevención de delitos de lavado de dinero y activos y financiamiento al terrorismo. (Anexo N° 6).
- Programas de Auditoría Interna, que faciliten la verificación del cumplimiento del trabajo de gestión de riesgos. (Anexo N° 7).

- Control de clientes clasificados como Personal Políticamente Expuestas (PEP's). (Anexo N° 8 y 9).
- Mejoramiento de las políticas de control de interno para gestionar los riesgos de lavado de dinero.
- Manual del Oficial de Cumplimiento. (Anexo N° 10).
- Plan de trabajo para el trabajo en la gestión de riesgos para el Oficial de Cumplimiento. (Anexo N° 11).
- Plan de capacitación al personal de ElectroniCash, S.A. en materia de prevención de riesgos de lavado de dinero. (Anexo N° 12).

3.6. Etapa 5: divulgación y documentación

3.6.1. Sistema de documentación y registro de los elementos del sistema de gestión del riesgo

Los responsables de la documentación del sistema de gestión de riesgos de lavado de dinero, son la Junta Directiva en coordinación con la Oficialía de cumplimiento. La información contenida en el registro tiene respaldo físico y electrónico, lo que permite su consulta oportuna, por parte del personal encargado de la gestión de riesgos.

El sistema de registro comprende la siguiente documentación:

Conocimiento general:

- Código de Ética.
- Manual de prevención de lavado de dinero y activos.
- Manual de Oficial de Cumplimiento.
- Resumen que contenga los controles y procedimientos implementados para la mitigación de los eventos de riesgos.
- Programas de capacitación.
- Sanciones por incumplimiento de controles.
- Políticas de debida diligencia.

Documentación sensible:

- Información relacionada con las contrapartes (datos personales, detalle de transacciones, origen de fondos)
- Análisis y Reportes de Operaciones Sospechosas

- Informes presentados por supervisores, oficial de cumplimiento, Junta Directiva, Auditoría Interna, Auditoría Externa y demás entes fiscalizadores
- Planes de capacitación al personal en materia de prevención de delitos de lavados de dinero.

3.6.2. Procedimientos para la realización de reportes internos y externos

Reportes internos

Transacciones Inusuales: este tipo de reportes es elaborado por el supervisor de zona, una vez la plataforma electrónica ha levantado una señal de alerta, que indique que el cliente ha sobrepasado los parámetros establecidos.

Operaciones sospechosas: cada agente autorizado tiene a su alcance un formulario para reportar cualquier operación sospechosa, esta información es transmitida inmediatamente al supervisor, quien reúne la documentación de soporte necesaria, para que sea analizada por el Oficial de Cumplimiento y este informa de la situación a Junta Directiva, quien decide si la información de la operación es transmitida a las instituciones pertinentes para que procedan con las investigaciones del caso.

Incumplimiento de empleados: cada vez que un empleado de la entidad incurra en faltas al sistema de prevención de lavado de dinero, se realiza un reporte que indique la infracción cometida y las sanciones aplicadas. Anexando al expediente el seguimiento y resolución del caso.

Reportes Externos

Reporte de Operaciones Sospechosas: son presentados a la Unidad de Investigación Financiera de la FGR, para que esta inicie las investigaciones pertinentes sobre los clientes involucrados en casos de transacciones ilícitas.

3.6.3. Diseño de planes y programas de capacitación

Se elabora un plan de capacitación anual que es impartido tanto en el proceso de inducción de los nuevos empleados, como con los empleados con mayor antigüedad creando una política de educación continua en materia de prevención de riesgos con el objetivo de contar con personal altamente capacitado capaz de responder ante cualquier eventualidad.

Dicho plan es elaborado y actualizado por el oficial de cumplimiento de la entidad, el cual es autorizado por la junta directiva. Además de contar con un instrumento de evaluación el cual permite medir el nivel de aprendizaje obtenido por los empleados.

Los programas de capacitación tienen la función de informar y comunicar a los miembros de la organización los controles diseñados para la gestión de los riesgos de lavado de dinero, haciendo énfasis en el papel que desarrolla cada empleado en la aplicación de los mismos. Estos son elaborados por la Oficialía de Cumplimiento e incluyen la temática a desarrollar, los objetivos, actividades a realizar, y el periodo en el que se ejecutaran.

3.7. Etapa 6: Seguimiento y Monitoreo

Para dar seguimiento y monitoreo se necesita realizar una apreciación constante de los riesgos y controles aplicables.

3.7.1. Definición de actividades de monitoreo

- ✓ Realizar revisiones periódicas a los documentos contenidos en el sistema de registro de la entidad con el fin de evitar su desfase con el marco normativo aplicable.
- ✓ Segregación de las funciones de los responsables de la gestión de los riesgos.
- ✓ Realizar evaluaciones periódicas a los sistemas computacionales.
- ✓ Mantener actualizo los estudios de zonas geográficas donde se encuentran los agentes autorizados.
- ✓ Mantener un seguimiento constante de los casos reportados como operaciones sospechosas ante las instituciones de investigación.
- ✓ Rotación de los supervisores de zonas de agentes autorizados.

3.7.2. Procedimientos para la realización de actividades de monitoreo.

Tabla N° 14: *Procedimientos para la realización de actividades de monitoreo.*

Actividad	Encargado	Procedimiento
Realizar revisiones periódicas a los documentos contenidos en el sistema de registro de la entidad con el fin de evitar su desfase, con el marco normativo aplicable.	Oficialía de Cumplimiento	Se revisará anualmente los manuales y políticas para la prevención de los riesgos, y se realizaran modificaciones a estos, cuando el marco normativo y legal así lo requiere. Además se realizaran actualizaciones a la base de datos de los clientes.

Actividad	Encargado	Procedimiento
Segregación de las funciones de los responsables de la gestión de los riesgos.	Oficial de Cumplimiento	Anualmente se revisará las funciones asignadas a los responsables de la gestión de los riesgos, con el fin de evaluar el desempeño en sus funciones
Realizar evaluaciones periódicas a los sistemas computacionales.	Gerente de informática	Cada año se realizará una auditoría externa a los sistemas informáticos de la entidad.
Mantener actualizo los estudios de zonas geográficas donde se encuentran los agentes autorizados.	Gerente de Operaciones	Dos veces al año, se realizará un estudio de zonas geográficas, consideradas como de alto riesgo y se evaluará si se sigue contando con los agentes autorizados en esas áreas.
Mantener un seguimiento constante de los casos reportados como operaciones sospechosas ante las instituciones de investigación.	Oficialía de Cumplimiento	Mensualmente se evaluará las operaciones irregulares, con el fin de determinar si es necesario reportarlas como operaciones sospechosas a la UIF.
Rotación de los supervisores de zonas de agentes autorizados.	Jefe de supervisores de agentes autorizados.	Para mejorar la independencia de los supervisores de agentes autorizados, se rotaranualmente, de la zona en la que están asignados.

CAPÍTULO IV CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

- ✚ Es de vital importancia que las Sociedades proveedoras de dinero electrónico implementen los controles preventivos y detectivos necesarios para llevar a cabo una adecuada gestión de los riesgos relacionados con los delitos de lavado de dinero y activos, estos controles deben estar diseñados bajo la base legal y normativa aplicable, y constar en documentos que estén al alcance de todos los miembros de la organización, de manera que se pueda generar la prevención de riesgos de lavado como una cultura empresarial, en el que tanto directivos como demás personal trabajen juntos en la mitigación de riesgos.
- ✚ Las sociedades proveedoras de dinero electrónico están sujetas a reportar sobre cualquier operación sospechosa que indique que los servicios con dinero electrónico prestados, están siendo objeto para que organizaciones con fines ilícitos tengan acceso al Sistema Financiero del país, por lo tanto se debe contar con sistemas de alerta eficientes que permitan una comunicación adecuada y oportuna con la Superintendencia del Sistema Financiero y la Unidad de Investigación Financiera de la Fiscalía General de la Republica.
- ✚ Es necesario que los profesionales en Contaduría Pública puedan formarse, tanto en el aspecto legal como normativo, sobre el área de la gestión de riesgos de lavado de dinero y activos, lo que les permitirá en caso de ser nombrados como oficiales de cumplimiento, realizar un trabajo de gestión de riesgos idóneo que contribuirá a un mejor desempeño en las operaciones llevadas a cabo en la organización.
- ✚ La aplicación adecuada del principio de debida diligencia permite que toda operación llevada a cabo con dinero electrónico, lleve inherente un menor riesgo de lavado de dinero, para esto es necesario que los puntos que funcionan como agentes autorizados de proveer dinero electrónico conozcan sobre las diferentes técnicas y etapas del blanqueo de capitales, de manera que se prevenga y detecte a tiempo cualquier operación sospechosa. Cada agente necesita saber cómo actuar sobre cualquier situación que se presente, evitando de esta manera que la sociedad se vea involucrada en otros tipos de riesgos operativos, reputacional o legales.

4.2. Recomendaciones

- ✚ Cada sociedad proveedora de dinero electrónico debe elaborar y aplicar un adecuado sistema de gestión de riesgos de lavado de dinero y activos, que permita detectar y prevenir cualquier irregularidad u operación sospechosa durante la realización de sus operaciones. Para ello se recomienda hacer uso de las diferentes leyes y normas aplicables, que servirán de guía para la formulación de las medidas de mitigación, además de incluir constantemente un monitoreo que verifique que el sistema de gestión de riesgos está funcionando eficientemente.

- ✚ Dentro del sistema de gestión de riesgos las sociedades proveedoras de dinero electrónico deben preparar, detenidamente, cuáles serán los diferentes procesos y canales de comunicación que se tendrán con las diferentes instituciones reguladoras, para que en caso de presentarse alguna operación sospechosa, esta sea informada rápidamente y se tomen las medidas necesarias.

- ✚ Las instituciones encargadas de la educación superior en nuestro país, deben incluir dentro de la preparación académica de los profesionales de Contaduría Pública, materias sobre la gestión de riesgos de lavado de dinero, lo que implica la formulación de controles de mitigación para estos eventos de riesgo y el monitoreo constante que se debe tener sobre la aplicación de estos, ya que el fenómeno del lavado de dinero es un riesgo latente para cualquier tipo de organización empresarial. Además, el contador público debe mantenerse actualizado de manera independiente, sobre las diferentes leyes aplicables a los delitos de lavado de dinero, así como la normativa local e internacional que se emita a efecto de reducir eventos de riesgo de lavado, por lo tanto es necesario, participar en los diferentes seminarios o capacitaciones que se imparten en esta materia.

- ✚ Para que se lleve a cabo una adecuada aplicación de las políticas de debida diligencia, las sociedades proveedoras de dinero electrónico, deben realizar capacitaciones constantes a los encargados de funcionar como agentes autorizados, de manera que se prevenga y detecte a tiempo cualquier operación sospechosa. Estas capacitaciones deben estar acompañadas de evaluaciones contantes que permitan medir el grado de conocimiento que el agente autorizado tiene sobre las diferentes etapas y técnicas del delito de lavado de dinero y activos.

BIBLIOGRAFÍA

- Asamblea Legislativa de la Republica de El Salvador. (2006). *Ley Especial Contra Actos de Terrorismo*. SAN SALVADO.
- Asamblea Legislativa de la Republica de El Salvador. (2012). *Ley de Supervision y Regulacion del Sistema Financiero* . SAN SALVADOR.
- Asamblea Legislativa de la Republica de El Salvador. (2015). *Ley Para Facilitar la Inclusion Financiera*. SAN SALVADOR.
- Cámara de Comercio de Bogotá. (s.f.). *Modelo de Gestión del Riesgo de LA/FT para el Sector Real*. Bogotá. Recuperado el 30 de abril de 2016
- Comité de Normas del Banco Central de Reserva de El Salvador. (09 de Marzo de 2016). NORMAS TÉCNICAS PARA EL INICIO DE OPERACIONES Y FUNCIONAMIENTO DE LOS PROVEEDORES DE DINERO ELECTRONICO. *Normas para inicio de operaciones y funcionamiento de los proveedores de dinero electronico*. San Salvador, San Salvador, El Salvador: Version para Comentarios.
- Duarte, A. G. (2012). *El Dinero Electrónico como sustituto parcial del efectivo y posible mecanismo para masificar el acceso a los servicios financieros. Análisis de la normativa costarricense y la comparada.* San José, Costa Rica .
- El Diario de Hoy. (5 de Octubre de 2015). El Diario de Hoy. *Tigo Money registró crecimiento de 75% en sus usuarios y va camino a alcanzar el millon*, pág. 34. Recuperado el Noviembre de 2015, de www.elsalvador.com
- Endeavor. (2010). *esmas.com*. Recuperado el abril de 2016, de <http://www2.esmas.com/emprendedor/herramientas-y-articulos/financiamiento/183732/dinero-electronico-tarjetas-inteligentes-smart-cards-software-intercambio-y-servicios-internet/>
- Financiero, Superintendencia del Sistema. (2011). *Colección de Leyes del Sistema Financiero N° 11* (4ta. Reimpresión ed.). San Salvador, San Salvador, El Salvador: Mena Impresiones-Salvador Ernesto Mena.
- Gobierno de Chile. (2016). *Unidad de Analisis Financiero*. Recuperado el 22 de Abril de 2016, de <http://www.uaf.cl/lavado/terrorismo.aspx>

La Prensa Gráfica. (julio de 2004). *La Prensa Gráfica*. Recuperado el mayo de 2016, de <http://especiales.laprensagrafica.com/2004/50casos/casos01.asp>

La Prensa Gráfica. (27 de Septiembre de 2011). *FGR recibe 200 sospechas de lavado de dinero al mes*. Recuperado el 18 de Abril de 2016, de <http://www.laprensagrafica.com/el-salvador/judicial/220347-fgr-recibe-200-sospechas-de-lavado-de-dinero-al-mes>

R24N NOTICIAS. (19 de Marzo de 2016). *R24N NOTICIAS*. Recuperado el Noviembre de 2015, de De Al Capone a Lázaro Baéz: <http://r24n.com.ar/noticia/118349/de-al-capone-a-lazaro-baez>

Superintendencia del Sistema Financiero. (2012). *Preguntas y Respuestas sobre La Ley Contra el Lavado de Dinero y de Activos* (4ta Reimpresión ed., Vol. 923). San Salvador, San Salvador, El Salvador: Diseño e Imprenta Ricaldone.

ANEXOS

ÍNDICE

CONTENIDO

ANEXO N°1: Guía de entrevista.

ANEXO N°2: Análisis de entrevista.

ANEXO N° 3: Glosario.

ANEXO N° 4: Carta compromisode Empleados.

ANEXO N° 5: Código de Conductade ElectroniCash, S.A.

ANEXO N° 6:Manual de prevención de lavado de dinero y activos y financiamiento al terrorismo.

ANEXO N° 7:Programa de auditoria Interna.

ANEXO N° 8: Formulario PEP's.

ANEXO N° 9: Declaración jurada del origen lícito de fondos.

ANEXO N° 10: Manual del oficial de cumplimiento.

ANEXO N° 11: Plan de trabajo del oficial de cumplimiento.

ANEXO N° 12: Plan de capacitación al personal.

ANEXO N° 13: Formulario ROS-01.

GUÍA DE ENTREVISTA

TEMA: Modelo de gestión de riesgos como herramienta en la prevención de lavado de dinero y activos y de financiamiento al terrorismo para los agentes autorizados de proveer dinero electrónico en El Salvador.

OBJETIVO DE LA ENTREVISTA: Conocer sobre la gestión de riesgos de lavado de dinero y activos y de financiamiento al terrorismo, llevada a cabo por los agentes autorizados de proveer dinero electrónico en el país.

DIRIGIDO A:

Nombre: _____

Fecha: _____

Empresa: _____

Cargo: _____

INTRODUCCIÓN: La siguiente entrevista a realizarse se enfoca principalmente en la gestión de riesgos de lavado de dinero y activos y de financiamiento al terrorismo, que se aplica a las operaciones con dinero electrónico efectuadas por los agentes autorizados y sus clientes.

GUÍA DE PREGUNTAS:

- 1- ¿En la empresa que usted representa, se gestionan riesgos?
- 2- ¿Cuentan con un manual de políticas y procedimientos para gestionar estos riesgos?
- 3- ¿Qué tipo de herramientas se utilizan para mitigar riesgos al realizar operaciones con dinero electrónico?
- 4- ¿Se realiza un monitoreo constante en las operaciones realizadas, para supervisar y controlar cualquier evento?
- 5- Entre los diferentes eventos de riesgos que se han identificado, ¿Cuáles cree usted que son los más importantes?
- 6- ¿Se maneja una matriz de riesgo que permita estimar las probabilidades e impactos de estos eventos?
- 7- ¿Qué tipo de alertas son utilizadas para informar que se está frente a un posible caso de Lavado de Dinero mediante el uso del dinero electrónico?

- 8- ¿Existe una comunicación oportuna entre el personal y los responsables de la gestión de riesgos de la entidad, para informar sobre cualquier anomalía?
- 9- Dentro de esta comunicación, ¿Existe una relación de información con la Unidad de Investigación Financiera de la Superintendencia del Sistema Financiero y la Fiscalía General de la República?
- 10- ¿La Junta Directiva u otra forma de gobierno de la entidad ha nombrado un Oficial de Cumplimiento para el trabajo de la gestión de riesgos?
- 11- ¿Se ha trabajado en la formación de un comité asignado para la gestión de riesgos? ¿Quiénes integran este comité?
- 12- ¿Se brindan capacitaciones al personal en materia de mitigación de riesgos? ¿Qué tipo de capacitaciones se imparten?
- 13- ¿Las Auditorías Internas y Externas que se realizan, verifican si se cumple o no con la gestión de riesgos?
- 14- En cuanto a los perfiles de los clientes, ¿Se elaboran expedientes de información por cada uno de ellos? ¿Para la elaboración de estos expedientes se pone en práctica la debida diligencia y el método de “conoce a tu cliente”?
- 15- Para el caso de las personalidades expuestas políticamente, ¿Existen medidas adicionales que permitan establecer la debida diligencia?
- 16- ¿Le han cancelado la cuenta a un cliente por el uso indebido del servicio?
- 17- ¿Existe un procedimiento para asegurarse que un cliente posea una sola cuenta?
- 18- ¿Qué mecanismo se utiliza para evitar que el límite establecido de operaciones no sea sobrepasado por los clientes?
- 19- ¿Tiene un modelo operativo de traslado del dinero electrónico-físico?
- 20- ¿Se establece un control para los destinatarios finales de las transacciones hechas por los clientes?
- 21- En cuanto al hardware y software que utiliza para brindar el servicio de dinero electrónico, ¿Se realizan verificaciones constantes para asegurarse de su buen uso y evitar su obsolescencia?
- 22- La ley de inclusión financiera nos menciona sobre fondos en cuentas de dinero electrónico inactivas, ¿A la fecha registra cuentas inactivas? ¿Después de cuanto tiempo son consideran inactivas?

ANÁLISIS DE ENTREVISTA

TEMA: Modelo de gestión de riesgos como herramienta en la prevención de lavado de dinero y activos y de financiamiento al terrorismo para los agentes autorizados de proveer dinero electrónico en El Salvador.

OBJETIVO DE LA ENTREVISTA: Conocer sobre la gestión de riesgos de lavado de dinero y activos y de financiamiento al terrorismo, llevada a cabo por los agentes autorizados de proveer dinero electrónico en el país.

DIRIGIDO A:

Nombre: Carlos Marroquín

Fecha: 27 de Junio de 2016

Empresa: Mobile Cash, S.A. de C.V

Cargo: Encargado de Negocios TigoMoney

INTRODUCCIÓN: La siguiente entrevista a realizarse se enfoca principalmente en la gestión de riesgos de lavado de dinero y activos y de financiamiento al terrorismo, que se aplica a las operaciones con dinero electrónico efectuadas por los agentes autorizados y sus clientes.

GUÍA DE PREGUNTAS:

1- ¿En la empresa que usted representa, se gestionan riesgos?

Si. De hecho es un aspecto fundamental dentro de la operación de nuestro negocio, todo riesgo enmarcado en la Ley contra el lavado de dinero y activos, es gestionado para no vernos envueltos en problemas judiciales ni casos que perjudiquen la imagen de nuestro negocio.

ANÁLISIS: La gestión de riesgos en una entidad es de vital importancia, ya que la ocurrencia de delitos relacionados con el lavado de dinero tiene un impacto que perjudica el aspecto financiero y negocio en marcha de cualquier entidad, sobre todo cuando se trata de servicios de dinero novedosos, como es el dinero electrónico, se está más expuesto a que se utilice el negocio para cometer delitos por parte de los clientes.

2- ¿Cuentan con un manual de políticas y procedimientos para gestionar estos riesgos?

Si. Existe un manual de políticas y procedimientos que se le proporciona a todo el personal involucrado en la gestión de riesgos, desde los niveles con mayor jerarquía hasta los empleados que tienen contacto directo con los usuarios del negocio.

ANÁLISIS: Pese a que existe un Manual de políticas y procedimientos en la entidad, este no es una herramienta suficiente que permita la mitigación de los riesgos de lavado de dinero, se necesita algo más completo, que englobe cada área de la entidad, se necesitan más herramientas, como manuales asignados para cada encargado, por ejemplo, manuales para un Oficial de Cumplimiento, manuales para el Comité de Gestión de riesgos, planes de trabajo, planes de capacitaciones al personal, lo cual es el propósito de la creación de este modelo, poder proporcionarle a la entidad un modelo paso a paso, con las herramientas necesarias para hacer más eficaz el trabajo de la mitigación de riesgos.

- 3- ¿Qué tipo de herramientas se utilizan para mitigar riesgos al realizar operaciones con dinero electrónico?

Existen medidas preventivas como los límites de dinero fijados en las operaciones diarias que se realizan por cada cliente, el principio del conocimiento del cliente al momento de realizar la apertura de una cuenta y el debido registro de cada transacción.

ANÁLISIS: Se puede notar una deficiencia en cuanto a la existencia de herramientas que permitan gestionar los riesgos, se necesita de una serie de políticas y procedimientos adicionales para prevenir eventos.

- 4- ¿Se realiza un monitoreo constante en las operaciones realizadas, para supervisar y controlar cualquier evento?

Hay dos entidades que lo hacen que es la Unidad de Investigación Financiera de la Fiscalía General de la República y la entidad a la cual represento. La empresa mantiene una comunicación constante y oportuna de cualquier evento que se pueda presentar y que signifique un riesgo para la entidad.

ANÁLISIS: Si bien existe una comunicación oportuna entre la entidad e instituciones como la Fiscalía General de la República, a través de la Unidad de Investigación Financiera, es importante enfatizar en la necesidad de establecer una comunicación adecuada con la Superintendencia del Sistema Financiero y el Banco Central de Reserva de El Salvador, que también forman parte importante en la operación del negocio.

- 5- Entre los diferentes eventos de riesgos que se han identificado, ¿Cuáles cree usted que son los más importantes?

Antes lo que más se daba era la no identificación de las personas que realizaban las transacciones, pero ahora ya no, hoy se lleva un mejor control sobre todos los clientes y sus operaciones. Por ejemplo si hoy un cliente quiere recargar dinero a su cuenta se le pide su Documento Único de Identidad para verificar su identidad y si esta ya se encuentra registrada en la base de datos, el intermediario adicional a esto también pide el PIN de seguridad asignado al usuario para poder proceder a realizar la operación. Además con la entrada en vigencia de la Ley de inclusión financiera se ha minimizado más el riesgo de lavado de dinero, se han podido superar muchas deficiencias encontradas. Antes era sencillo acercarse a un punto Tigo Money y pedir al intermediario que él realizara la transacción, hoy ya no, hoy tiene que ser la propia persona que requiere el servicio la que debe presentar sus documentos.

También se tiene como innovación el contrato que se celebra entre el cliente y la empresa, y los límites que se mencionó anteriormente, hoy son \$ 750.00 mensuales y \$ 250.00 diarios los que se pueden transferir, esto restringe y hace que el cliente lo piense dos veces en usar nuestro negocio para cometer delitos. Pero pese a los esfuerzos que se han realizado, la entidad no puede tener una certeza absoluta de que el negocio no sea utilizado para cometer alguna clase de delito de lavado de dinero.

ANÁLISIS: Según esta repuesta, es difícil asegurar que las operaciones con dinero electrónico realizadas por la entidad, no llevan un porcentaje de probabilidad de ocurrencia de algún riesgo de lavado de dinero, se necesita establecer controles más rigurosos, desde el momento de la apertura de una cuenta hasta el control del destinatario final de la transferencia de dinero.

6- ¿Se maneja una matriz de riesgo que permita estimar las probabilidades e impactos de estos eventos?

Si. Siempre se desarrollan planes de contingencia entre la empresa y la UIF de la Fiscalía General de la Republica. Esta herramienta de estimación es realizada por un comité colegiado que trabaja bajo un principio denominado “Principio de los cuatro ojos”, las decisiones no se toman solas si no que involucran a todos los interesados.

ANÁLISIS: Las matrices de riesgo que se llevan a cabo, sirven para detectar la probabilidad de deficiencias en la operatividad del negocio, y el impacto que pueda tener la ocurrencia de algún evento de riesgo, estas matrices necesitan tener una guía de elaboración, con criterios de clasificación bien definidos, y determinar el riesgo inherente y tolerable para la entidad, y a partir de esto, tomar las decisiones pertinentes para mitigar riesgos.

- 7- ¿Qué tipo de alertas son utilizadas para informar que se está frente a un posible caso de Lavado de Dinero mediante el uso del dinero electrónico?

Cuando se celebra un contrato se le pide al cliente un parámetro de su transaccionalidad, esto se registra electrónicamente y si el cliente realiza una operación mayor a este parámetro dado, automáticamente se da una alerta y se investiga, se hace un reporte en la empresa y se envía a la UIF para que ellos comiencen la investigación. Diariamente estos reportes se llevan a cabo para no tener ninguna investigación en espera.

ANÁLISIS: Los reportes elaborados diariamente por los intermediarios autorizados, son elaborados únicamente si existe un caso de algún cliente que sobrepase su parámetro de transacciones en dinero informado al momento de celebrar el contrato, pero es de notar que existen más hechos que nos dan un indicio de que el cliente puede estar cometiendo delitos de lavado de dinero, por ejemplo, puede realizar operaciones más recurrentes, aunque con el mismo monto de dinero, utilizar una red de personas, lo que se conoce como "Pitufeo" para cometer los delitos.

- 8- ¿Existe una comunicación oportuna entre el personal y los responsables de la gestión de riesgos de la entidad, para informar sobre cualquier anomalía?

Las deficiencias y acciones a tomar no son notificadas a todos los empleados por motivos de seguridad, porque se tratan de solucionar dentro del comité. Pero en cuestión de intermediarios si hay supervisores directos quienes guardan unas bitácoras de todos los acontecimientos que vayan sucediendo y también en muchas ocasiones estos supervisores se reúnen con los demás supervisores de su zona para realizar un análisis más profundo y cerciorarse de primera mano de cualquier circunstancia que esté sucediendo.

ANÁLISIS: Si bien existe una comunicación oportuna entre los responsables del negocio y el personal, se necesita hacer acciones que complementen dicha comunicación, como comunicar las acciones correctivas a problemas frecuentes, esto permitirá una mayor eficiencia en la resolución de estos problemas.

- 9- Dentro de esta comunicación, ¿Existe una relación de información con la Unidad de Investigación Financiera de la Superintendencia del Sistema Financiero y la Fiscalía General de la República?

Si. Esta relación es muy estrecha con la FGR., toda sospecha es informada inmediatamente a esta entidad para que ellos tomen las acciones que consideren

pertinentes. En cuanto a la comunicación con la SSF, no se mantiene una relación constante, más bien se trata del cumplimiento de la normativa y leyes que esta emite.

ANÁLISIS: Se debe mantener una comunicación con ambas instituciones, ya que estas se complementan, la Fiscalía General de la Republica enmarca en su materia penal y la Superintendencia del Sistema Financiero vigila por que se cumple con la normativa legal y técnica establecida para los casos de lavado de dinero.

10- ¿La Junta Directiva u otra forma de gobierno de la entidad ha nombrado un Oficial de Cumplimiento para el trabajo de la gestión de riesgos?

Si. Existe una persona encargada de velar por el trabajo realizado en materia de prevención de riesgos de lavado de dinero. Este oficial esta también asignado a las demás aéreas de negocio de la empresa no solamente lo que tiene que ver con dinero electrónico.

El oficial de Cumplimiento forma parte del Comité de Aseguramiento de Ingreso, como se le llama, en donde se ve toda la parte de la gestión de riesgos de toda la entidad.

ANÁLISIS: la definición de un Oficial de Cumplimiento dentro de la entidad es de vital importancia, pero desde un punto de vista más eficiente, la carga laboral que este tiene debe ser más liviana, debido a que la empresa como tal maneja una gran cantidad de operaciones, debe asignarse más personal para este cargo. Podría asignarse un Oficial de Cumplimiento para cada área de negocio.

11- ¿Se ha trabajado en la formación de un comité asignado para la gestión de riesgos? ¿Quiénes integran este comité?

Sí, es el Comité de Aseguramiento de Ingresos, es un comité muy amplio, sin embargo lo lideran cuatro personas que son las que están directamente relacionadas con los riesgos que se pueden presentar para cada área, riesgos de Tigo Star, riesgos de Tigo Smart, riesgos de Tigo Business y riesgos de Tigo Money.

ANÁLISIS: Dentro de la empresa se recomienda que se cuente con un comité que ayude al Oficial de Cumplimiento en la gestión y mitigación de los riesgos, sobre todo cuando se trate de situaciones o eventos que son considerados de alto riesgo.

12- ¿Se brindan capacitaciones al personal en materia de mitigación de riesgos? ¿Qué tipo de capacitaciones se imparten?

Si. Incluso algunas de estas capacitaciones son calificadas, es decir, que el personal realiza una evaluación sobre el material que se les imparte, sobre las leyes, normas y

demás contenido impartido. De hecho en muchas ocasiones la empresa se ha visto forzada a ya no necesitar del personal, por la falta de conocimiento que este tiene, sobre la materia de prevención de lavado de dinero.

ANÁLISIS:El contar con un personal calificado es sumamente importante por lo que se está obligado a dar capacitaciones constantes, en ellas se imparten temas importantes sobre leyes, reglamentos y normas en materia de prevención de lavado de dinero y activos y financiamiento al terrorismo, el realizar evaluaciones lo vuelve más eficaz ya que se puede determinar que personal está debidamente preparado ante cualquier evento.

- 13- ¿Las Auditorías Internas y Externas que se realizan, verifican si se cumple o no con la gestión de riesgos?

Si. Hay un departamento de Auditoria Interna, que se encarga de la supervisión de las operaciones de dinero electrónico y por supuesto de todo el entorno del negocio.

ANÁLISIS:El departamento de auditoria interna es de vital importancia para verificar el buen funcionamiento de los controles establecidos, pero debe de adoptar medidas adicionales como lo son programas de auditoria exclusivos al dinero electrónico.

- 14- En cuanto a los perfiles de los clientes, ¿Se elaboran expedientes de información por cada uno de ellos? ¿Para la elaboración de estos expedientes se pone en práctica la debida diligencia y el método de “conoce a tu cliente”?

Si, Por el mismo principio de conocimiento del cliente que establece la norma, se crea el expediente de cada uno de los clientes los que se identifican por su número telefónico.

ANÁLISIS:se debe tener el máximo cuidado al generar una cuenta, ya que al realizar la debida diligencia y al momento de conocer al cliente, se asegura que este cumpla con todos los requisitos que establece la ley para luego ser creado el respectivo expediente de cada cliente.

- 15- Para el caso de las personalidades expuestas políticamente, ¿Existen medidas adicionales que permitan establecer la debida diligencia?

No se lleva un expediente ni medidas adicionales para este tipo de personas ya que se lleva un control por número de telefónico y número de DUI, pero se emiten las mismas alertas a todos tipo de clientes no importando si son personas públicamente expuestas.

ANÁLISIS:La norma para la gestión de los riesgos nos establece que debe de contarse con una base de datos de las personas expuestas políticamente, haciendo uso de la debida diligencia ampliada para el caso de dichos clientes, y así poder tener un mayor control de las transacciones que realizan.

16- ¿Le han cancelado la cuenta a un cliente por el uso indebido del servicio?

Si, incluso si estos números poseen aún dinero electrónico en sus teléfonos, se lleva a un proceso de reciclaje donde se desactivan y son llevados a un proceso de limpieza donde se anula este número por completo del sistema y no es otorgado a otros clientes después de un periodo establecido como en otros casos.

ANÁLISIS:Es necesario establecer sanciones para los usuarios del sistema de dinero electrónico en caso de no hacer un buen uso, es importante que el cliente este enterado de lo que puede o no hacer con una cuenta de dinero electrónico y las consecuencia que conlleva su mala utilización que en el peor de los casos puede ser la cancelación del servicio.

17- ¿Existe un procedimiento para asegurarse que un cliente posea una sola cuenta?

Si, el sistema está programado para que se emita una cuenta por un solo DUI, aunque se puede eliminar una cuenta con un número anterior y crear una nueva con un número nuevo siempre con el mismo cliente.

ANÁLISIS:Es difícil determinar que un cliente cuente con una sola cuenta, se realizan esfuerzos constantes para cumplir con esta medida dentro de ella esta programar el sistema de forma que solo permita un DUI por cuenta, en un solo teléfono móvil.

18- ¿Qué mecanismo se utiliza para evitar que el límite establecido de operaciones no sea sobrepasado por los clientes?

Desde el cliente es prácticamente imposible que se sobrepase el límite, al igual que para los empleados ya que modificar algo que está establecido en las plataformas es sumamente difícil y costoso.

ANÁLISIS:Uno de los principales riesgos con los que se cuentan es que se burle el sistema y se modifique los límites de saldos establecidos por la ley, la empresa en cuestión manifiesta que es casi imposible debido a su gran complejidad y alto costo el modificar algún parámetro de la plataforma virtual.

19- ¿Tiene un modelo operativo de traslado del dinero electrónico-físico?

Hay un monto mínimo de \$ 300 que cada agente debe de manejar tanto físico como electrónico, aunque existen agentes que cuentan con mucha transaccionalidad se puede aumentar el monto asignado, en cuanto al traslado físico del dinero se le entrega el excedente del monto mínimo que cada agente debe poseer al encargado de proveerle ese dinero electrónico al agente y este lo traslada a la cuenta de la empresa.

ANÁLISIS: Debido al alto volumen de transacciones que realizan y la gran cantidad de dinero que se mueve al utilizar este servicio es recomendable contar con un modelo operativo de traslado de dinero, sobre todo aquellos agentes autorizados que manejan un alto volumen de dinero electrónico-físico, es recomendable que se utilice un servicio de traslado de valores.

20- ¿Se establece un control para los destinatarios finales de las transacciones hechas por los clientes?

Se está implementando más controles para el destinatario final entre ellos que debe contar con una cuenta debidamente registrada, además se pondrán límites en la cantidad que pueda retirar.

ANÁLISIS: Actualmente no se encuentra regulado el destinatario final el cual no cuenta con un límite de saldo el cual pueda recibir en un periodo de tiempo, volviendo lo un riesgo, ya que puede ser utilizado por organizaciones delictivas para el lavado de dinero y activos y financiamiento al terrorismo.

21- En cuanto al hardware y software que utiliza para brindar el servicio de dinero electrónico, ¿Se realizan verificaciones constantes para asegurarse de su buen uso y evitar su obsolescencia?

Todo el software y hardware utilizados por la compañía están a la vanguardia de la tecnología y tiene un mantenimiento constante, se cuenta con personal encargado de verificar el buen funcionamiento de todo el sistema.

ANÁLISIS: El hardware y software son herramientas fundamentales, por lo que contar un mantenimiento constante es de vital importancia ya que el descuido de los mismos puede traer consecuencias legales y económicas, por lo que es necesario contar con personal debidamente capacitado que verifique el buen funcionamiento de los mismos.

22- La ley de inclusión financiera nos menciona sobre fondos en cuentas de dinero electrónico inactivas, ¿A la fecha registra cuentas inactivas? ¿Después de cuánto tiempo son consideradas inactivas?

A la fecha no se registran cuentas inactivas ya que el periodo es de 5 años para poder hacer el traspaso de fondos al Estado.

ANÁLISIS: actualmente la empresa cuenta con cuatro años brindando tal servicio por lo que aún no se puede determinar cuentas inactivas según la ley.

GLOSARIO

Conceptos básicos relacionados con el dinero electrónico.

- **Cliente:** Persona natural titular de un registro de dinero electrónico.
- **Comercio afiliado:** Personas Naturales o Jurídicas con las cuales los proveedores de dinero electrónico hayan suscrito un contrato, en los cuales se realizarán las operaciones de pago por medio de dinero electrónico.
- **Debida diligencia ampliada o mejorada:** Es el conjunto de políticas, procedimientos y medidas diferenciadas de control interno razonablemente más rigurosas, exigentes exhaustivas que las entidades deben diseñar y aplicar a los clientes clasificados como de alto riesgo, a partir del análisis de los factores.
- **Dinero electrónico:** Es el valor monetario registrado a favor de un titular, que constituye una obligación de pago exigible a su proveedor, el cual es aceptado por los demás actores que hayan convenido recibir o prestar este servicio, como un medio de pago en un monto equivalente al dinero efectivo entregado, y se almacena en un soporte electrónico. Su titular podrá utilizarlo para hacer transferencias locales, pagos y conversión a dinero en efectivo al valor nominal.
- **Dinero flotante:** Cantidad de dinero electrónico total que está habilitado en la plataforma electrónica de un proveedor de dinero electrónico.
- **Operaciones con dinero electrónico:** Pagos y cobros, acreditaciones de registros de dinero electrónico, conversión de dinero electrónico a dinero en efectivo y cualquier tipo de transferencia de dinero electrónico a dinero en efectivo y cualquier tipo de transferencia de dinero electrónico realizadas por medio de depósitos móviles.
- **Operaciones irregulares o sospechosas:** Todas las operaciones poco usuales, que se encuentran fuera de los patrones de transacciones habituales y las que no sean significativas pero sí periódicas, sin fundamento económico o legal evidentes, y todas aquellas operaciones inconsistentes o que no guardan relación con el tipo de actividad económica del cliente.
- **Participantes en el manejo con dinero electrónico:** Personas naturales o jurídicas que intervienen en el proceso de proveeduría de dinero electrónico, como son los titulares de comercios, los puntos de atención, distribuidores, entre otros. Éstos dependerán del modelo de negocio que defina cada proveedor de dinero electrónico.

- **Plataforma electrónica o tecnológica:** Conjunto de componentes de hardware y software, en los cuales se recolecta, procesa, transmite y almacena la información utilizados para administrar el dinero electrónico total habilitado por el proveedor.
- **Proveedores de dinero electrónico:** Son las sociedades proveedoras, Bancos, Bancos Cooperativos y Sociedades de Ahorro y Crédito autorizados para proveer dinero electrónico.

Conceptos básicos relacionados con lavado de dinero y activos.

- **El comité de prevención de lavado de dinero:** es el responsable de velar por el cumplimiento de la Ley y el Reglamento contra el lavado de dinero y activos y del Instructivo de la Unidad de Investigación Financiera para la prevención de lavado de dinero y activos de las instituciones de intermediación financiera y aquellas disposiciones de otras leyes y normas externas e internas que al efecto sean emitidas con posterioridad
- **Factores de riesgo:** Estos pueden ser; clientes, usuarios, productos y servicios canales de distribución, zona geográfica y países considerados como paraísos fiscales.
- **Financiamiento al Terrorismo (FT):** es 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 fondos para llevar a cabo sus actividades, cuyo origen puede provenir de fuentes legítimas, actividades delictivas, o ambas.
- **GAFI:** Grupo de Acción Financiera Internacional, organismo internacional, generador de las nuevas cuarenta recomendaciones y sus criterios esenciales, contra el lavado de dinero y financiamiento al terrorismo.
- **GAFIC:** Grupo de Acción Financiera Internacional Caribe. Es el organismo internacional que evalúa el cumplimiento de las cuarenta recomendaciones y sus criterios esenciales de los países del Caribe, México, Centroamérica y Venezuela en la prevención de lavado de dinero y financiamiento al terrorismo.
- **Gestión de riesgos:** es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.
- **Inclusión financiera:** tener acceso a un conjunto de productos y servicios financieros que incluyen crédito, ahorro, seguros, sistema de pagos y pensiones, así como educación financiera y protección al consumidor.

- **Manual de políticas:** Manera de alcanzar objetivos. Es un plan permanente que proporciona guías generales para canalizar el pensamiento administrativo en direcciones específicas.
- **Matriz de riesgo:** Una matriz de riesgo constituye una herramienta de control y de gestión normalmente utilizada para identificar las actividades (procesos y productos) más importantes de una empresa, el tipo y nivel de riesgos inherentes a estas actividades y los factores exógenos y endógenos relacionados con estos riesgos (factores de riesgo). Igualmente, una matriz de riesgo permite evaluar la efectividad de una adecuada gestión y administración de los riesgos financieros que pudieran impactar los resultados y por ende al logro de los objetivos de una organización.
- **Modelo de gestión de riesgos:** Esta es una guía que fortalece, complementa y apoya la gestión empresarial contra los riesgos de lavado de activos, la financiación del terrorismo y el contrabando. Así mismo permite que los empresarios adopten medidas preventivas y de control para evitar ser usados en estas actividades delictivas.
- **Lavado de dinero y activos:** Mecanismo mediante el cual las personas depositan, retiran, convierten o transfieren fondos, bienes o derechos relacionados que proceden directamente o indirectamente de actividades delictivas con el objeto de encubrir su origen ilícito. También se entenderá por lavado de dinero y de activos, cualquier operación, transacción, acción u omisión encaminada a ocultar el origen ilícito y a legalizar bienes y valores provenientes de actividades delictivas cometidas dentro o fuera del país.
- **Objetivo de la gestión de riesgos:** es reducir diferentes riesgos relativos a un ámbito preseleccionado a un nivel aceptado por la sociedad. Puede referirse a numerosos tipos de amenazas causadas por el medio ambiente, la tecnología, los seres humanos, las organizaciones y la política. Por otro lado, involucra todos los recursos disponibles por los seres humanos o, en particular, por una entidad de manejo de riesgos (persona, staff, organización).
- **Oficial de cumplimiento:** Es el funcionario designado por la Junta Directiva y responsable de velar por el cumplimiento del marco regulatorio aplicable.
- **Oficialía de cumplimiento:** Unidad administrativa de la entidad cuyo objetivo fundamental es velar por el cumplimiento del marco legal y normativo en materia de riesgos de lavado de dinero y financiamiento al terrorismo.
- **Personas Políticamente Expuestas (PEP's):** Son aquellas personas naturales identificadas al inicio o en el transcurso de la relación contractual, nacionales o extranjeras, que desempeñan o han desempeñado funciones públicas en nuestro país o país de origen, así como sus parientes

en primer y segundo grado de consanguinidad o afinidad compañeros de vida y sus asociados comerciales o de negocios.

- **Riesgo de lavado de dinero y de activos y de financiamiento al terrorismo:** Probabilidad de pérdida o daño que puede sufrir una entidad como consecuencia de ser utilizada de manera directa o a través de sus operaciones como instrumento para el lavado de dinero, activos y como canalizadora de recursos para el financiamiento del terrorismo o el encubrimiento de activos provenientes de dichas actividades delictivas.
- **Reportes de Operaciones Sospechosas (ROS):** contienen información sobre operaciones o transacciones que los sujetos obligados a informar a la UAF detecten como inusuales de acuerdo a los usos y costumbres de la actividad que ellos desarrollan, carentes de justificación económica o jurídica aparente, ya sea que se realicen en forma aislada o reiterada.
- **Sistemas de alerta:** Las señales de alerta como su nombre lo indica nos, muestran los comportamientos particulares de los clientes y las situaciones atípicas que presentan las operaciones y que pueden encubrir operaciones de lavado de activos. Hay que tener en cuenta que no todas las operaciones que presentan comportamientos atípicos e inusuales son operaciones ilegales, por tal razón, el hecho de identificar señales de alerta no significa que la operación deba ser reportada de manera inmediata y automática a las autoridades como sospechosa.

Carta Compromiso

San Salvador, ___ de _____ de20__

Yo, _____, con Documento Único de Identidad número _____, en mi capacidad de empleado (ya sea fijo o temporal) y en consideración de la relación laboral que mantengo con la empresa ElectroniCash, S.A., así como del acceso que se me permite a sus bases de información, constato que:

1. Soy consciente de la importancia de mis responsabilidades en cuanto a no poner en peligro la integridad, disponibilidad y confidencialidad de la información que maneja mi empresa. Entiendo y me comprometo a cumplir los Procedimientos de Seguridad de los Sistemas de Información que corresponden a mi función en la empresa.
2. Me comprometo a cumplir, asimismo, todas las disposiciones relativas a las políticas de la empresa en materia de uso y divulgación de información, y al trabajo relacionado con la gestión de riesgos de lavado de dinero y activos y financiamiento al terrorismo.
3. Que mi persona no mantiene relación alguna con organizaciones delictivas, que signifiquen un riesgo importante para la entidad en cuanto a ser objeto de actividades ilícitas, que dañen sus operaciones y su imagen empresarial.
4. Entiendo que el incumplimiento de cualesquiera de las obligaciones que constan en el presente documento, intencionadamente o por negligencia, podrían implicar en su caso, las sanciones disciplinarias correspondientes por parte de la empresa y la posible reclamación por parte de la misma de los daños económicos causados.

Firma: _____

Nombre del Empleado

Código de Conducta

ElectroniCash, S.A.



PRINCIPIOS FUNDAMENTALES.

El presente código se compone de principios fundamentales de aplicación general a las personas que, por razón de su cargo o puesto de trabajo tengan o desarrollen responsabilidades y funciones relevantes, en lo sucesivo el "Empleado" o los "Empleados" de ElectroniCash, S.A.

La Junta Directiva en conjunto con la Oficialía de Cumplimiento dará a conocer el presente Código de Conducta a sus empleados, quienes deberán cumplir con todas las normas establecidas en el mismo, ya que se trata de una serie de preceptos que deben regir en todo momento su conducta en los servicios que presta como parte de nuestra empresa.

En virtud de lo antes señalado, el presente documento establece las políticas básicas para la solución de situaciones a las que nos tendremos que enfrentar con frecuencia.

a) Principios que deberán regir en todo momento nuestra conducta:

✓ Honestidad, integridad y justicia.

Un principio fundamental para el éxito de una empresa es brindar un trato justo a todas las personas. Como miembro del equipo de ElectroniCash posiblemente se tendrá un trato directo con clientes, proveedores, auditores, accionistas, funcionarios públicos, competidores, etc. Todos, incluidos nuestros competidores, tienen derecho a esperar que nuestra actuación sea de manera honesta, íntegra y justa en todos aspectos.

✓ Servicio.

Es un valor que se debe desarrollar e inculcar entre todos los compañeros de trabajo, para lograr que cada quien trabaje enfocando sus energías, su intención y entusiasmo en busca de satisfacer las necesidades del cliente.

✓ Eficiencia.

Es procurar hacer las cosas correctamente, en el momento indicado y sin desperdicios, de esta manera se optimizan los recursos y se protegen los intereses de la empresa.

✓ Excelencia.

Es el compromiso de hacer siempre mejor las actividades, manteniendo una superación permanente.

✓ No discriminación.

Es preciso ser objetivo al relacionarse con otras personas, tratando siempre con justicia a todo aquel con el que se esté en contacto (clientes, aspirantes a un puesto, colegas, proveedores, etc.).

Toda empresa considera importantes estos principios fundamentales. Para una empresa de servicios de dinero electrónico como ElectroniCash, cuyo éxito en el mercado depende de los más altos estándares de conducta ética, son especialmente importantes.

De acuerdo a lo anterior, el actuar diario se deberá enfocar en todo momento: a contar con los más altos principios de integridad en todos los niveles, a aplicar la verdad y equidad en cada labor diaria, a incluir siempre la más alta calidad en los servicios brindados, a cumplir siempre con lo establecido por las Leyes y Reglamentos y a poner los intereses de la empresa por encima de los propios.

Es importante recordar que la reputación de la empresa constituye su bien máspreciado y se funda en el acatamiento de los valores antes señalados. Todos deben aplicar estos valores en la conducción de los asuntos que de acuerdo a cada función se han encomendado. Se debe tener presente que la reputación que ha tomado años constituir se puede perder en cualquier momento por conductas irresponsables o deshonestas.

Marco normativo:

El presente Código de Conducta está diseñado, teniendo en cuenta lo previsto en el Instructivo de la Unidad de Investigación Financiera para la prevención del lavado de dinero y activos, que establece que todas las instituciones que conforman el Sistema Financiero del país, deberán regir su actuar diario en las operaciones del negocio bajo un Código de Ética, en el que se establecen las normas y principios éticos que comprometan a los dueños y empleados a trabajar con absoluta honestidad y transparencia.

Todos los Empleados de ElectroniCash, recibirán una copia del presente Código, el cual deberá ser leído cuidadosamente con la finalidad de comprender su contenido. En caso de existir duda sobre alguno de los preceptos utilizados en el presente documento, se deberá contactar a la Oficialía de Cumplimiento, quien será la unidad encargada de apoyar y aclarar las dudas planteadas.

INFORMACIÓN PRIVILEGIADA (O RESERVADA).

a) Normas de actuación en supuestos de Información Privilegiada (o Información Reservada):

Los empleados que se ubiquen en los supuestos de información reservada deberán controlar el acceso, disponibilidad y uso de la misma en los términos previstos en este Código.

Los empleados que dispongan de información privilegiada deberán abstenerse de utilizarla de forma abusiva o desleal, previniendo y evitando en lo posible esta forma de utilización y adoptando además, las medidas necesarias para corregir las consecuencias que de ello pudieran derivarse,

Los empleados que se ubiquen en un puesto de información reservada deberán abstenerse de ejecutar por cuenta propia o ajena, directa o indirectamente, las siguientes conductas:

1. Comunicar dicha información a terceros, salvo en el ejercicio normal de su trabajo, profesión o cargo, de conformidad con lo previsto en este Código.
2. Recomendar a un tercero que apertura cuentas o realice transferencias de dinero electrónico o que haga que otro aperture o transfiera dinero basándose en dicha información.

CONFIDENCIALIDAD.

En el carácter de empleados de ElectroniCash, se tendrá la obligación de tratar la información sobre los clientes, negocios y sistemas de la empresa con una estricta confidencialidad, no se deberá dar aviso o información alguna a terceras personas e incluso a otros empleados, si no se justifica plenamente el que cuenten con dicha información, lo anterior comprenderá toda información relacionada con: saldos de cuentas electrónicas, planes administrativos, financieros y futuros de los negocios, de los salarios de los empleados y de la clientela, así como aquella información obtenida en el curso de relaciones con nuestros clientes.

En carácter de empleados de ElectroniCash, se tiene la obligación de guardar absoluto secreto profesional respecto de lo señalado en el párrafo que antecede, así como de toda la información mientras ésta no se haya hecho pública, lo anterior en cumplimiento a lo señalado por los siguientes Artículos:

A. Código de Trabajo:

Art. 31.-Son obligaciones de los trabajadores:

Guardar rigurosa reserva de los secretos de la empresa de los cuales tuvieren conocimiento por razón de su cargo y sobre los asuntos administrativos cuya divulgación pueda causar perjuicios a la empresa;

B. Instructivo de la Unidad de Investigación Financiera para la Prevención del Lavado de Dinero y de Activos en las Instituciones de Intermediación Financiera.

Capítulo IX del Instructivo-Reserva y confidencialidad

Los funcionarios de la Unidad de Investigación Financiera y de los Organismos de Fiscalización y Supervisión, así como los empleados, funcionarios, directivos, oficiales de cumplimiento, auditores internos y auditores externos de las Instituciones, deberán mantener la más absoluta reserva respecto de los reportes a que se refiere el presente Instructivo, absteniéndose de dar cualquier información o aspecto, que no sea a las autoridades competentes expresamente previstas.

CONFLICTOS DE INTERÉS.

a) Políticageneral:

Si bien como empleado de ElectroniCash, se tiene vida personal e intereses fuera del trabajo, en calidad de empleado de una institución proveedora de dinero electrónico, se debe manejar los asuntos financieros y de negocios sin incurrir en conflictos de interés, ni en nada que lo parezca.

En caso de enfrentar un conflicto de esta índole en el desempeño de un cargo, se deberá informar al respecto a la Oficialía de Cumplimiento lo más pronto posible y presentar una descripción de los hechos que dieron lugar al conflicto y quedar en espera de las instrucciones de Cumplimiento sobre el particular.

b) Regalos de proveedores o clientes:

Las normas Internas de ElectroniCash prohíben que como empleado se acepte o soliciten para uso personal o para terceros cualquier cosa de valor (incluidos efectivo, servicios o cualquier bien) de parte de clientes, proveedores o cualquier persona a cambio de información del negocio, de servicios o sobre aspectos importantes o estratégicos de la empresa.

Existen algunas excepciones a la prohibición general de solicitar o aceptar algo de valor, a saber:

- i. Comidas, cenas y otras formas de entretenimiento (por ejemplo: eventos deportivos, golf, etc.) ofrecidos en el curso ordinario de los negocios de proveedores o clientes y en situaciones en las que normalmente la empresa reembolsaría el costo como gastos comerciales;
- ii. Servicios o descuentos brindados por proveedores o clientes en el curso ordinario de sus negocios; y
- iii. Regalos promocionales como encendedores, lápices, calendarios y similares, distribuidos de manera rutinaria por el donante, u obsequios relacionados con eventos tradicionales y acostumbrados (por ejemplo: Navidad, promociones, etc.) de un valor no mayor que US\$40.00 dólares.

No se podrá aceptar regalos en efectivo, cheques o certificados de regalo convertibles a efectivo, independientemente de la cantidad. En todo caso se deberá informar este hecho a la Oficialía de Cumplimiento.

Si bien es cierto que en algunas ocasiones los proveedores o clientes, pueden enviar regalos costosos sin que la entidad pueda prever esta situación, se tiene que saber qué hacer en estos casos.

En primer lugar será necesario hacer saber del conocimiento dicha situación a la Oficialía de Cumplimiento, quien deberá orientar en el proceso que se deberá seguir en cada caso en particular.

La Oficialía de Cumplimiento enviará a la Gerencia General un reporte de la situación para tomar la mejor decisión colegiada y sin afectar al cliente o proveedor.

COMPORTAMIENTO EMPRESARIAL.

i. Trato con funcionarios públicos:

Las relaciones de ElectroniCash para con los funcionarios públicos no deben comprometer la integridad ni vulnerar la reputación del empleado, se deberá dar por sentado que tales actividades se convierten en asuntos del dominio público.

Si bien es cierto que muchas veces es necesario, por las funciones dentro de la empresa, tener contacto con funcionarios públicos, es necesario tener cuidado de que toda declaración atribuida a ElectroniCash sea compatible con la filosofía de la entidad.

ii. Pagos improcedentes:

La política de ElectroniCash prohíbe el uso de fondos de la empresa para pagar sobornos o hacer pagos improcedentes de todo tipo a personas u organizaciones con el fin de hacer negocios o influir en sus políticas o decisiones, o por cualquier otra razón.

ElectroniCash ha adoptado el Principio 10 de Global Compact de la Organización de las Naciones Unidas. El principio dice a la letra: "Las empresas deberán combatir todas las formas de corrupción, incluida la extorsión y el soborno"

Esta prohibición incluye los pagos no previstos por la ley, para funcionarios, empleados o agentes nacionales o extranjeros. También queda prohibida toda "comisión clandestina" o el intercambio de honorarios con quienes representan a los clientes o los proveedores de la entidad.

En caso de duda sobre la legalidad de los pagos, o si se tiene la sospecha de una comisión clandestina, soborno u otro arreglo ilegal, se deberá reportar de inmediato a la Oficialía de Cumplimiento.

iii. Malas Prácticas de Negocios:

Como empleado de ElectroniCash, se debe evitar en todo momento las conductas que se mencionan a continuación:

- ✓ La demora en el ingreso de las transacciones en beneficio de la cuenta de un cliente preferido o en beneficio propio como empleado.
- ✓ Los negocios a espaldas de los clientes a fin de obtener un mejor trato para otro cliente.
- ✓ La cancelación de negocios importantes en perjuicio de ElectroniCash.

COMPORTAMIENTO INTERNO.

Como empleado de ElectroniCash, se deberá dar prioridad a los intereses de la entidad sobre los individuales, actuar siempre dentro del orden jurídico, respetando las Leyes y Ordenamientos locales al igual que el presente Código de Conducta, todos los empleados son responsables de tratar a sus colegas con dignidad y respeto y de crear un ambiente de trabajo libre de discriminación indebida, acoso sexual, hostigamiento o burla sin importar sexo, identidad de género, embarazo, edad, estado civil, incapacidad, sexualidad, origen racial/étnico, color, religión, creencia o nacionalidad. ElectroniCash no tolerará actos que incumplan esta política y, cualquier muestra de dicho comportamiento, o supuesto comportamiento, se investigará completamente y se estará sujeto a los procedimientos disciplinarios correspondientes.

Se deberá obedecer las órdenes de superiores jerárquicos cumpliendo con todas las funciones y responsabilidades que se tengan por cada cargo, siempre y cuando la ejecución de éstas o el cumplimiento de aquellas no signifiquen la comisión de un delito.

Además, se observará un trato digno y decoroso hacia los empleados que se encuentran bajo el mando del cargo, con estricto apego a los derechos humanos y a las normas disciplinarias aplicables.

Cada empleado desempeñará con honradez, responsabilidad, diligencia y veracidad el servicio encomendado, debiendo abstenerse en todo momento de caer en cualquier acto de corrupción o faltas a la ética, así como de hacer uso de sus atribuciones para lucrar y obtener beneficio alguno por medio del tráfico de influencias.

De igual forma, se deberá evitar en todo momento realizar comparaciones dolosas de los productos de la competencia, debiendo ponderar de manera objetiva los elementos positivos y negativos de los

servicios que presta la empresa y los ajenos, enfatizando los aspectos en los cuales nuestros servicios, superen a los de la competencia, tales como costo o calidad.

No se deberán generar condiciones falsas de demanda u oferta de servicios, con la finalidad de influir artificialmente en sus costos.

PREVENCIÓN DE LAVADO DE DINERO.

ElectroniCash cuenta con un Manual de políticas para prevenir y detectar operaciones con recursos de procedencia ilícita, el cual encuadra los procedimientos para la prevención y detección de lavado de dinero.

Lavado de Dinero:

Las sociedades proveedoras de dinero electrónico pueden, sin darse cuenta, ser utilizados como intermediarios para la transferencia de fondos derivados de actividades delictivas y, por lo tanto, verse involucrados en el proceso de lavado de dinero.

Muchos países del mundo cuentan con leyes contra el lavado de dinero que establecen que se incurre en delito cuando una persona a sabiendas de lo que hace colabore con alguien que realice operaciones con recursos de procedencia ilícita sin informar sus sospechas a la autoridad correspondiente. Lo anterior consiste en no informar una sospecha razonable sobre la existencia de lavado de dinero; o bien no revele a una persona que es objeto de un informe sobre sospecha o de una investigación penal.

De acuerdo a la legislación vigente, ElectroniCash cuenta con procedimientos contra el lavado de dinero contenidos en el manual de prevención de lavado de dinero y activos. Los puntos principales de este manual de prevención de lavado de dinero y activos son:

- ✓ Se deberá verificar cuidadosamente la identidad de todos los clientes nuevos y deberá establecerse adecuadamente la titularidad de todos los contratos; los clientes nuevos que no puedan probar su identidad no podrán abrir ninguna cuenta para los servicios prestados.
- ✓ Las operaciones que se caractericen por ser inusualmente importantes o sospechosas en la operatividad normal del negocio, o de acuerdo con la actividad conocida del cliente, deberán informarse inmediatamente a la Oficialía de Cumplimiento. Se debe recordar que no es necesario estar seguros en un cien por ciento de que una transacción implique dinero ilícito antes de elaborar un informe, la sospecha razonable es suficiente; por lo tanto cada empleado deberá estar alerta y prestar atención a las transacciones inusuales que puedan dar lugar a sospechas;

las que deberán ser informadas a la unidad correspondiente, para que se pueda comprobar si la transacción es sospechosa o no. Si se requiere mayor asesoramiento sobre este importante tema, se podrá consultar con el Oficial de Cumplimiento de ElectroniCash.

CAPACITACIÓN.

La Oficialía de Cumplimiento conjuntamente con la Gerencia de Recursos Humanos, coordinarán la aplicación del curso de capacitación anual en materia de prevención del lavado de dinero y activos y código de conducta, el cual deberá acreditarse en función a cada puesto y responsabilidad de los empleados. Sobre el particular será necesario contar con la certificación correspondiente, misma que se podrá obtener mediante la presentación de un examen.

SANCIONES APLICABLES.

El incumplimiento del presente Código de Conducta, en cuanto a normas internas de ElectroniCash, puede dar lugar a responsabilidades administrativas, civiles, penales y laborales.

El incumplimiento de las normas podrá traer aparejadas las siguientes sanciones:

- **Sanciones Laborales:** Las que conjuntamente lleguen a considerar la Oficialía de Cumplimiento y el departamento de Recursos Humanos, por violaciones al presente Código, las cuales serán impuestas a cada empleado.
- **Sanciones Administrativas:** estas serán las que apliquen las autoridades correspondientes por violaciones a las Leyes.

Manual de Prevención de Lavado de Dinero y Activos y Financiamiento al Terrorismo.



INTRODUCCIÓN

Los Accionistas, el Director, la Gerencia General y todos los trabajadores de ElectroniCash, se encuentran ética y profesionalmente comprometidos con los aspectos relacionados a la prevención de lavado de activos y del financiamiento del terrorismo y con la Implementación de medidas necesarias para combatir el uso del sistema financiero para este tipo de actividades.

ElectroniCash, en cumplimiento a las regulaciones nacionales e internacionales, cuenta con políticas y programas de prevención del lavado de activos basados en la identificación de riesgos, las que incluyen los controles necesarios para evitar su utilización como intermediario para estos ilícitos. Las políticas establecidas incluyen: La política conozca a su cliente, conozca a su empleado, política de capacitación para el personal y las diferentes políticas de debida diligencia necesarias en cumplimiento a la normativa vigente, cuyo cumplimiento es obligatorio para todos los miembros de nuestra entidad.

Para cumplir con las políticas y procedimientos de prevención de lavado de activos y financiamiento al terrorismo, ElectroniCash cuenta con herramientas tecnológicas actualizadas de acuerdo con las mejores prácticas que le permiten asegurar a sus clientes un trabajo comprometido en materia de prevención de lavado de activos y financiamiento al terrorismo, bajo un modelo de gestión de riesgos.

La administración de la empresa se asegurará que la conducción de los negocios en la institución se lleve a cabo con ética y que las leyes y las regulaciones pertinentes a las actividades financieras sean cumplidas en toda su extensión. La entidad no ofrecerá o proveerá asistencia en transacciones que tenga buenas razones para suponer que éstas están asociadas con actividades de lavado de activos o vinculadas con el financiamiento del terrorismo.

Con la finalidad de que la organización no sea inadvertidamente utilizada como intermediaria para transferir o aceptar dinero derivado de actividades ilegales, ha desarrollado políticas y procedimientos que le permita a sus colaboradores acceder a herramientas suficientes y necesarias para cumplir con las exigencias normativas nacionales e internacionales, así como el compromiso de mantener un personal permanentemente capacitado y actualizado en la aplicación de mejores prácticas de prevención de lavado de activos y financiamiento al terrorismo.

El cumplimiento del contenido de este manual es obligatorio y la responsabilidad en el cumplimiento de las normativas para la prevención e identificación del lavado de activos y financiamiento del terrorismo, es de todas las autoridades legalmente constituidas y el personal de la entidad (Junta de Accionistas, Junta

Directiva, gerentes, supervisores, agentes autorizados, empleados, asesores, auxiliares, pasantes, temporales y contratados externos).

Cualquier inobservancia o incumplimiento a las normas contenidas en este manual, serán causal suficiente para iniciar las acciones legales que sean del caso, sin perjuicio de las sanciones internas a que dieren lugar, según lo determinado en el Reglamento Interno de la entidad.

I. OBJETIVOS

A. OBJETIVOS GENERALES

- Establecer, políticas, normas, procedimientos y medidas de control apropiadas, que eviten que la entidad, sea utilizada como instrumento en la realización de operaciones y transacciones relacionadas con las actividades del lavado de activos y financiamiento del terrorismo; y, que permitan mantener los registros para notificar a los organismos de control sobre las transacciones financieras inusuales e injustificadas, a fin de prevenir y detectar este delito.
- Contar con un manual efectivo que permita a los directivos y empleados de la entidad disponer de políticas, procedimientos y mecanismos de control que minimicen el riesgo de que la entidad sea utilizada para el lavado de activos y/o financiamiento al terrorismo.

B. OBJETIVOS ESPECÍFICOS

- Establecer políticas y procedimientos internos que permitan a todos los empleados y funcionarios de la entidad, contar con criterios objetivos y técnicos para prevenir actividades ilícitas e inusuales dentro de la misma.
- Aplicar las disposiciones establecidas por los órganos reguladores y demás normas aplicables a la materia.
- Contribuir a la construcción de elementos de juicio sólidos y relevantes, que sirvan como punto de partida para la eficiente investigación y juzgamiento de los casos sobre lavado de activos y/o financiamiento del terrorismo.
- Establecer los medios necesarios para que los empleados y funcionarios de la entidad puedan identificar de manera clara y objetiva las transacciones realizadas en ElectroniCash, a fin de no ser partícipes de actividades ilícitas.
- Mantener la imagen institucional para que los clientes de la entidad realicen sus transacciones con seguridad y confianza.

II. ALCANCE Y ENTES LOCALES

A. Alcance

El contenido de este manual será aplicado por todo el personal, funcionarios y directivos de la entidad y en forma específica por: Gerentes, Supervisores, Agentes Autorizados, personal operativo, personal de negocios y atención al cliente, los mismos que deberán conocer y aplicar especialmente la política "Conozca a su Cliente", como mecanismo para prevenir el lavado de activos y financiamiento al terrorismo en las actividades y negocios que realiza la entidad.

Al adherirse a la política de prevención de lavado de activos y financiamiento al terrorismo, la entidad espera que sus empleados y directivos se manejen de acuerdo a los más altos principios y estándares éticos.

En conformidad al Código de Ética, el incumplimiento de todo lo expuesto en el presente manual implica la aplicación desde una acción disciplinaria en contra del empleado hasta incluir, la terminación anticipada del contrato, sin perjuicio de las sanciones regulatorias y legales aplicables a cada caso.

El presente manual será de consulta obligatoria para directivos, funcionarios y empleados de la entidad.

B. Entes Reguladores y Fiscalizadores Locales.

- ✓ Unidad de Investigación Financiera (UIF) de la Fiscalía General de la República de El Salvador, cuyo objetivo fundamental es la investigación, prevención, detección y erradicación de los delitos previstos en la Ley contra el lavado de dinero y de activos.
- ✓ Superintendencia del Sistema Financiero.

III. NORMATIVAS APLICABLES.

A. Normativa Local.

- ✓ Ley contra el lavado de dinero y de activos. Decreto Legislativo No. 498, vigente a partir del dos de junio de mil novecientos noventa y nueve; Reforma aplicada en el decreto Legislativo N° 568, aprobado el 05 de diciembre de 2013.
- ✓ Reglamento de la Ley contra el lavado de dinero y de activos. Decreto Ejecutivo No. 2, aprobado a los veintiún días del mes de enero del año dos mil.
- ✓ Ley para facilitar la inclusión financiera.

- ✓ Instructivo de la Unidad de Investigación Financiera para la prevención del lavado de dinero y de activos, última actualización en acuerdo N°085, vigente a partir del 01 de junio de 2013.
- ✓ Ley especial contra actos de terrorismo.
- ✓ Ley orgánica de la Fiscalía General de la Republica.
- ✓ Normas técnicas para la gestión de los riesgos de lavado de dinero y de activos y de financiamiento al terrorismo, (NRP-08), del Banco Central de Reserva de El Salvador, (Como Aplicación subsidiaria).

B. Normativa Internacional

- ✓ Recomendaciones del Grupo de Acción Financiera Internacional (GAFI), tomando las últimas recomendaciones (40) vigentes a partir de febrero de 2012.
- ✓ Recomendaciones del Grupo de Acción Financiera Internacional del Caribe (GAFIC).
- ✓ Convenio Centroamericano para la prevención y la represión de los delitos de lavado de dinero y de activos relacionados con el tráfico ilícito de drogas y delitos. Decreto Legislativo No. 126, de fecha 4 de diciembre de 1997.
- ✓ Resoluciones de la Oficina de Control de Bienes Extranjeros del Departamento de Estado de los Estados Unidos de América (Lista de Ciudadanos Especialmente Designados - Lista OFAC)

IV. DEFINICIONES

Para una mejor interpretación del presente documento, se presentan a continuación definiciones sobre el uso de palabras, frases o abreviaturas:

CONCEPTO	DEFINICIÓN
ALTA GERENCIA Y SUS FUNCIONES	<p>La Alta Gerencia es responsable de asignar los recursos y velar porque se implemente adecuadamente la gestión de los riesgos de LD/FT y se cumpla con las políticas, procedimientos, lineamientos, pautas y directrices aprobadas por la Junta Directiva, además tendrá entre otras las siguientes funciones:</p> <p>a) Asegurarse que todas las actividades de negocios que son concretados por el personal de la entidad con los clientes y usuarios sean llevadas a cabo de conformidad con las leyes, normas y estándares éticos establecidos a fin de prevenir los</p>

	<p>riesgos de LD/FT;</p> <p>b) Asegurarse que el marco regulatorio en materia de prevención de LD/FT sea del conocimiento de todo el personal de la entidad y facilitar su acceso de consulta a través de los medios tecnológicos existentes u otros que consideren pertinentes;</p> <p>c) Crear o establecer canales de comunicación que faciliten al personal de la entidad a informar a la oficialía de Cumplimiento cualquier irregularidad que ponga en riesgo a la entidad y que sea considerada como atentatoria a las disposiciones legales aplicables en materia de prevención de LD/FT;</p> <p>d) Asegurarse que la Oficialía de Cumplimiento incluya en sus planes anuales, programas de capacitación, en atención a lo dispuesto en el Art. 35 literal "j" de la Ley de supervisión y regulación del Sistema Financiero; y</p> <p>e) Asegurarse que la Oficialía de Cumplimiento informe a la Junta Directiva de la entidad, los resultados de sus evaluaciones relacionadas con la prevención de LD/FT, por lo menos trimestralmente, dependiendo del grado de riesgo de cada entidad.</p>
CLIENTE	<p>Persona natural o jurídica, pública o privada, nacional o extranjera con la que una institución controlada establece, de manera ocasional o permanente, una relación contractual de carácter financiero, económico o comercial.</p>
DEBIDA DILIGENCIA.	<p>Es el conjunto de procedimientos y medidas para prevenir, detectar, controlar y reportar la LD/FT. ElectroniCash aplica la debida diligencia en todos sus procedimientos, normas y políticas establecidas en el presente manual.</p>
ACTIVIDADES GENERADORES DE LAVADO DE DINERO.	<p>Aquellos delitos base o precedentes, cuyo producto (dinero o bienes) se busca ocultar dado su origen ilícito. Estos delitos son:</p> <ul style="list-style-type: none"> • Comercio de Personas; • Administración fraudulenta; • Hurto y robo de vehículos; • Secuestro;

	<ul style="list-style-type: none"> • Extorsión; • Enriquecimiento ilícito; • Negociaciones ilícitas; • Peculado;(por empleados del estado) • Soborno; • Comercio ilegal y depósito de armas; • Evasión de impuestos; • Contrabando de mercadería; • Prevaricato; (por jueces) • Estafa; y, • Todo acto de encubrimiento y legalización de dinero o bienes procedentes de actividades delictivas.
ELEMENTOS DE PREVENCIÓN DE LAVADO DE ACTIVOS	Son políticas, procedimientos, documentación, estructura organizacional, órganos de control interno, infraestructura tecnológica, formación del personal y divulgación de normas y principios.
FACTORES DE RIESGO	Son las circunstancias y características particulares del cliente, productos, canales y ubicación en la que se realiza una operación, que determinan la mayor o menor probabilidad de que se trate de una operación inusual o que genere un riesgo de lavado de dinero.
FINANCIAMIENTO AL TERRORISMO	Proveer, recolectar, transferir, entregar, adquirir, poseer, negociar o gestionar fondos, bienes, recursos o derechos, sea mediante el ejercicio de actividades legales o ilegales, con la intención de que se utilicen o sabiendo que se utilizarán, en su totalidad o en parte por un terrorista. Así como organizar y dirigir la comisión del delito de terrorismo.
REPORTE DE OPERACIONES SOSPECHAS (ROS)	Documento de carácter confidencial y privado elaborado por el Oficial de Cumplimiento, con el objeto de comunicar a la Unidad de Investigación Financiera una operación calificada como sospechosa.
GESTIÓN DE RIESGO	Es el conjunto de acciones que contribuyen a la administración efectiva del riesgo, éstas son: Identificación, medición, control y mitigación, monitoreo y reporte.
IMPACTO	Es la consecuencia daño o alcance de los efectos que puede causar el

	LD/FT, en ámbitos social, financiero, económico, político, estructural, reputacional, personal, entre otros.
JUNTA DIRECTIVA Y SUS FUNCIONES	<p>La Junta Directiva u órgano equivalente, es la responsable de velar por una adecuada gestión del riesgo de LO/FT, por lo que tendrá las responsabilidades siguientes:</p> <ul style="list-style-type: none"> a) Aprobar un manual para la prevención de lavado de dinero y financiamiento del terrorismo, así como sus modificaciones, en donde se establezcan las políticas, procedimientos, lineamientos, pautas y directrices para la gestión de los riesgos de LD/FT, lo que deberá ser revisado o actualizado al menos una vez al año; b) Crear la Oficialía de Cumplimiento presidida por un Oficial de Cumplimiento que cuente con recursos humanos idóneos, tecnológicos y materiales para una adecuada gestión del riesgo de LD/FT; c) Nombrar al Oficial de Cumplimiento de la entidad, con cargo gerencial y con suficiente autoridad e independencia para la toma de decisiones; d) Establecer que las Auditorías Interna y Externa, verifiquen el cumplimiento del marco regulatorio en materia de prevención de LD/FT; e) Aprobar los planes de trabajo de la Oficialía de Cumplimiento; f) Aprobar programa de capacitación anual en materia de prevención.
LD/FT	Lavado de Dinero y de Activos/Financiamiento al Terrorismo.
LAVADO DE ACTIVOS O LEGITIMACIÓN DE GANANCIAS ILÍCITAS	Proceso en virtud del cual los bienes o activos de origen delictivo se integran en el sistema económico legal, con apariencia de haber sido obtenidos en forma lícita. El lavado de activos es la conversión o transferencia de propiedad, a sabiendas de que se deriva de una actividad criminal, con el objeto de ocultar o disfrazar su origen ilícito o ayudar a una persona que está involucrada en la comisión del crimen, a evadir las consecuencias legales de sus acciones.
LISTAS OFAC	Es un listado de personas, países, entidades y organizaciones de todo tipo (comerciales, políticas, militares, etc.), posiblemente vinculadas a actividades delictivas graves a nivel mundial, publicada por el Tesoro de los Estados Unidos de América y de acceso libre y actualizada frecuentemente.
MITIGADORES DE	Son todas las políticas y procedimientos internos, desarrollados y

RIESGO	ejecutados por ElectroniCash, S.A., para cada factor de riesgo, con el propósito de minimizar o controlar el riesgo al que están expuestos.
MANUAL	Es una expresión formal de todas las informaciones e instrucciones necesarias para operar en un determinado sector, es una guía que permite encaminar en la dirección adecuada de los esfuerzos del personal en una institución,
MERCADO	Conjunto de operaciones o acuerdos de intercambio de bienes o servicios entre individuos o asociaciones de individuos.
NIT	Número de Identificación Tributaria.
OFAC (Office of Foreign Assets Control – Oficina de Control de Activos y Extranjeros)	Es una entidad del Tesoro Americano que administra el control de activos extranjeros y relacionados a estos, en vista de aquellas personas naturales o jurídicas señaladas como terroristas, traficantes internacionales de narcóticos, y aquellos involucrados en actividades relacionadas con la proliferación de armas de destrucción masiva.
OFICIAL DE CUMPLIMIENTO	Es el funcionario designado por la junta directiva y responsable de velar por el cumplimiento del marco regulatorio aplicable. El Oficial debe ocupar como mínimo un cargo gerencial dentro de la organización, contar con suficiente facultad e independencia, a efecto de gestionar los riesgos asociados con el lavado de dinero y de activos y financiamiento al terrorismo.
OFICIALÍA DE CUMPLIMIENTO Y SUS FACULTADES	<p>Unidad administrativa de la entidad cuyo objetivo fundamental es velar por el cumplimiento del marco legal y normativo en materia de riesgos de LD/FT.</p> <p>La Oficialía de Cumplimiento como unidad encargada de la prevención de los riesgos de LD/TF, debe ejercer únicamente funciones de prevención de los riesgos LD/FT, debiendo cumplir con las facultades establecidas en el artículo 16 del Capítulo VII del Instructivo de la UIF y adicionalmente con las siguientes responsabilidades:</p> <ul style="list-style-type: none"> a) Deberá dar estricto cumplimiento al marco legal y normativo en materia de prevención de lavado de dinero y de activos y de financiamiento al terrorismo e instrucciones generadas por la UIF y a la Superintendencia; b) Elaborar las políticas y procedimientos de prevención de LD/FT para su posterior aprobación por la Junta Directiva u Órgano de

	<p>Administración;</p> <ul style="list-style-type: none">c) Elaborar una matriz de riesgos en la cual se evalúen e identifiquen los riesgos a que está expuesta la entidad considerando los factores de riesgos definidos por las normas;d) Realizar monitoreos permanentes a través de sistemas informáticos y de otros medios a las transacciones realizadas por los clientes, usuarios y empleados de la entidad, para establecer la existencia de los casos considerados como irregulares o sospechosos que ameriten informarse a la UIF y a la Superintendencia, de conformidad con lo previsto en las disposiciones legales vigentes;e) Elaborar, desarrollar y difundir a todo el personal de la entidad, por lo menos una vez al año, programas de capacitación relacionados con la prevención de los riesgos de LD/FT;f) Comunicar en forma directa a la UIF, a la Superintendencia y a otras autoridades competentes, de acuerdo con cada caso y en lo que sea pertinente, la información siguiente:<ul style="list-style-type: none">I. Reportes de operaciones irregulares o sospechosas;II. Reportes de operaciones en efectivo de conformidad al umbral establecido en la Ley contra el lavado de dinero y de activos según las disposiciones legales; y,III. Los actos y de las operaciones internas que impliquen actividades que generen preocupación en las entidades y, en su caso, de los empleados, funcionarios o miembros de la Junta Directiva involucrados que por tal motivo se hayan separado de sus puestos.g) Implementar las herramientas informáticas para el control y monitoreo de las transacciones efectuadas por los clientes y usuarios de la entidad;h) Valorar el contenido de los reportes de operaciones inusuales recibidos de las diferentes áreas de negocios de la entidad con el objeto de determinar la necesidad de aplicar la debida diligencia
--	---

	<p>ampliada o establecer si éstos cumplen con los principios fundamentales de la adecuada aplicación de la política conoce a tu cliente y al principio de inconsistencia de clientes para ser informados a al UIF y a la Superintendencia;</p> <p>i) Elaborar y mantener expedientes electrónicos o físicos de los clientes reportados como irregulares o sospechosos a la UIF y a la Superintendencia; durante el plazo establecido en la Ley;</p> <p>j) Requerir a las áreas de negocios la actualización del expediente clientes cuyas operaciones resultan inconsistentes con el perfil declarado;</p> <p>k) Informar a la Junta Directiva sobre las actividades desarrolladas por la Oficialía de Cumplimiento; y,</p> <p>l) Elaborar el plan de trabajo y someterlo a aprobación de Junta Directiva.</p>
OPERACIONES Y TRANSACCIONES	Todas aquellas actividades realizadas bajo un identificador único de cliente y de producto financiero en la entidad.
OPERACIÓN INUSUAL	Se entenderán aquellas que no guarden correspondencia con los patrones regulares de las actividades económicas que normalmente realiza el sujeto por analizar, y cuyo valor debe justificarse; en sí son aquellas operaciones cuyo monto o magnitud, características particulares, y periodicidad o velocidad de rotación con que son ejecutadas, no guardan relación con la actividad económica del/la cliente; salen de los parámetros de normalidad vigente en el mercado en el que se desenvuelve el/la cliente, o no tienen un fundamento legal evidente u objeto lícito.
OPERACIÓN SOSPECHOSA	<p>Son aquellas operaciones tentadas o realizadas, que habiendo sido detectadas como inusuales, luego del análisis y evaluación realizados por ElectroniCash S.A., las mismas no guardan relación con las actividades lícitas declaradas por el cliente, ocasionando sospecha de LD/FT o aun tratándose de operaciones relacionadas con actividades lícitas, exista sospecha de que estén vinculadas o que vayan o que vayan a ser utilizadas para el FT.</p> <p>También es considerada una transacción como sospechosa cuando el/la</p>

	cliente se niega a proporcionar mayor información o cuando las explicaciones y los documentos presentados por este sean marcadamente inconsistentes, incorrectos o no logren eliminar la duda que tiene la entidad.
PARAISOS FISCALES Y CENTROS FINANCIEROS "OFF SHORE"	Son los países que eximen del pago de impuestos a los inversores extranjeros que mantienen cuentas bancarias o constituyen sociedades en su territorio.
PERFIL DE CLIENTE	Es el conjunto de elementos que permite a la entidad controlada determinar información general y actualizada de sus clientes, así como el tipo, magnitud y periodicidad de los servicios y operaciones que el cliente utilizará durante un determinado tiempo.
PERSONAS PÚBLICAS Y/O POLÍTICAMENTE EXPUESTAS (PEP)	Es el nacional o extranjero que desempeña o ha desempeñado funciones públicas destacadas en el país o en el exterior, por ejemplo, Jefe de Estado o de un Gobierno, político de alta jerarquía funcionario gubernamental, judicial o militar de alto rango, ejecutivo estatal de alto nivel, funcionario importante de partidos políticos, así como su conyugue y sus parientes dentro de cierto grado de consanguinidad o de afinidad. La persona calificada por la institución como políticamente expuesta (PEP) será considerada especial solo para efecto de información y para el seguimiento del oficial de cumplimiento, según lo dispongan las leyes y normas vigentes.
REGLAMENTO DE LA UIF	Instructivo de la Unidad de Investigación Financiera para la prevención del lavado de dinero y de activos. Documento que regula las acciones a las que son sometidas las instituciones sometidas al control de la ley de PLD.
RIESGO DE CLIENTES	Es el riesgo intrínseco de los clientes ya sean personas naturales o jurídicas, que debido a la actividad que realizan, área geográfica donde operan, comportamiento transaccional que tienen, etc., pueden utilizar a la entidad en actividades de LD/FT.
RIESGO DE PRODUCTOS Y SERVICIOS	Es el riesgo intrínseco de cada producto y servicio que derivado de su propia naturaleza o característica los expone a ser utilizados para la LD/TF.
RIESGO DE CANALES DE DISTRIBUCIÓN	Es el riesgo inherente de los medios utilizados para prestar, ofrecer y promover los servicios y productos, que por su propia naturaleza o características los expone a ser utilizados para la LD/FT.

RIESGO GEOGRÁFICO	Es el riesgo intrínseco en el área geográfica donde la entidad ofrece sus productos y servicios, que por su ubicación y características, la expone a ser utilizadas para la LD/FT.
RIESGO DE LD/FT.	Se entiende a este riesgo como la posibilidad o probabilidad de pérdida o daño que pueda sufrir ElectroniCash por ser utilizado directamente o a través de sus operaciones como instrumento para la legitimación de ganancias ilícitas o para el FT. Este riesgo se materializa a través de los riesgos relacionados, estos son: el legal, reputacional y el operativo, a los que se expone la entidad, con el consecuente efecto económico negativo que ello puede representar cuando es utilizada para tales actividades.
SARLAFT.	Sistema para la Administración del Riesgo de Lavado de Activos y Financiamiento del Terrorismo.
SEÑALES DE ALERTA	Son hechos, situaciones, eventos cuantías o indicadores financieros que la experiencia nacional e internacional ha identificado como elementos de juicios a partir de los cuales se puede inferir la posible existencia de un hecho o situación que escapa a la que la entidad en el giro normal de sus operaciones ha determinado como normal.
SEGMENTACIÓN	Son las operaciones de clasificación utilizadas por las instituciones del sistema financiero para definir, identificar y analizar adecuadamente los grupos de sus clientes en relación con la gestión del riesgo.
SOCIEDADES PANTALLA	<p>Son formas de sociedades que pretenden ocultar la identificación de quienes han obtenido ganancias ilícitas, las cuales pueden darse en forma enunciativa y no limitativa, bajo las siguientes modalidades:</p> <ul style="list-style-type: none"> • Sociedades Aparentes: Personas jurídicas legalmente constituidas que participan o afirman participar en actividades comerciales, industriales o de prestación de servicios y que una parte importante de su giro de negocios en efectivo podría provenir de la legitimación de ganancias ilícitas. • Sociedades Fantasmas: Personas jurídicas que sólo existen con nombre, sin documentos de registro y de establecimiento, aparecen con mayor intensidad en documentos de expedición y en las órdenes de transferencias de fondos como consignatarios y sirven

	<p>para esconder el origen de fondos provenientes de actividades ilícitas.</p> <ul style="list-style-type: none"> • Sociedades de Domicilio: Personas jurídicas que no se dedican a operaciones comerciales o industriales en el país donde está fijado su domicilio principal y que podrían intervenir en el proceso de acumulación de ganancias ilícitas. Estas personas jurídicas pueden tener vinculación de propiedad, control y/o administración con otras empresas. • Sociedades en Estante: Personas jurídicas que presentan un capital constituido por acciones al portador y permiten a personas naturales realizar operaciones financieras, escondiendo su verdadera identidad. La finalidad de estas personas jurídicas es esconder la propiedad real de las acciones al portador que adquieren de sociedades constituidas.
SUJETO OBLIGADO	Es toda persona natural o jurídica que desarrolla actividades financieras y/o económicas, que está obligada al cumplimiento de la Ley sobre la detección, prevención, control y reporte de LD/FT.
TRANSACCIÓN FINANCIERA	Transacciones que realiza un cliente de cliente de transferencia o pago, en efectivo o por medio de un instrumento electrónico monetario con ElectroniCash.
UIF	Unidad de Investigaciones financieras, Órgano desconcentrado con autonomía funcional, administrativa y operativa que forma parte de la estructura orgánica de la FGR (Fiscalía General de la República).

V. ESTRUCTURA ORGANIZACIONAL

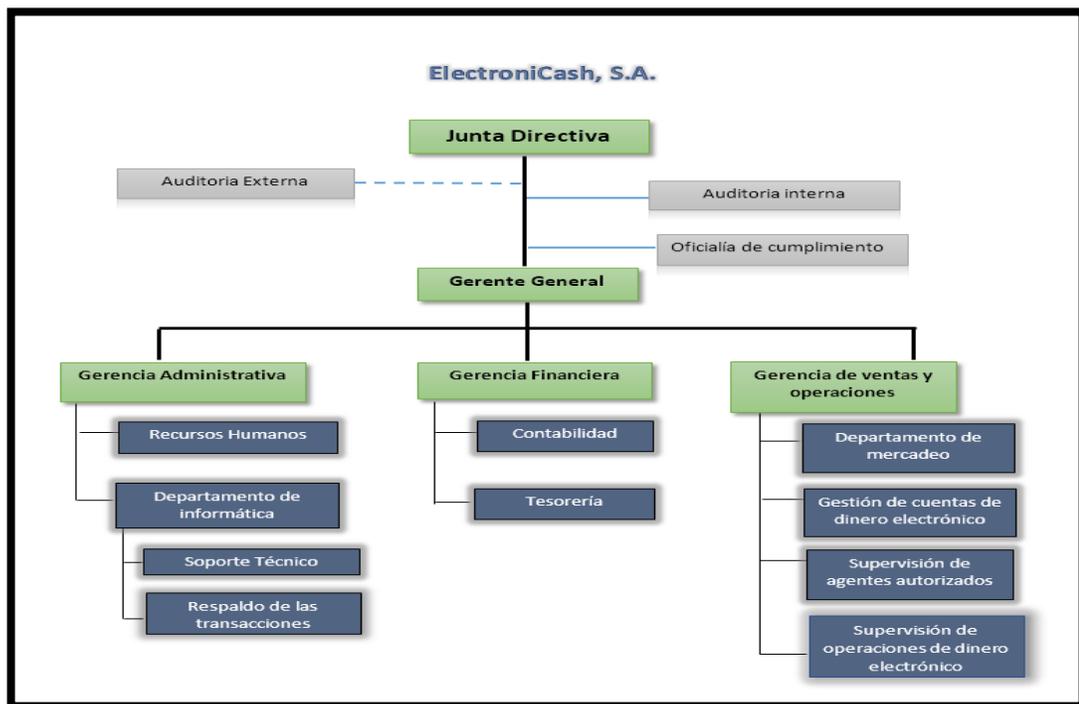
A. ORGANIGRAMA

La estructura organizacional para la prevención del lavado de activos en ElectroniCash, considera responsabilidades en las siguientes instancias, gestiones y cargos:

- Junta Directiva
- Oficialía de Cumplimiento

Junta Directiva, al ser el máximo órgano ejecutivo de la entidad, se constituye en el mayor responsable de la ejecución de las políticas de prevención de lavado de activos de la entidad, sin embargo, operativamente, es el Oficial de Cumplimiento, quien busca el adecuado cumplimiento de las disposiciones plasmadas en el presente manual, así como en las disposiciones legales nacionales. El Oficial de Cumplimiento se contactará con los supervisores de zonas, coordinadores de negocios y otros funcionarios a cargo de administración de agentes quienes actuarán de enlace interno en lo relativo a prevención de lavado de activos.

A fin de explicar la estructura adecuadamente, a continuación se presenta el Organigrama General Gerencial de la entidad:



De la estructura anterior, es posible apreciar que el Oficial de Cumplimiento, mantiene una posición independiente bajo un nivel de jerarquía gerencial, lo cual le permite administrar labores e información adecuadamente. El Oficial de Cumplimiento, asesora al personal operativo, pero depende de la Junta Directiva, manteniendo autonomía funcional para la administración de decisiones dando cumplimiento a lo dispuesto en la regulación vigente y goza con la suficiente autonomía y posición, para requerir todo tipo de información y transferir resultados. La Junta Directiva le permite alimentarse de la información necesaria, para llevar las decisiones y los resultados de información a la Junta de Accionistas.

Auditoría Interna por su parte, responde a una función de asesoría hacia la dirección, pero dada su función de control sobre las políticas de prevención de lavado de activos, mantiene una función de reporte funcional a la Junta Directiva.

La Gerencia General, reflejando su posición de autoridad en la entidad, se hace cargo de la administración y control del cumplimiento de las disposiciones generales establecidas en el manual por parte de cada enlace de cumplimiento (gerencias y jefaturas a cargo).

Estas estructuras reflejan necesariamente la determinación de responsabilidades debidamente justificadas para la consecución de los objetivos de prevención en cada uno de los actores involucrados. Estas responsabilidades se describen en el siguiente punto.

B. RESPONSABILIDADES (ESTRUCTURA FUNCIONAL).

1) JUNTA DIRECTIVA (JD)

La JD, entre otras, tendrá las siguientes funciones:

- a) Aprobar y emitir las políticas generales para la prevención de LD/FT, en el marco de las disposiciones emitidas por los organismos de control vigentes;
- b) Aprobar el código de ética en relación a LD/FT y sus actualizaciones;
- c) Aprobar el manual de prevención LD/FT y sus actualizaciones;
- d) Aprobar plan de capacitación anual en materia de prevención de lavado de dinero
- e) Aprobar, cada año, el plan de trabajo de la oficialía de cumplimiento en materia de prevención de lavado de activos, así como el informe de esta unidad correspondiente al año inmediato anterior;
- f) Llevar a conocimiento de la Junta de Accionistas, los documentos referidos en el numeral anterior;
- g) Aprobar la designación del oficial de cumplimiento, de conformidad con el perfil y requisitos exigidos para ocupar el cargo y removerlo de sus funciones, cuando existan méritos para ello;
- h) Conocer y realizar un seguimiento de las resoluciones adoptadas por la oficialía de cumplimiento, dejando expresa constancia en el acta respectiva;
- i) Aprobar la adquisición de los recursos técnicos y la contratación de los recursos humanos necesarios para implementar y mantenerlos procedimientos de prevención de lavado de activos;
- j) Brindar las facilidades y recursos necesarios y suficientes al Oficial de Cumplimiento para la ejecución de sus funciones y el cumplimiento de sus responsabilidades;

- k) Pronunciarse sobre los informes presentados por la Unidad de Auditoría Interna y hacer seguimiento a las observaciones o recomendaciones presentadas, dejando la expresa constancia en la respectiva acta.
- l) Pronunciarse sobre los informes presentados por la Oficialía de Cumplimiento de LD/FT, referentes a las decisiones y gestiones sobre el tema.
- m) Aprobar los límites de exposición al riesgo de LD/FT.
- n) Aprobar las sanciones para quien incumpla con los procesos de prevención de lavado de activos y financiamiento al terrorismo.

2) EL OFICIAL DE CUMPLIMIENTO Y LA OFICIALÍA DE CUMPLIMIENTO.

Como es posible apreciar en la estructura orgánica, la Oficialía de Cumplimiento, está conformada por el Oficial de Cumplimiento, sin embargo, debido a las funciones asignadas, es necesario considerar que se tratan de labores que representan a una unidad y no solo a una persona y que en el tiempo estas pueden desligarse en función al crecimiento de la misma. En este sentido, la Oficialía de Cumplimiento es la unidad responsable de llevar adelante las actividades de prevención de LD/FT en el ElectroniCash. Esta unidad, representada por el Oficial de Cumplimiento, tiene jerarquía gerencial y depende directamente de la Junta Directiva y reporta a esta las acciones alcanzadas. Su personal principal, el Oficial de cumplimiento, es el encargado de proteger a la entidad, y de evitar la introducción de dineros, derechos y activos provenientes de actividades ilícitas, así como de coordinar y vigilar la observancia, de parte de todos y cada uno de los miembros de la organización de las disposiciones legales y normativas, manuales y políticas internas, prácticas, procedimientos y controles.

La Oficialía de Cumplimiento es una gerencia independiente y cuenta con el apoyo de unidades operativas tales como, sistemas, auditoría interna, operaciones, finanzas, control interno y diversas jefaturas y unidades operativas y de negocios. Además está facultada para acceder a toda la información de la entidad y realizar visitas de inspección a agentes, oficinas y dependencias de la entidad con el objetivo de verificar el cumplimiento de las normas en prevención de LD/FT.

Además La Oficialía de Cumplimiento como unidad encargada de la prevención de los riesgos de LD/FT, debe ejercer únicamente funciones de prevención de los riesgos de LD/FT, debiendo cumplir con las facultades establecidas en el artículo 16 del Capítulo VIII del Instructivo de la UIF y adicionalmente con las siguientes responsabilidades:

- Deberá dar estricto cumplimiento al marco legal y normativo en materia de prevención de lavado de dinero y de activos y de financiamiento al terrorismo e instrucciones generadas por la UIF y a la Superintendencia;
- Elaborar las políticas y procedimientos de prevención de LD/FT para su posterior aprobación por la Junta Directiva u Órgano de Administración;
- Elaborar una matriz de riesgos en la cual se evalúen e identifiquen los riesgos a que está expuesta la entidad considerando los factores de riesgos definidos por estas normas;
- Realizar monitoreos permanentes a través de sistemas informáticos y de otros medios a las transacciones realizadas por los clientes y empleados de la entidad, para establecer la existencia de casos considerados como irregulares o sospechosos que ameriten informarse a la UIF y a la Superintendencia, de conformidad con lo previsto en las disposiciones legales vigentes;
- Elaborar, desarrollar y difundir a todo el personal de la entidad, por lo menos una vez al año, programas de capacitación relacionados con la prevención de los riesgos de LD/FT;
- Comunicar en forma directa a la UIF, a la Superintendencia y a otras autoridades competentes, de acuerdo con cada caso y en lo que sea pertinente, la información siguiente:
 - Reportes de operaciones irregulares o sospechosas;
 - Reportes de operaciones en efectivo de conformidad al umbral establecido en la Ley contra el lavado de dinero y de activos según las disposiciones legales; y,
 - Los actos y de las operaciones internas que impliquen actividades que generen preocupación en las Entidades y, en su caso, de los empleados, funcionarios o miembros de la Junta Directiva involucrados que por tal motivo se hayan separado de sus puestos.
- Implementar las herramientas informáticas para el control y monitoreo de las transacciones efectuadas por los clientes y usuarios de la entidad;
- Valorar el contenido de los reportes de operaciones inusuales recibidos de las diferentes áreas de negocios de la entidad con el objeto de determinar la necesidad de aplicar la debida diligencia ampliada o establecer si éstos cumplen con los principios fundamentales de la adecuada aplicación de la política conoce a tu cliente y al principio de inconsistencia de clientes para ser informados a la UIF y a la Superintendencia;
- Elaborar y mantener expedientes electrónicos o físicos de los clientes reportados como irregulares o sospechosos a la UIF y a la Superintendencia; durante el plazo establecido en la Ley;

- Requerir a las áreas de negocios la actualización del expediente de clientes cuyas operaciones resultan inconsistentes con el perfil declarado;
- Informar a Junta Directiva sobre las actividades desarrolladas por la Oficialía de Cumplimiento; y,
- Elaborar el plan de trabajo y someterlo a aprobación de Junta Directiva.
- Supervisar el adecuado funcionamiento del programa de prevención en concordancia con las disposiciones legales vigentes, en todas las unidades de la entidad, informando a la JD sobre el resultado de los análisis realizados.

El Directorio es consciente que en caso de ausencia temporal o definitiva del oficial de cumplimiento, lo reemplazará un nuevo Oficial de Cumplimiento, aspecto que se deberá comunicar a la UIF en un plazo no mayor a 3 días hábiles. Para este tema, es una obligación que el Oficial de Cumplimiento nuevo cumpla con los requisitos descritos en la normativa aplicable.

La responsabilidad asumida por el Oficial de Cumplimiento no exime a los demás funcionarios, especialmente en áreas operativas, de la obligación de realizar el máximo esfuerzo en detectar y reportar internamente las operaciones inusuales.

Los supervisores de zonas y agentes autorizados, serán los enlaces o encargados de cumplimiento en sus puestos de trabajo, cuyas funciones básicas se resumen en aplicar las políticas de prevención, control y conocimiento del cliente, debiendo reportar al Oficial de cumplimiento su proceder.

Las funciones del Oficial de Cumplimiento se resumen básicamente en el cumplimiento de los objetivos generales establecidos para la Oficialía de Cumplimiento, sin embargo, las funciones específicas se describen a continuación:

- **En relación a la entidad:**

- Elaborar el manual de prevención de LD/FT y sus actualizaciones, para conocimiento y posterior aprobación por parte del JD;
- Velar que el manual de prevención de LD/FT y sus modificaciones se divulgue entre el personal;
- Verificar el cumplimiento de las disposiciones relacionadas a la prevención del LD/FT contenidas en las disposiciones legales vigentes, en el manual de prevención, en el código de ética y en otras normas aplicables;

- Formular estrategias para establecer los controles necesarios con base en el grado de exposición al riesgo de LD/FT;
- Supervisar que las políticas y procedimientos respecto de la prevención de LD/FT sean adecuados y se mantengan actualizados;
- Verificar la aplicación de procedimientos específicos para la prevención de LD/FT por parte de los empleados;
- Controlar permanentemente el cumplimiento de las políticas "Conozca a su cliente", "Conozca a su empleado";
- Verificar permanentemente, en coordinación con los responsables de las diferentes áreas de la entidad, que las transacciones realizadas por los clientes cuenten con los documentos de soporte necesarios;
- Confirmar que los formularios para registrar las transacciones, sean debidamente diligenciados por parte del agentes autorizados quienes son los encargados de atender al cliente al momento que se realiza la transacción;
- Monitorear permanentemente las operaciones o transacciones que se realizan en la entidad, a fin de detectar las inusuales;
- Recibir los informes de operaciones o transacciones inusuales o sospechosas, de acuerdo al mecanismo implementado por la entidad en la política de reporte de transacciones inusuales de LD/FT;
- Realizar el análisis de las operaciones o transacciones inusuales o sospechosas, detectadas y/o reportadas, a fin de determinar el envío o no del reporte a la UIF;
- Dejar constancia de lo actuado sobre la transacciones mencionadas en los puntos anteriores, informes y documentos que, evidencien lo acontecido, deben conservarse por un tiempo mínimo de cinco (5) años;
- Orientar la conservación de los documentos relativos a la prevención de LD/FT, de modo que éstos sean archivados de acuerdo a lo estipulado en este manual;
- Presentar a Junta Directiva, los informes sobre operaciones o transacciones sospechosas reportadas. El informe trimestral y el informe anual de gestión deben referirse como mínimo a los resultados de los procesos de cumplimiento y actividades desarrolladas, sugiriendo acciones de mejoramiento;
- Absolver consultas del personal de la entidad relacionadas con la naturaleza de las transacciones frente a la actividad del cliente;

- Realizar un reporte de aquellas faltas o errores que impliquen responsabilidad de los empleados o funcionarios de la entidad;
 - Coordinar el desarrollo de programas de capacitación y sensibilización dirigidos a empleados de nuevo ingreso y programas de capacitación continua sobre LD/FT para los demás empleados;
 - Cumplir con el rol de enlace con autoridades e instituciones en materia de prevención de LD/FT;
 - Consignar su visto bueno a los nuevos productos y servicios que vaya a implementar la entidad, previa su implementación;
 - Actualizar y depurar la (s) base (s) de datos de clientes que posea la entidad para la aplicación de las medidas de prevención de LD/FT;
 - Definir las responsabilidades y funciones de los asistentes de cumplimiento en función a las tareas descritas en los puntos precedentes;
 - Coordinar y canalizar programas de capacitación internos y con la UIF;
 - Capacitar al personal de la entidad, coordinando con el departamento de Recursos Humanos;
 - Administrar el modelo de gestión de riesgos, monitoreando los factores y variables involucrados;
 - Administrar el Software de prevención de LD/FT, analizando los riesgos vinculantes consecuentes de la generación de alertas.
- **En relación a la Unidad de Investigaciones Financieras (UIF):**
 - Ser registrado ante la UIF como Oficial de Cumplimiento de la entidad.
 - Remitir a la UIF el manual de PLD/FT y sus reformas, previamente aprobados por la Junta Directiva;
 - Acreditarse cuando así lo requiera la UIF, con el objeto de obtener nombre y clave de usuario para efectos de reportes.
 - Reportar a la UIF toda operación y transacción cuya cuantía sea igual o superior a los umbrales establecidos por la ley vigente; así como las operaciones que determine la UIF a través de sus reglamentos.
 - Reportar a la UIF las operaciones y transacciones consideradas sospechosas.
 - Responder de manera oportuna a los requerimientos de información de la UIF.

- Coordinar con la UIF las actividades de reporte, a fin de cumplir adecuadamente las obligaciones de la entidad en esta materia.
- Cooperar activamente con la UIF en la entrega oportuna de la información que ésta solicite; y, comunicar en forma permanente a los directivos, funcionarios y empleados de la entidad acerca de la estricta reserva con que deben mantenerse los requerimientos de información realizados por la UIF.

En cada una de las responsabilidades del Oficial de Cumplimiento y de la Oficialía de Cumplimiento en sí, los analistas de cumplimiento deberán colaborar de acuerdo a las tareas designadas en el manual de funciones y todas aquellas que mejor aprovechen la consecución de los objetivos de la Oficialía de Cumplimiento.

- **Prohibiciones al Oficial de Cumplimiento:**

- Delegar el ejercicio de su cargo;
- Dar a conocer a personas no autorizadas los informes sobre operaciones o transacciones inusuales y/o sospechosas.
- Revelar datos contenidos en los informes, o entregar a personas no relacionadas con las funciones de control, información respecto a los negocios o asuntos de la entidad, obtenidos en el ejercicio de sus funciones.

3) RESPONSABILIDADES DE OTRAS ÁREAS EN LA PREVENCIÓN DEL LAVADO DE DINERO Y ACTIVOS.

1) AUDITORIA INTERNA

- Evaluar la implementación del sistema de gestión del riesgo de LD/FT.
- Evaluar el cumplimiento de la entidad de todas las políticas, normas, procedimientos y mecanismos de control interno relacionados a la LD/FT.
- Poner a disposición de los/as funcionarios/as de la UIF, cuando éstos soliciten, los programas desarrollados y/o evaluaciones realizadas.
- Realizar tareas para evaluar el cumplimiento del presente manual así como de la normativa emitida por la UIF.
- Incluir dentro de su programa operativo tareas para evaluar el sistema de gestión del riesgo de LD/FT.

- Presentar informes al menos semestralmente a Junta Directiva de los resultados de las revisiones realizadas en el tema de PLD/FT.

2) GERENCIA GENERAL

La Gerencia General tendrá las siguientes responsabilidades:

- Asignar los recursos y velar porque se implemente adecuadamente la gestión de los riesgos de LD/FT y se cumpla con las políticas, procedimientos, lineamientos, pautas y directrices aprobadas por la Junta Directiva, además tendrá entre otras las siguientes funciones:
 - Asegurarse que todas las actividades de negocios que son concretados por el personal de la entidad con los clientes, sean llevadas a cabo de conformidad con las leyes, normas y estándares éticos establecidos a fin de prevenir los riesgos de LD/FT;
 - Asegurarse que el marco regulatorio en materia de prevención de LD/FT sea del conocimiento de todo el personal de la entidad y facilitar su acceso de consulta a través de los medios tecnológicos existentes u otros que consideren pertinentes;
 - Crear o establecer canales de comunicación que faciliten al personal de la entidad a informar a la Oficialía de Cumplimiento cualquier irregularidad que ponga en riesgo a la entidad y que sea considerada como atentatoria a las disposiciones legales aplicables en materia de prevención de LD/FT;
 - Asegurarse que la Oficialía de Cumplimiento incluya en sus planes anuales, programas de capacitación;
 - Asegurarse que la Oficialía de Cumplimiento informe a la Junta Directiva de la entidad, los resultados de sus evaluaciones relacionadas con la prevención de LD/FT, por lo menos trimestralmente, dependiendo del grado de riesgo de cada entidad.

3) CONTADOR GENERAL

Es responsable de mantener los archivos contables y demás transacciones, incluyendo los respaldos y documentación sustentadora por un periodo no menor de cinco años contados a partir de la fecha del cierre del ejercicio y reporte. Auditoría verificará el cumplimiento de ésta disposición.

4) ÁREA DE SISTEMAS

- Será el responsable de brindar soporte al administrador el sistema informático de prevención de LD/FT de la entidad y coordinar su mantenimiento con el Oficial de Cumplimiento, cuando el mismo sea establecido.
- Dar prioridad a los requerimientos de desarrollos en sistemas que provengan del Oficial de Cumplimiento.

5) SUPERVISORES DE ZONA

- Mantener actualizado y en perfectas condiciones de lectura, toda la información remitida por la Oficialía de Cumplimiento, manuales, políticas, boletines etc.
- Realizar visitas de verificación de información de clientes cuando así sea necesario en virtud de proteger a la entidad.
- Ser el enlace entre el Oficial de Cumplimiento y los clientes.
- Verificar que los formularios hayan sido llenados adecuadamente.
- Verificar que el personal bajo su dependencia conozca y aplique la política "Conoce a tu Cliente" y que recabe toda la información establecida para los clientes de la entidad.
- Responder a la Oficialía de Cumplimiento dentro de los plazos establecidos cualquier solicitud de información respecto a alguna transacción o cliente.
- Reportar al Oficial de Cumplimiento las operaciones consideradas como inusuales.
- Reportar obligatoriamente al Oficial de Cumplimiento los casos de rechazo de apertura de cuentas, si se establece que el titular, podría estar implicado con el lavado de activos y financiamiento del terrorismo u otro causal de delito.
- Realizar las justificaciones a las operaciones inusuales dentro del plazo establecido por el Oficial de Cumplimiento.
- Presentar informes semestrales al Oficial de Cumplimiento, los mismos deben ser elaborados con corte al 30 de junio y 30 de noviembre de cada año y ser enviados hasta el 05 de julio y 05 de diciembre de cada año según corresponda. Los informes deben contener como mínimo la ocurrencia de eventos que podrían incrementar el riesgo de LD/FT por cada agente autorizado. Además de las transacciones que desde su punto de vista fueron consideradas como inusuales. Este informe debe contener el nombre del agente autorizado, la zona geográfica a la cual pertenece y estar refrendado con su firma y sello.

- Mantener total confidencialidad respecto a números de contrato o cualquier otra información de los/as clientes; el incumplimiento a lo señalado, acarreará sanciones establecidas por ley.
- Mantener total confidencialidad respecto a los clientes cuya información haya sido requerida por el Oficial de Cumplimiento.
- Analizar el comportamiento de las/as trabajadoras/as bajo su dependencia, informando sobre cualquier situación inusual al Oficial de Cumplimiento.

6) AGENTES AUTORIZADOS

Las responsabilidades de los agentes autorizados son:

- Llenar el formulario de registro de clientes (persona natural y persona jurídica), de acuerdo a los procedimientos establecidos en la entidad.
- Solicitar información detallada acerca de la actividad del/la cliente y registrarla en sistema.
- Registrar en sistema y físicamente de manera clara y correcta la información proporcionada por el/la cliente. Generar respaldos de toda esa información.
- Verificar en el sistema interno que todos los datos requeridos para la apertura de operaciones tanto para las personas naturales como jurídicas hayan sido plenamente registrados acorde a lo establecido en el presente manual.
- Solicitar claramente al cliente información sobre el origen y destino de los fondos, además del motivo de la transacción (cuando corresponda). Registrar claramente la información brindada por el/la cliente. Verificar que no existan incoherencias en la información registrada.
- Cuando corresponda, verificar el adecuado llenado de forma manual del F-UIF 01 por parte del/la cliente.
- Verificar que la firma estampada en el F-UIF 01 sea igual a la de documento de identidad de la persona que realiza la transacción.
- Mantener total confidencialidad respecto a números de contrato o cualquier operación que los/as clientes realicen; el incumplimiento a lo señalado, acarreará sanciones establecidas por ley.
- Dar la alerta de transacciones inusuales al Oficial de Cumplimiento.
- Mantener actualizada la información de todos los clientes de la entidad. Dicha actualización deberá realizarse mínimamente con una frecuencia de un año.

7) UNIDADES OPERATIVAS Y PERSONAL EN GENERAL

- La confidencialidad con que se debe manejar toda la información de la empresa debe cumplirse en todo momento, igualmente, quedan prohibidos poner en conocimiento de persona alguna el hecho de alguna información que haya sido solicitada por la autoridad competente o proporcionada a la misma. La violación de esta prohibición, obligará al oficial de cumplimiento a comunicar del particular a la Junta Directiva y esta a su vez notificará a la Unidad de Investigaciones Financieras - UIF, para que se incluyan los nombres de los funcionarios o empleados que hubieren transgredido esta prohibición.
- Por la oportuna presentación de los informes, reportes, formularios, y otros que tengan que ver con el control para prevenir el lavado de activos y financiamiento al terrorismo.
- El cumplimiento de todas las disposiciones procedimientos y controles emitidos por el presente manual de prevención de lavado de activos y financiamiento del terrorismo.
- Porque sus informes y reportes sobre la prevención del lavado de activos sean confiables, ya que en base a ellos se emite los informes a la UIF y otros organismos de control.
- El personal en general y unidades operativas serán corresponsables de la detección y reporte interno de transacciones u operaciones inusuales efectuadas por los clientes, para lo cual se regirán a lo que establece las señales de alerta establecidas por la entidad.

VI. PROCEDIMIENTOS Y CONTROLES OPERATIVOS ASPECTOS GENERALES

La aplicación de los procedimientos específicos de prevención contra el lavado de activos y financiamiento al terrorismo, considera todas las políticas descritas en el presente manual, son de obligatorio cumplimiento de todos los miembros de la entidad en lo relativo a sus funciones, obligaciones y responsabilidades.

En inicio, es importante señalar los siguientes aspectos:

- ❖ Si bien el análisis transaccional y de vinculación que se realiza a través del sistema de prevención de la entidad es propia de la oficialía de cumplimiento; sin embargo es una responsabilidad indiscutible de los agentes autorizados quienes atienden clientes y los supervisores de zona, que realicen periódicamente un monitoreo del perfil de sus clientes y de ser necesario informen al Oficial de Cumplimiento sobre cualquier anomalía en los mismos.
- No obstante a los aspectos que a continuación se detallan, todos los empleados y funcionarios de la entidad, independiente al área que correspondan, al momento de conocer de alguna

transacción u operación que tenga la característica de inusual e injustificada, están en la obligación de reportar la misma, bajo el proceso indicado en las políticas de reporte.

- Al detectar una transacción inusual, no se debe alertar al cliente sobre los reglamentos y disposiciones establecidos por la entidad; simplemente se debe proseguir con la transacción u operación y de inmediato ponerlo en conocimiento al Oficial de Cumplimiento por correo electrónico o cualquier reporte diseñado para el caso.
- Se debe recordar que por lo general, aquellas personas que se "molestan" extremadamente cuando se les solicita información podrían ser potenciales "Estafadores o Lavadores" o quienes quieran utilizar a la entidad para sus actos delincuenciales.
- El conocimiento y aplicación de este manual es de carácter obligatorio para todo empleado y funcionario de la entidad, así como para aquellas personas que, aún sin pertenecer a esta prestan sus servicios profesionales.

VII. SANCIONES Y CORRECTIVOS

De tener constancia material o física que un empleado hubiese incumplido las normas establecidas en el presente manual relacionado a la prevención del lavado de activos y financiamiento al terrorismo, será inmediatamente notificado al Oficial de Cumplimiento y a la Gerencia General para el inicio del proceso administrativo correspondiente.

Las sanciones que se establecen por la inobservancia a cualquiera de las políticas emitidas en el manual de prevención de LD/FT, código de ética y demás normativas vigentes al respecto se sancionarán de la siguiente manera y en correspondencia a lo señalado en el reglamento interno de la entidad:

1. Llamada de atención por escrito si ha obviado algún control, con el compromiso de regularizarlo en un plazo de cinco días laborables y comprometerse a cumplirlo en adelante o por una falta leve de otra índole.
2. En caso de reincidencia sobre la misma falta o por no haber regularizado el error dentro del plazo indicado en el inciso anterior, o por una falta grave sin daño económico o reputacional para la entidad, se le hará llamada de atención por escrito con copia al expediente del empleado.
3. Si se reincidiera por tercera vez en la misma falta, o una falta grave con daño económico o reputacional para la empresa se procederá con la expulsión del empleado de la entidad; sin perjuicio de ser demandado legalmente si el caso lo amerita.

4. Los empleados que se vean implicados ya sea como actores directos o cómplices en razón de permitir o favorecer a alguna(s) persona(s) para ingresar o manejar fondos sin el debido control y procedimiento necesario, serán reportados a la Unidad de Investigación Financiera para deslindar responsabilidad mayor a la entidad; de manera adicional, la empresa podrá iniciar cualquier acción legal si así lo estima pertinente.
5. En caso de multas impuestas por la UIF ocasionadas por negligencia o incumplimiento del empleado, éste cancelará la multa que le imponga el organismo regulador a la empresa. Si para el cumplimiento de un área determinada o por petición oportuna de la misma, se requiere de información y/o documentación que forma parte de la función y responsabilidad de otra(s) área(s), y no la entregan a tiempo, la multa la deberá ser cancelada por el(los) empleado(s) de la(s) otra(s) área(s) que no la gestionaron o no la entregaron oportunamente.
6. Si la sanción representa la suspensión temporal del permiso para operar, es decir hubo reincidencia negligente de incumplimiento, las pérdidas sufridas, recaerán en parte o en su totalidad, sobre su jefe inmediato y/o responsable, por no haber tomado las acciones correctivas necesarias y permitir que se vuelva reincidente el problema, a más de las acciones administrativas que la Gerencia General considere oportunas.

Cuando un empleado se vea implicado por su negligencia o incumplimiento en una acción legal por parte de terceros, la entidad no se involucrará en su defensa, pero si defenderá la reputación de la empresa aun en contra de los intereses del empleado.

Como referencia a las sanciones establecidas por la Ley contra el lavado de dinero, se tienen:

Artículo 7. Delito de Encubrimiento:

- Los que no informaren a las autoridades después de darse cuenta de una actividad delictiva.
- Los que ayudaren a eludir las investigaciones.

Sanción de 5 a 10 años de prisión.

Artículo 8. Encubrimiento Culposo

- Si se produjere por negligencia, impericia o ignorancia inexcusable en las atribuciones de los funcionarios o empleados.

Sanción de 2 a 4 años de prisión.

Estas penalidades son aplicables a los miembros de la entidad, si se prueba el conocimiento de la violación, si se ha actuado con negligencia, impericia, ignorancia inexcusable o ceguera intencional en las atribuciones.

El incumplimiento de las leyes y regulaciones resultará en severas penalidades para empleados y la entidad.

- Largas sentencias en la cárcel por cada ofensa.
- Multas hasta de 2,500 salarios mínimos mensuales.

VIII. POLÍTICAS PARA PREVENCIÓN DE LAVADO DE DINERO.

GENERALES

- Las políticas son las regulaciones operativas y reglas internas de la entidad que definen como deben proceder sus empleados y que permitan a los funcionarios adoptar las decisiones para prevenir los delitos de LD/FT en la empresa.
- Es política de la entidad, cumplir con las disposiciones legales emanadas por los organismos reguladores y de control, así como cumplir con el manual de controles internos para prevenir LD/FT proveniente de actividades ilícitas.
- El presente manual y las políticas, bien administrados no interferirá en la relación de la entidad con sus buenos clientes.
- El desconocimiento de las políticas y procedimientos de la entidad que han recibido normal difusión, no será justificación frente a las consecuencias de inobservancia.
- Por lo menos una vez cada doce meses se realizará la toma de pruebas del manual y de las políticas y/o procedimientos, a los funcionarios y empleados que tengan relación con las áreas involucradas en la operación y administración del negocio y sus controles, la prueba podría ser escrita o verbal.
- El auditor interno está en la obligación de verificar el cumplimiento de las presentes políticas y manuales relacionados a la PLD/FT.
- Mantener actualizados los datos y más información de sus clientes de acuerdo a las disposiciones del ente regulador cuando así corresponda, mediante la suscripción del perfil de datos firmados por cada cliente, como también actualizará en forma periódica los procedimientos y controles respecto a la prevención de LD/FT, de acuerdo a lo que dispongan los organismos de control Vigentes y organismos internos de la entidad.

- Es política de la entidad, si un cliente se rehúsa a entregar la información requerida, la relación no será establecida, así mismo si los documentos que el cliente quedó a entregar a futuro no son presentados, cualquier relación ya establecida deberá terminarse.
- El cumplimiento de las normas y procedimientos del presente manual, exige la colaboración de todas las unidades de la entidad, así como también de sus autoridades, funcionarios y empleados, haciéndose corresponsables de los procesos de trabajo y control que se vean afectados por las políticas y procedimientos descritos en el presente documento.
- Para los efectos del apartado anterior, todos los miembros de la entidad, observarán lo previsto en las disposiciones vigentes en la materia y lo contemplado en el presente manual.
- Las políticas específicas que contribuirán en la prevención de lavado de dinero y financiamiento al terrorismo serán las siguientes:
 1. Política conozca a su cliente.
 2. Política conozca a su empleado.
 3. Política de capacitación al personal.
 4. Política de reporte de transacciones inusuales y/o sospechosas.
 5. Política de prevención contra el financiamiento al terrorismo. Podrán adicionarse políticas de acuerdo a los requerimientos de nuestra legislación referente a la PLD/FT y/o a los resultados de las evaluaciones de riesgo que se realicen en el futuro.

1. POLITICAS CONOZCA A SU CLIENTE.

- **Políticas generales**

El conocimiento del cliente se constituye en la herramienta fundamental para prevenir el desarrollo de transacciones u operaciones ilícitas dentro de los procesos de la entidad, fortaleciendo la necesidad de generar negocios con responsabilidad.

Se considera una obligación de todos los funcionarios y empleados el conocer a sus clientes, considerando que, esto supone una relación permanente que permita acceder a las actividades que realiza, sus negocios y el entorno en que se desenvuelve.

Para conocer al cliente, se estiman cuatro aspectos muy importantes:

1. La información proporcionada por el cliente al momento de la vinculación,
2. La verificación de información de vinculación,
3. La actualización de información proporcionada por el cliente,

4. La información transaccional del cliente y su monitoreo.

En los tres primeros aspectos, la responsabilidad principal de controlar esta política recae en el área de servicios al cliente con los agentes autorizados, quienes son los que van a mantener el primer contacto con el cliente de la empresa, para empezar una relación comercial, en los diferentes servicios ofrecidos por la empresa. Lo anterior, no exime de responsabilidad al resto de los funcionarios de la organización, que al entablar relaciones con sus clientes, orienten a estos sobre su actualización de datos para fortalecer el trabajo del área de servicios al cliente.

Durante el aspecto número cuatro, la responsabilidad principal, recae en el Oficial de Cumplimiento, el cual verifica que la información transaccional sea conforme a la información de vinculación del cliente. Al igual que en el punto anterior, este aspecto, no exime de responsabilidad al resto de los funcionarios de la entidad de las diferentes áreas, que al entablar relaciones con sus clientes, identifiquen que su transaccionalidad, no corresponde a su información de vinculación e informarán al Oficial de Cumplimiento.

Se entiende como clientes a las personas que acceden a los servicios que ofrece la entidad, y que suscriben contratos por algún servicio y por lo tanto se convierten en clientes de la entidad y acceden a los beneficios que esto conlleva.

Para efectos de la prevención y control de LD/FT, el cliente está sujeto a cumplir con lo establecido en la legislación aplicable, someterse a análisis de monitoreo constante y más aún, cuando se detecten movimientos inusuales que serán reportados a los organismos de control pertinentes.

La política de conocimiento del cliente, considera los siguientes aspectos:

- Identificar al cliente, lo que implica el conocimiento y verificación de todos los datos de la persona natural o jurídica con la que se iniciará la relación contractual.
- Conocer el volumen de los negocios del cliente o cualquier otra actividad económica a la que se dedican;
- Características, montos de transferencia de ingreso y egreso;
- Respecto de los clientes, la empresa establecerá un control sobre el perfil de su información considerando las características y montos de sus operaciones; así como la actualización periódica de información.
- Actualización anual de la información de los clientes y cuando el Oficial de Cumplimiento considere conveniente en función del riesgo de algún cliente observado.

- Para el monitoreo permanentemente de las operaciones de los clientes, los agentes autorizados, supervisores, en coordinación con el Oficial de Cumplimiento, analizarán:
 - ✓ El perfil transaccional del cliente;
 - ✓ Confirmar que el volumen y movimiento de dinero electrónico que realizan, guarde relación directa con la actividad y capacidad económica de los mismos;
- Informar al Oficial de Cumplimiento de cualquier relación inusual observada del cliente con respecto a su información, verificación de información, actualización de información o relación de negocios;

Los aspectos antes citados, consideran políticas generales de obligatorio cumplimiento por parte de los miembros de la entidad, así como políticas específicas.

Dentro de las políticas generales de **debida diligencia o conozca a su cliente**, se tienen:

1. La entidad, no mantendrá cuentas anónimas, cuentas cifradas o cuentas bajo nombres ficticios ni suscribirá contratos con nombres falsos o de cualquier otra modalidad que encubra la identidad real del titular.
2. La entidad, establecerá procedimientos para la debida identificación y verificación de la identidad de los clientes, tanto internos como externos según las políticas establecidas en el presente manual.
3. La entidad, evitará establecer relaciones comerciales con empresas o sociedades constituidas en el extranjero al amparo de una legislación que permita o favorezca el anonimato de los verdaderos dueños, accionistas o administradores, incluyendo en esta categoría a las sociedades anónimas cuyas acciones sean emitidas al portador.
4. La entidad evitará relacionarse con clientes, cuya fuente de riqueza provenga de actividades reconocidas como susceptibles al lavado de activos.
5. La entidad evitará relacionarse o realizar operaciones que de alguna forma se presuman están relacionadas con el terrorismo u organizaciones que ayudan o respalden el terrorismo.

Cuando el Oficial de Cumplimiento determine, reforzar el proceso de debida diligencia, deberá realizarse en un plazo no mayor a ocho días, realizando un informe del caso soportando las acciones tomadas. La Oficialía de Cumplimiento, definirá las acciones a seguir sobre la continuación de operaciones con el cliente, la finalización de operaciones y/o el reporte a la Unidad de Investigación Financiera si así amerita el caso.

En consideración a políticas específicas de debida diligencia se tiene inicialmente que cumplir con la obligación de identificar adecuadamente al cliente; la entidad, establece los requisitos de información que se deben obtener de los clientes naturales y jurídicos al momento de vincularlos, verificar sus datos y actualizar su información.

La información a solicitar a las personas naturales y jurídicas, se halla en el sistema informático y la misma se resume en la siguiente información:

- **Para personas naturales:**
 - ✓ Nombre completo.
 - ✓ Tipo y Número de Documento de Identidad.
 - ✓ Lugar y fecha de expedición.
 - ✓ Tipo y número de un segundo documento de identidad (NIT, si cuenta con uno).
 - ✓ Sexo.
 - ✓ Departamento y Municipio de residencia.
 - ✓ País de residencia.
 - ✓ Fecha de caducidad.
 - ✓ Lugar y fecha de nacimiento.
 - ✓ Nacionalidad.
 - ✓ Domicilio según documento de identidad.
 - ✓ Domicilio actual.
 - ✓ Estado civil.
 - ✓ Nombre del cónyuge (si aplica o sea si esta descrito en el documento de identidad).
 - ✓ Números telefónicos casa, celular.
 - ✓ Profesión, (según documento de identidad).
 - ✓ Ocupación actual.

- **Para personas jurídicas:**
 - ✓ Razón social.
 - ✓ Escritura de Constitución.
 - ✓ Número de Identificación Tributaria.
 - ✓ Número de Registro de Contribuyente.
 - ✓ Nómina de Accionistas.
 - ✓ Miembros de Junta Directiva.

- ✓ Datos personales del Representante Legal o Apoderado.
- ✓ DUI y NIT del Representante Legal o Apoderado.
- ✓ Credencial de Representante Legal o poder en caso de Apoderado.

- **Políticas Específicas**

- **Procedimiento de verificación de información**

La información de parte de los clientes de la entidad, es verificada por el agente autorizado, desarrollando el mecanismo siguiente:

- 1) El agente autorizado, utilizará como medio de verificación fehaciente los datos básicos del cliente, los registrados en su Documento Único de Identidad al ser un documento legal de identificación personal emitido por autoridades competentes. Asimismo, la verificación del domicilio de sus clientes se realizará a través de la presentación de un segundo documento de identidad, donde conste la dirección declarada por la persona al momento de ser registrado como cliente o un recibo de agua, teléfono o energía eléctrica, si no cuenta con el documento se consultará al cliente de forma verbal.
- 2) Por otro lado, cuando se trate de clientes que declaren origen de fondos independientes por actividades privadas informales, el agente autorizado, analizará si en función al monto, deba o no realizar una investigación adicional de verificación de la información, para comprobar la fuente de recursos.
- 3) Por cada investigación adicional realizada para la verificación de la información, se deberá establecer un informe básico de comprobación de datos de los resultados obtenidos, adjuntando los documentos de respaldo necesarios en el archivo del cliente
- 4) Es importante señalar que el procedimiento antes descrito se aplican de manera independiente y en coordinación con el supervisor de zona.

- **Debida diligencia para Personas Políticamente Expuestas (PEP's)**

Las políticas de debida diligencia para Personas Políticamente Expuestas, consideran una clasificación especial de clientes categorizados como PEP: Jefes de Estado o de un Gobierno, políticos de alta jerarquía, funcionarios gubernamentales, judiciales o militares de alta jerarquía, altos ejecutivos de empresas estatales, dirigentes de partidos políticos, así como su cónyuge y sus parientes dentro del tercer grado de consanguinidad o segundo de afinidad.

Para este tipo de clientes, la política de debida diligencia reforzada de la entidad, considera:

- a) Al momento de la vinculación, cuando un cliente, es encontrado en la base de datos de PEP's o declara por sí mismo ser una persona PEP según la definición y alcance establecido en el presente manual, deberá entonces, procederse a completar un formulario especial de registro de cliente y declaración de origen lícito de recursos.
- b) Todo inicio o continuación de alguna relación con un PEP's debe contener por escrito la autorización del Oficial de Cumplimiento.
- c) Para estos casos, se realizará el seguimiento de manera semestral, analizando el comportamiento transaccional, al perfil del/la cliente y a la actividad del/la cliente.
- d) Un informe de la verificación de información, deberá ser incorporado al archivo del cliente PEP y una copia enviada al Oficial de Cumplimiento.
- e) Clasificación del cliente en una base de datos de clientes de alto riesgo.
- f) El monitoreo transaccional semestral del cliente es obligatorio.
- g) Ponderación de riesgo en el perfil de clientes superior a los de un cliente natural o jurídico no categorizado como PEP.
- h) El Oficial de Cumplimiento, realizará el seguimiento a la base de PEP's y de su comportamiento e informará en su reporte semestral a Junta Directiva sobre la situación actual.
- i) La clasificación de la persona como PEP, no podrá ser modificada, inclusive después de haber cesado en las funciones que desempeñaba, hasta que la UIF se pronuncie al respecto.
- j) La Oficialía de Cumplimiento llevará un archivo correspondiente a cada cliente PEP que haya contratado una relación comercial. Esta información será alimentada por datos del cliente físicos, transaccionales, registros externos y de internet. Asimismo, la Oficialía de Cumplimiento controlará estos archivos de forma confidencial, reportando los mismos cuando la ley o un organismo de control se lo solicite.

- **Aceptación del Cliente**

ElectroniCash sólo establece relaciones comerciales con personas naturales que cumplan lo establecido en los requerimientos de información del presente manual. Asimismo, en ningún caso acepta como clientes a:

- Personas o empresas de honestidad cuestionable, especialmente de quienes se tenga conocimiento de su vinculación con el narcotráfico, lavado de activos, terrorismo o crimen organizado;
- Personas o empresas que no entreguen la documentación de identificación requerida por la entidad;
- Empresas no domiciliadas en el país o personas involucradas en la constitución de dichas empresas, que se encuentren registradas en listados internacionales (verificados en listados OFAC);
- Operaciones con nombres ficticios, anónimos, seudónimos o cifradas en vez del nombre verdadero del/la cliente;
- Salas de juego, tragamonedas y afines; en casos especiales de excepción deberán contar obligatoriamente con la aprobación del Oficial de Cumplimiento;
- Personas relacionados con la comercialización de armas.

○ **Actualización de información proporcionada por el cliente.**

La actualización de información de los clientes, se constituye en una política indispensable para administrar adecuadamente los perfiles de riesgo de los clientes, las matrices y en consecuencia la gestión eficiente del riesgo de lavado de dinero y activos y financiamiento del terrorismo.

Las políticas principales para mantener actualizada la información en la entidad, son las siguientes:

- Los agentes autorizados, son los encargados de mantener la base de datos actualizada, por lo cual, semestralmente el sistema, dará un aviso de clientes con antigüedad de registro igual o mayor a seis meses.
- El supervisor de zona, deberá realizar una visita de campo por requerimiento especial del Oficial de Cumplimiento, con el fin de actualizar los datos de clientes que por su forma de operar o el volumen de operaciones así lo requieran.
- Para dar cumplimiento a la actualización, la Oficialía de cumplimiento creará una alerta, para que en el momento de la realización de cualquier transacción a cargo del cliente con información no actualizada en el período de seis meses, y así, determinar todos aquellos clientes que no fueron actualizados en su momento por el agente autorizado.

Los aspectos anteriores, no limitan la observancia de cualquier funcionario o del Oficial de Cumplimiento o de supervisores que en el proceder de sus actividades, identifiquen clientes no actualizados, solicitando al área de agentes autorizados su actualización con un plazo justificado de presentación de resultados.

- **Monitoreo transaccional del Cliente**

El monitoreo de las transacciones y operaciones realizadas por los clientes es una de las tareas fundamentales de la entidad, en el entendido de poder verificar que la información de vinculación concuerda con el comportamiento transaccional del cliente.

Para el cumplimiento adecuado de esta tan importante labor, la entidad ha establecido un modelo de gestión que considera las siguientes políticas:

- 1) Monitoreo diario en función a señales de alerta establecidos en el sistema de prevención de lavado de dinero de la entidad, definidos los mismos en función a:
 - ✓ Cantidad de operaciones, superior a las registradas en el perfil de cliente.
 - ✓ Frecuencia de operaciones, superior a las registradas en el perfil de cliente.
 - ✓ Frecuencia de operaciones, con un solo servicio.
 - ✓ Operaciones que no concuerden con la actividad económica del cliente
 - ✓ Otros que estime pertinente el Oficial de Cumplimiento.
- 2) Monitoreo diario en función al análisis de operaciones inusuales arrojadas por el sistema.
- 3) Monitoreo mensual del comportamiento de clientes internos (empleados) en función a operaciones con servicios varios prestados por el negocio.
- 4) Monitoreo mensual en función al comportamiento del segmento de clientes según niveles de riesgo.

Las políticas de monitoreo no estarían nunca completas si las mismas no contaran con el análisis de parte del Oficial de Cumplimiento y de las áreas operativas y de negocios que respaldan las mismas. Para este cometido, el Oficial de Cumplimiento establece la correspondencia de transacciones con el perfil de riesgo presentado en el sistema de prevención de lavado de dinero de la entidad, verificando la calificación de riesgo de su matriz. Sus observaciones deben ser justificadas a través de la solicitud de información a los funcionarios que atienden a los clientes, los cuales deberán informar en el plazo de 48 horas la justificación que generó las variaciones en su perfil y presentar los documentos relacionados (si existiere justificación).

2. POLÍTICAS CONOZCA A SU EMPLEADO.

En materia de prevención de lavado de activos y financiamiento al terrorismo, el conocimiento de los empleados que trabajan dentro de la entidad tiene una importancia vital debido a que se espera prevenir un comportamiento que comprometa a la organización, o que provoque el pago de multas/sanciones, o que sea participe directo o indirecto de actos ilícitos individuales o colectivos dentro o fuera de la empresa. En tal sentido, en ElectroniCash, se han adoptado una serie de medidas tendientes a lograr un conocimiento adecuado de los empleados buscando integridad ética y moral del personal, así como la adhesión a los valores institucionales.

Los aspectos generales que hacen a la política conozca a su empleado son:

- ✓ Es deber y responsabilidad de todos los empleados desarrollar sus labores con total honestidad, competencia y alta moral profesional, además de conocer y aplicar a cabalidad lo estipulado en el reglamento interno de trabajo, código de conducta, manual de prevención de LD/FT y demás normas que se expidan en su momento.
- ✓ Es deber y responsabilidad de todos los empleados desarrollar sus labores con total honestidad, competencia y alta moral profesional, además de conocer y aplicar a cabalidad lo estipulado en el código de conducta, manual de prevención de riesgos y demás normas que se expidan en su momento.
- ✓ Es responsabilidad de la administración estar alerta sobre operaciones o transacciones inusuales realizadas por empleados de la entidad, con el fin de precautelar los intereses de todas las personas que trabajan en esta.

Para el cumplimiento de los aspectos antes señalados, el área de Recursos Humanos, adoptará las medidas de prevención más apropiadas para asegurar la integridad de sus empleados, para ello se han definido tres políticas específicas:

- Selección, competencia profesional y contratación del personal.
- Actualización de datos y características del entorno residencial.
- Monitoreo de transacciones.

A continuación se describen cada una de ellas:

- **Políticas de selección de personal**

Cuando se trata de selección de personal, el departamento de Recursos Humanos seleccionará a los aspirantes más idóneos para ocupar las vacantes que se produzcan, dando especial importancia al recurso humano ya existente al interior de la entidad.

Las personas seleccionadas a ingresar a la entidad, deberán entregar como mínimo la siguiente información:

- Currículo Vitae actualizado.
- 1 fotografía reciente.
- Fotocopia de Documento de Identidad vigente. (DUI, Pasaporte o Carnet de Residente).
- Fotocopia de Tarjeta de Número de Identificación Tributaria (NIT).
- Fotocopia de tarjeta del Seguro Social, o en su defecto verificación de número en el ISSS.
- Fotocopia de tarjeta de AFP.
- Fotocopia del último Título académico obtenido, certificado por el Ministerio de Educación.
- Fotocopia de certificado de notas en caso de estudiantes universitarios.
- Fotocopia de certificados de seminarios y cursos asistidos, si los hubiere.
- Fotocopia de constancia del último trabajo, si lo hubiere solvencia otorgado por la Policía Nacional Civil.
- Certificación de Antecedentes Penales.
- Solicitud de empleo, (formato ElectroniCash).
- Antes de vincular al postulante deberá de realizar una prueba poligráfica. Los empleados extranjeros, deberán de tramitar su permiso de trabajo otorgados por el Ministerio de Trabajo (sección de trabajadores migrantes).

En caso de postulantes a plazas temporales, pasantías o servicios profesionales, será lo siguiente:

- Currículo Vitae actualizado.
- Fotocopia de Documento Único de Identidad vigente. (DUI, Pasaporte o Carnet de Residente).
- Fotocopia de tarjeta de Número de Identificación Tributaria (NIT).
- Fotocopia y original de referencias laborales y/o personales.
- Solicitud de empleo, (formato ElectroniCash para empleados eventuales).
- Los empleados extranjeros, deberán de tramitar su permiso de trabajo otorgados por El Ministerio de Trabajo (sección de trabajadores migrantes).

Es responsabilidad del departamento de Recursos Humanos, requerir, revisar y validar la documentación del postulante (para el caso de las plazas temporales evaluar si la información es suficiente de acuerdo al grado de riesgo que conlleve el puesto de trabajo), al momento que este se vincule. Asimismo, en el caso de presentarse alguna observación inusual posiblemente vinculada a alguna intención fraudulenta, deberá reportar a la Gerencia General y al Oficial de Cumplimiento dichos hechos.

Es también responsabilidad del departamento de Recursos Humanos crear un expediente físico por cada empleado con la documentación suministrada al inicio de la relación laboral y las demás actualizaciones que se realicen. En este proceso también, se realizará una verificación fehaciente del domicilio del postulante, previa firma del contrato de trabajo. Esta verificación se realizará con el documento de algún servicio público y/o verificación vía telefónica.

Ahora bien, una vez que el nuevo funcionario se ha incorporado a la entidad, recibirá un proceso de inducción coordinado por el departamento de Recursos Humanos, que contemplará como mínimo temas referentes a la prevención del lavado de activos y financiamiento al terrorismo. Asimismo, se le hará entrega del código de conducta, el reglamento interno de la entidad y el manual de prevención de lavado de dinero y financiamiento al terrorismo, siendo los mismos de obligatorio cumplimiento y su lectura igual.

- **Políticas de actualización de datos**

La actualización de información por parte de los empleados de la entidad, se realizará obligatoriamente una al año a través de los formularios diseñados para el efecto por el departamento de Recursos Humanos. El departamento de Recursos Humanos, estará a cargo de dicha labor y el Oficial de Cumplimiento, verificará el cumplimiento de la presente disposición. Los formularios de actualización serán parte del archivo de cada funcionario.

Por su parte, es responsabilidad de los funcionarios informar sobre cambios importantes en su información personal como ejemplo, cambios en su domicilio o estado civil, así mismo el área de Recursos Humanos deberá establecer los procedimientos necesarios para mantener actualizada la base de datos de los empleados y personal contratado.

Como medida de control, el Oficial de Cumplimiento, podrá verificar aleatoriamente y en cualquier momento y sin previo aviso, el expediente de los empleados. Asimismo, si como resultado de aquella actividad evidenciare actividades inusuales por parte del empleado, se solicitará al jefe inmediato del funcionario su justificación en los siguientes 15 días hábiles. Pasado el tiempo estipulado, si no se ha aclarado la actividad inusual, el Oficial de Cumplimiento emitirá un informe y reporte para su respectivo

tratamiento por la administración de la entidad. Semestralmente, el Oficial de Cumplimiento realizará una verificación de la información de los empleados de la entidad a fin de verificar que sea actual y este de acuerdo con su actividad laboral.

Los documentos de los empleados y su información en general contenida en cada expediente se considerara como información restringida; por lo tanto, se establecerán los controles correspondientes alrededor de la misma, manteniendo la confidencialidad del caso.

- **Políticas de monitoreo de transacciones**

La Oficialía de Cumplimiento monitoreará periódicamente las transacciones realizadas por todos los empleados de la entidad que ocurran dentro de la misma, (no así sobre las transacciones en cualquier institución financiera donde reciben su salario), especialmente de aquellos relacionados con puestos de alto riesgo o que dentro de sus funciones mantengan los siguientes: encargados de la plataforma electrónica, otorgación de cuentas a los clientes, relación con proveedores, etc.

El Oficial de Cumplimiento podrá realizar monitoreo de operaciones de los miembros de todas las gerencias y jefaturas de la entidad.

El Oficial de Cumplimiento, no considerará procesos reducidos o diferenciados de control para los miembros de las gerencias o jefaturas de la entidad.

Finalmente, es importante considerar que el monitoreo también considera la verificación de señales de alerta tales como:

- ✓ Variación en el nivel de vida.
- ✓ Estilos de vida o posibilidades financieras que no corresponden con el nivel salarial, de ingresos o patrimonial.
- ✓ Renuencia a salir de vacaciones.
- ✓ Recepción de regalos o atenciones de clientes que excedan la práctica habitual.
- ✓ Asesorar o cumplir funciones en otra entidad, sin previa autorización de la Gerencia General.
- ✓ Permanecer dentro de las instalaciones de la entidad fuera de los horarios de trabajo sin justificación alguna.

Cuando exista una sospecha por parte del supervisor acerca de la conducta de uno o varios de sus supervisados, sobre los puntos antes descritos, deberá poner en conocimiento inmediato de la Gerencia General y del Oficial de Cumplimiento.

- **Sanciones para empleados y proceso de imposición.**

Se deja establecido que la inobservancia de las políticas del presente manual, ya sea por negligencia o desconocimiento de las mismas, puede generar pérdidas a la entidad, razón por la cual, todo empleado que incumpla con las disposiciones emitidas en este manual será objeto de las sanciones que la Oficialía de Cumplimiento le imponga, independientemente del proceso administrativo correspondiente, de acuerdo a lo previsto en las políticas establecidas por la entidad para el caso. Asimismo, estas se describen en el presente manual en el apartado de sanciones y correctivos.

Es responsabilidad del departamento de Recursos Humanos, a solicitud de la Oficialía de Cumplimiento, elaborar un reporte trimestral sobre los actos por operaciones internas realizadas por empleados, que generen preocupación a la entidad y que por este acto hayan sido separados de sus puestos.

3. POLÍTICAS DE CAPACITACIÓN AL PERSONAL.

ElectroniCash, es consciente que una entidad que no instruye a su personal, es una entidad susceptible a cometer errores involuntarios y ser usada como vehículo para actividades delictivas. En tal sentido, considera lo estipulado en la regulación vigente en vista de mantener un plan anual de capacitación para el personal, inducción sobre el tema a todo el personal de nuevo ingreso, así como instrucción específica para el Oficial de Cumplimiento, supervisores y agentes autorizados y todo el equipo que deben acreditarse ante los organismos de control (UIF). En vista de lo anterior, se han definido las siguientes políticas:

- El Oficial de Cumplimiento en coordinación con el encargado de Recursos Humanos, elaborarán un plan anual de capacitación de carácter obligatorio para todos los funcionarios de la entidad.
- El contenido del plan será diferenciado por niveles y responsabilidades, en función a la realidad del entorno, tendencias y solicitudes de los organismos de control.
- El plan anual de instrucción presentará una evaluación obligatoria para todos los funcionarios, siendo la misma parte de su evaluación anual de Recursos Humanos.
- Es responsabilidad del Oficial de Cumplimiento, impartir el plan de instrucción o buscar medios alternativos que lo reemplacen, como la exposición de un consultor de alto nivel, la instrucción a

cargo de alguna autoridad de alto nivel de la UIF o la contratación de un sistema de instrucción virtual.

- Es de exclusiva responsabilidad del Oficial de Cumplimiento informar a los organismos de control si lo requieren, sobre el desarrollo del plan de capacitación en materia de lavado de dinero y activos que se realicen dentro de la entidad, el mismo que será debidamente documentado.
- El contenido de instrucción de los planes de capacitación deberán tomar en cuenta mínimamente: las políticas conozca a su cliente, conoce a tu empleado, las disposiciones legales vigentes y los procesos de control actuales, buscando los siguientes resultados:
 - Generar en toda la entidad una real conciencia del riesgo de lavado de dinero y activos y financiamiento al terrorismo y la necesidad de actuar dentro del marco de una “Cultura de Prevención”.
 - Mejorar el conocimiento por parte de los/as trabajadores/as de la entidad en la prevención de lavado de dinero.
 - Acercar a la Oficialía de Cumplimiento con las distintas áreas de negocios de la empresa.
 - Lograr que el personal del contacto de la entidad con la UIF cuente con el conocimiento adecuado en materia de prevención de lavado de dinero.
 - Comprender que conozca a su cliente es la forma más adecuada de hacer negocios para la entidad, poniendo a salvo su reputación.
 - Transmitir el hecho de que todo/a trabajador/a que tiene contacto con clientes es responsable primario de identificar y conocer a sus clientes.
 - Incorporar técnicas y procedimientos que permitan conocer a los clientes.
 - Conocer las normas internas de la entidad.
 - Conocer la problemática internacional.
 - Conocer conceptos básicos de los principales documentos emitidos por los organismos internacionales.
- Todas las capacitaciones de inducción como manuales, incluirán un material específico sobre nociones básicas en prevención de lavado de dinero y de activos y financiamiento al terrorismo.
- En las capacitaciones impartidas al personal de la entidad se utilizarán las mejores herramientas e información disponible para transmitir de una manera adecuada las capacitaciones.

- Las evaluaciones sobre la instrucción impartida se podrán desarrollar al final de cada capacitación o después de realizadas todas las capacitaciones. Estas podrán ser de modalidad escrita, casos, orales o de selección múltiple.
- Los resultados de la instrucción y las evaluaciones serán de conocimiento del Gerente General, encargado de Recursos Humanos y el Oficial de Cumplimiento.
- Aquellos funcionarios que hayan reprobado la evaluación, deberán solicitar una nueva fecha para rendir otro examen, sin embargo, el antecedente quedará registrado en sus expedientes personales con una llamada de atención por el no aprovechamiento del curso de capacitación.

Por otra parte, la entidad, considera muy importante la instrucción coordinada del Oficial de Cumplimiento y Recursos Humanos al momento de inducción de nuevo personal. La entidad, reconoce que el Oficial de Cumplimiento y su equipo requieren de una instrucción continua, por lo cual programará en su presupuesto la participación de los mismos ya sea en programas de capacitación locales o internacionales que justifiquen su inversión.

POLÍTICA DE REPORTE DE TRANSACCIONES INUSUALES Y SOSPECHOSAS.

Es importante de manera inicial, diferenciar entre operación o transacción inusual y transacción sospechosa.

La transacción inusual es aquella cuyas características, cuantía o frecuencia, no guarda relación con el perfil registrado del cliente ni con la transaccionalidad del mismo.

La transacción sospechosa, es aquella que después de haber levantado todos los argumentos necesarios para buscar y justificar la transacción inusual, esto no ha sido posible y el Oficial de Cumplimiento no encuentra argumento lógico y válido sobre la discrepancia, convirtiéndose la operación de inusual a sospechosa y entonces corresponde su reporte a la Unidad de Investigación Financiera.

- **Políticas para el reporte de transacciones inusuales.**
 - Es obligación de todo el personal de la entidad, identificar las transacciones que aparenten ser inusuales en los movimientos cotidianos que realizan los clientes, ya sean estos internos o externos, poniendo en conocimiento de la Oficialía de Cumplimiento, lo antes posible.
 - Es obligación de todo el personal de la entidad, conocer las señales de alerta que se presentan en el manual de prevención, a fin de tener conocimiento de ciertas actividades atípicas en nuestro tipo de negocio y clientes.

- Cuando un agente autorizado ha identificado una operación inusual, se alimentará de la información que sustenta la operación inusual y reportará durante el mismo día de manera directa al supervisor. Anexando formato de reporte de operación sospechosa (ROS-01).
- El supervisor, habiendo recibido la señal de alerta, iniciará de inmediato su correspondiente análisis para buscar justificar la transacción inusual. Este análisis no debería demorar más de tres días hasta su informe. Durante este tiempo, el funcionario que realizó el reporte, deberá mantener un monitoreo cauteloso al cliente identificado, si es que este continua operando con la entidad.
- Una vez finalizado el informe, se remite al Oficial de Cumplimiento, para que este junto con los miembros Junta Directiva analicen si la transacción es justificable (o no sospechosa), entonces comunicará al funcionario que reportó la operación para bajar la tensión, pero no dejar de controlar.
- Independientemente del resultado del análisis, el Oficial de Cumplimiento deberá dejar evidencia de todo el proceso, para luego reportar de forma estadística a la Junta Directiva, del trabajo desarrollado. Si el informe no justifica la transacción, se deberá reportar la operación inusual ahora como sospechosa a la Unidad de Investigación Financiera.
- Cuando la operación inusual haya sucedido en alguna oficina administrativa de la entidad, el tratamiento es exactamente el mismo, aplicando las sanciones administrativas pertinentes si fuere el caso.
- Todo el proceso de análisis interno y la relación de información y soporte del informe del Oficial de cumplimiento, así como la comunicación con el agente autorizado que reportó, deberá mantenerse con estricta confidencialidad y no revelar datos a nadie y menos en la propia entidad.
- **Políticas para el reporte de transacciones sospechosas.**
 - Es obligación del Oficial de Cumplimiento, analizar y buscar justificar todas las operaciones inusuales y señales de alerta que se identifiquen en la entidad en las diferentes áreas.
 - El análisis del Oficial deberá considerar lograr la mayor cantidad de información necesaria para respaldar el trabajo seguido, tanto para justificar como para dotar de instrumentos de decisión que avalen su reporte.
 - Cuando el Oficial haya definido que la operación inusual no tiene argumento alguno y dado el proceso de análisis, la considere ahora sospechosa, deberá reportar la misma vinculada a lavado de dinero a la UIF en un plazo no mayor a tres días, utilizando el Formulario

respectivo, ya sea este manual o electrónico, así como toda la información y documentación que respalde el reporte.

El reporte de operación sospechosa, debe ir lo suficientemente respaldado a la UIF a fin que esta última entidad no vuelva a requerir mayor información que la presentada, apoyando la gestión de la autoridad y ganado tiempo para la institución.

Después de realizado el reporte ROS a la UIF, ElectroniCash podrá seguir manteniendo relaciones comerciales con el cliente y dará seguimiento de las operaciones del/la cliente, a objeto de que se continúe proporcionando información que pueda requerir la UIF o la que la entidad considere necesaria proporcionar, aun sin previo requerimiento de la UIF. En todas estas actuaciones, la entidad mediante el Oficial de Cumplimiento o el agente autorizado, mantiene en reserva cualquier información hacia el cliente, con relación al reporte de la operación sospechosa u otra situación que permita al cliente tomar conocimiento de este hecho. Si después del reporte a la UIF por segunda vez el mismo cliente actúa de manera sospechosa, el Oficial de Cumplimiento, deberá considerar el mantener la misma posición frente a un riesgo peligroso para la entidad, entonces, enviará a los miembros de Junta Directiva con carácter especial sus consideraciones a fin que los dueños de la entidad decidan la terminación de la relación con el cliente.

ELECTRONICASH, S.A.

PERIODO:

PROGRAMA PREVENCIÓN DE LAVADO DE DINERO Y ACTIVOS

ANEXO 7

Objetivo:

conocer si la entidad cuenta con los parámetros mínimos que establece la leyes y reglamentos en materia de prevención de lavado de dinero y activos, además de asegurarnos que cumplen con la debida diligencia, que es un factor clave para salvaguardar la imagen y posibles litigios de la entidad.

N°	Procedimiento	Referencia	Hecho por	Fecha	Comentario
1	Compruebe que la entidad ha identificado a todos sus clientes, sean estas personas naturales o jurídicas en cuyo nombre se mantiene una cuenta dentro de la compañía.				
2	Compruebe que la Junta General de Accionistas ha elegido al oficial de cumplimiento y aprobado su respectivo plan de trabajo.				
3	Verificar si la entidad cuenta con un expediente donde se determine la información referente a los clientes que posee, o si posee manuales o medidas concretas para identificar y conocer a sus clientes. La información mínima que debe tener el expediente es: a) Información general b) Número de Identificación Personal c) Actividad económica.				
4	Compruebe si la compañía posee clientes calificados con alto riesgo, de ser positivo, confirmar si se posee una lista donde se incluya la fecha en que fueron incorporados a esta y toda aquella información referente al porque es catalogado como alto riesgo. Todo debe estar debidamente documentado.				
5	Verificar que la entidad posea políticas o procedimientos para la actualización de los datos de los clientes.				
6	Indagar y dar seguimiento a las transacciones realizadas por los clientes calificados con alto riesgo y determinar si se presentan operaciones inusuales.				
7	Verifique que si la entidad realiza bitácoras de las transacciones realizadas con los clientes y que éstas no puedan ser modificadas por los funcionarios.				
8	Comprobar si la entidad posee procedimientos para la identificación de transacciones inusuales, transacciones de cliente que es imposible comprobar sus ingresos.				
9	Con la lista de los clientes proporcionada por la entidad seleccionar aquellos que realizan mayor número de transacciones o con montos elevados y facilitar un cuestionario a alguno de los clientes para verificar toda la información referente a su giro comercial, entorno empresarial, etc., luego comparar el resultado con los datos del cliente que posee la entidad para determinar si concuerda la información.				
10	Asegurarse que el oficial de cumplimiento tenga la debida independencia dentro de la compañía para que pueda desarrollar su cargo como es debido.				

 <p>ElectroniCash</p>	Formulario de identificación de PEP's
Nombre Completo del cliente:	
Cargo público que desempeña:	
Fecha de nombramiento:	
Periodo de nombramiento:	
Marque la opción según corresponda: Funcionario público <input type="checkbox"/> Persona relacionada/vinculada con un PEP <input type="checkbox"/>	
Para persona relacionada describa la relación con el PEP: Relación familiar Relación empresarial	
Nombres completos de sus parientes en primer grado y segundo grado de consanguinidad y afinidad compañero de vida y asociados comerciales o de negocio: 1. _____ 2. _____ 3. _____ 4. _____	
Razón social de las sociedades con las que el PEP tiene relación patrimonial (25% o más del capital accionario o participación en el patrimonio): 1. _____ 2. _____ 3. _____	
PARA USO EXCLUSIVO DE LA INSTITUCIÓN Declaro bajo juramento que la información anteriormente expuesta es el reflejo fiel de la verdad. Manifiesto que tengo conocimiento que incurriré en sanciones administrativas y penales en caso de incumplirlas normas y leyes establecidas en la Ley contra el lavado de dinero y de activos deactivos.	



ANEXO 9.

Declaración Jurada de Clientes y Personas Expuestas Políticamente

Fecha: _____ de _____ del año _____ Hora: _____

Transacción correspondiente No.: _____

Yo _____, con DUI número _____, número de NIT _____ y NRC _____ cliente de ElectroniCash S.A., declaro bajo juramento que no tengo vínculo alguno con actividades ilícitas, actividades del narcotráfico y otros delitos tipificados en la Ley contra el lavado de dinero y de activos.

A la vez, manifiesto que la/as transferencia/as de efectivo que envío provienen de fuentes honradas y lícitas; por lo tanto el dinero transferido _____ es de mi total propiedad y deseo sea enviada al destinatario que indique.

Afirmo que conozco las normas y leyes del país y que cualquier acto consciente e inconsciente que se realice en contravención a la Ley, estaré supeditado(a) a las sanciones correspondientes.

APARTADO IMPORTANTE:

Cliente es persona expuesta políticamente _____.

Firma del cliente/PEP

PARA EL USO EXCLUSIVO DE LA INSTITUCION

Declaro bajo juramento que la persona o institución anteriormente expuesta es el reflejo fiel de la verdad. Manifiesto que tengo conocimiento que incurriría en sanciones administrativas y penales en caso de incumplir las normas y leyes establecidas en la Ley contra el lavado de dinero y activos.

**MANUAL DEL OFICIAL DE
CUMPLIMIENTO**

ElectroniCash, S.A.



ElectroniCash

INTRODUCCIÓN

El presente manual elaborado para el Oficial de Cumplimiento de la sociedad proveedora de dinero electrónico denominada ElectroniCash, comprende la naturaleza del cargo del Oficial de Cumplimiento en una sociedad proveedora de dinero electrónico, cuyo papel que desempeña es de vital importancia para la prevención de delitos de lavado de dinero y activos y financiamiento al terrorismo. La legislación salvadoreña obliga a las sociedades integrantes del sistema financiero a cumplir con el establecimiento de una oficialía de cumplimiento que es presidida por el oficial de cumplimiento, es por ello que en el contenido de este manual se presentan las funciones y responsabilidades del Oficial de Cumplimiento en seis capítulos básicos con respecto a la protección de su entidad del delito de lavado de activos.

Se detalla cual es la metodología de trabajo del Oficial de Cumplimiento y se destaca la importancia del cargo que tiene esta persona dentro de la empresa, el cual se define por los estándares de calidad de la función de cumplimiento a nivel local e internacional.

Uno de los elementos más importantes de un sistema integral para la prevención del lavado de activos de cualquier entidad proveedora de dinero electrónico, lo constituye la designación de un funcionario encargado de promover la adopción de los procedimientos específicos de prevención, su actualización y su conformidad con las exigencias legales.

Dicha persona recibe el nombre de Oficial de Cumplimiento, en términos generales se puede decir que es el responsable de institucionalizar la cultura de cumplimiento y prevención del lavado de dinero en la entidad proveedora de dinero electrónico para la cual labora.

Finalmente, se espera que con el desarrollo de este trabajo la tarea del oficial de cumplimiento sea más ligera, en el sentido de lograr la eficiencia y eficacia de los procesos establecidos para la prevención del delito.

CAPITULO I

LA PERSONA DEL OFICIAL DE CUMPLIMIENTO

Definición del Oficial de Cumplimiento.

Es la persona designada por la Junta Directiva quien es el máximo órgano directivo de la sociedad proveedora de dinero electrónico ElectroniCash, para que asuma las responsabilidades de establecer el código de conducta, verificar la aplicación de la ley, formular y ejecutar procedimientos y diseñar controles adecuados, efectivos y de calidad, con el propósito de prevenir la utilización de la entidad para los delitos de lavado de dinero y activos y financiamiento al terrorismo.

Nivel organizacional del cargo.

Por las responsabilidades propias que tiene el oficial de cumplimiento, el cargo debe estar clasificado en el nivel de alta gerencia, con dependencia directa de la Junta Directiva.

La persona designada para ejercer el papel del oficial de cumplimiento tendrá la única función del oficial, y no de otras actividades dentro de la entidad.

Características del oficial de cumplimiento.

La entidad ElectroniCash, cuando requiera de los servicios profesionales de este ejecutivo, es recomendable que el aspirante cumpla el siguiente perfil:

- Profesional preferiblemente en áreas administrativas.
- Total disposición al cambio.
- De proceder recto e íntegro.
- Enérgico, activo, diligente, dinámico y creativo.
- De actuar precavido y reservado.
- Debe conocer de manera amplia la actividad y servicios de la entidad.
- Amplia experiencia en control y supervisión.
- Manejar aspectos legales sobre lavado de dinero y activos y financiamiento al terrorismo.
- Conocer ampliamente sobre la gestión de riesgos.

CAPITULO II

FUNCIONES Y RESPONSABILIDADES

Todos los empleados de la entidad son responsables de proteger su integridad y la de la organización ante la eventual introducción de recursos de procedencia ilícita al sistema del dinero electrónico. La responsabilidad de cumplimiento de las normas de prevención de lavado de dinero es de todos los empleados, de acuerdo con las funciones y responsabilidades que se le hayan asignado. Una de las responsabilidades del oficial de cumplimiento, es la de velar por que en el manual de prevención de lavado de dinero y activos y financiamiento al terrorismo, se hayan asignado de manera precisa para cada uno de los cargos de la entidad, las funciones que le corresponden con respecto al sistema de gestión de riesgo de lavado de dinero o programa de cumplimiento.

El oficial de cumplimiento, es el empleado responsable de velar por la aplicación de los procedimientos específicos para la prevención y control del lavado de activos, establecidos al interior de la entidad y de la observancia del Código de Conducta, por parte de todos y cada uno de los empleados en el desarrollo de sus funciones.

Funciones.

Las siguientes son labores que debe ejecutar el oficial de cumplimiento, en desarrollo del programa de cumplimiento:

- a) Promover el diseño de los procedimientos específicos y adecuados para prevenir y controlar el lavado de activos, como parte integral del sistema de control interno de la entidad que debe ser adoptado por la oficialía de cumplimiento.
- b) Evaluar su idoneidad y conformidad con las exigencias legales.
- c) Procurar la formulación de las estrategias de la entidad para establecer los controles necesarios, con base en el grado de exposición al riesgo de lavado de activos.
- d) Verificar la aplicación de los procedimientos específicos para la prevención del lavado de activos, por parte de los empleados. Para estos efectos es conveniente que el oficial de cumplimiento diseñe y ponga en funcionamiento un manual de inspección.
- e) Verificar la observancia del Código de Conducta en las actuaciones del personal de la entidad.
- f) Realizar, directamente o por interpuesta persona programas de sensibilización dirigida a funcionarios nuevos y programas de capacitación continua sobre prevención del lavado de activos para los demás funcionarios.

- g) Efectuar revisiones periódicas documentales sobre el conocimiento del mercado a través de los diferentes segmentos en que se encuentra dividido.
- h) Presentar informes periódicos a Junta Directiva sobre lo adecuado, efectivo y la calidad de los procedimientos específicos adoptados para la prevención del lavado de activos, y sugerir acciones de mejoramiento en caso de presentarse cualquier falla al sistema de gestión de riesgos.
- i) Reportar las faltas o errores que implique la responsabilidad de los funcionarios al estamento interno que corresponda y realizar un informe completo de la situación a las autoridades competentes para que lleven a cabo la investigación.
- j) Efectuar análisis de operaciones no usuales.
- k) Velar por el adecuado reporte de operaciones sospechosas a la Unidad de Investigación Financiera de la Fiscalía General de la República.
- l) Orientar la conservación de los documentos relativos a la prevención del lavado de activos, de modo que estos se archiven y custodien debidamente.
- m) Velar por la actualización del manual de procedimientos específicos para la prevención del lavado de activos y el código de conducta, de acuerdo con los cambios normativos y del entorno de negocio.
- n) Cumplir con el rol de enlace con las autoridades competentes.
- o) Coordinar con la administración de la entidad la formulación del plan anual de cumplimiento y seguimiento como parte integrante de la función de planeación general de la entidad.
- p) Elaborar estadísticas con base en los siguientes criterios: Concentración de operaciones por cada segmento de mercado, movimiento consolidado por cliente, clasificación de operaciones por montos, movimiento registrado por monedas, clasificación de clientes por direcciones, etc.
- q) Efectuar seguimiento a los compromisos adquiridos por los directores de dependencias y oficinas de emprender acciones correctivas por fallas detectadas en la aplicación de los mecanismos de prevención y control.
- r) Velar por el arraigo de una cultura de cumplimiento de la entidad.

Es importante profundizar sobre la labor que debe cumplir el oficial de cumplimiento con respecto a algunos de los puntos que conforman el programa de cumplimiento.

En relación con la política de la debida diligencia o conocimiento del cliente, la labor del oficial de cumplimiento se debe dirigir a:

- a) Participar con los directivos de la entidad y las áreas de mercadeo en la definición de la política del conocimiento del cliente.
- b) Coordinar la difusión de esta política.
- c) Verificar que los empleados encargados de vincular a los clientes apliquen la política de debida diligencia del cliente; es decir, que soliciten y documenten, en formularios especialmente diseñados para el efecto y con visitas, la información sobre sus datos personales y su actividad económica.
- d) Su labor es verificar que se ha obtenido la información necesaria de los clientes que permita un control de sus operaciones. Si la información no contiene los datos suficientes para conocer al cliente, podrá solicitar que ésta se complete.
- e) Vigilar que los datos suministrados por los clientes se verifiquen y actualicen periódicamente a través de los medios necesarios y en la forma en que la entidad considere más eficaz.
- f) Finalmente, debe verificar que la entidad aplique los instrumentos necesarios para alcanzar el conocimiento del mercado en que sus clientes desarrollan su actividad comercial.

La labor que debe cumplir el Oficial de Cumplimiento frente al control de operaciones es la siguiente:

- a) En materia del control de operaciones, el oficial de cumplimiento debe revisar que los formatos diseñados para registrar las transacciones iguales o superiores a las cuantías señaladas por la autoridad competente, cubran los aspectos que las autoridades requieren y en sus visitas de control debe confirmar que estos están siendo debidamente diligenciados por parte del agente autorizado encargado de atender al cliente al momento de la transacción, para lo cual podrá apoyarse en las instancias de control interno que hagan una verificación periódica de la aplicación de estos registros.
- b) Cuando recibe de algún empleado el informe de operaciones inusuales, es decir operaciones que se salen del perfil del cliente y del segmento del mercado en que están situadas, detectadas por quien efectúa, tramita, registra o controla la transacción, ya sea que se informen directamente o a través de canales internos para la correspondiente evaluación, debe colaborar en la evaluación de las operaciones inusuales para determinar su normalidad o anormalidad respecto de las transacciones del cliente y con base en estos análisis poner en consideración de las autoridades superiores de la entidad, con el fin de definir su calificación como operación sospechosa y proceder a su reporte a las autoridades competentes.

- c) En la aplicación de la política conocimiento del empleado, la cual es una herramienta fundamental de control, el oficial de cumplimiento debe verificar que esta política incluya controles sobre cambios del comportamiento y del estilo de vida de un empleado, los cuales permiten deducir una conducta desviada, sobre todo si se tiene en cuenta el poder corruptor de las organizaciones criminales, que pueden socavar la integridad de los funcionarios más débiles en su formación ética.
- d) En cuanto a las personas que va a vincularse a la entidad, verificar que el área de gestión humana ha incluido en sus políticas de vinculación de personal un detenido análisis de los antecedentes del candidato, en el que se tendrán en cuenta no sólo las cualidades profesionales y académicas, sino también las calidades de sus principios éticos y morales.
- e) Respecto de los empleados de la entidad, se deben aplicar controles con el fin de verificar el cumplimiento de su gestión preventiva del lavado de activos. Para ello el oficial de cumplimiento puede apoyarse en los informes presentados por las áreas de seguridad, contraloría, recursos humanos y auditorías. Este control debe hacerse tanto para los aspirantes como sobre aquellos que se encuentren vinculados a la entidad.

Alcance del trabajo

El propósito fundamental del trabajo que realiza el oficial de cumplimiento en la entidad, es prevenir y detectar bienes, recursos y derechos provenientes de actividades delictivas, que pretenden ingresar a la economía de la entidad a través de su portafolio de servicios.

Lo anterior requiere que los agentes autorizados, tengan el máximo cuidado al momento de vincular clientes y durante la realización de las operaciones.

Se requiere entonces, que la alta gerencia que encabeza al oficial de cumplimiento, efectúe sus seguimientos y análisis pertinentes con la debida profundidad para garantizar la protección de los empleados y de la organización.

A continuación se describe los elementos que determinan el alcance del trabajo del oficial de cumplimiento.

Objetivo

Evaluar constantemente los mecanismos para la prevención de lavado de dinero y activos y financiamiento al terrorismo, adoptados por la entidad, a efectos de establecer los más adecuados y efectivos y la calidad de ejecución de las responsabilidades inherentes al desarrollo de las operaciones.

Los mecanismos para la prevención deben tener como mínimo las siguientes características:

- Adecuados, si proveen razonable seguridad para alcanzar objetivos de prevención y control.
- Efectivos, si están funcionando como se espera.
- Tendrán calidad, sí los objetivos y metas organizacionales son alcanzados.
- Naturaleza y extensión de los procedimientos de revisión aplicados.

Para el logro de los objetivos descritos anteriormente, el oficial de cumplimiento debe aplicar los siguientes procedimientos de revisión:

- **Revisión documental:** el cual consiste en el examen de registros y documentos originados en las operaciones, y que se conservan en la entidad.
- **Observación:** mediante el examen a los procedimientos operativos que efectúan los empleados en el desempeño de su cargo en la entidad, los clientes en la realización de las operaciones, y, las herramientas automáticas que pueda ofrecer el desarrollo tecnológico de la entidad.
- **Revisión analítica:** mediante el estudio de fluctuaciones y operaciones inusuales, registradas en documentos de soporte de las operaciones efectuadas por los clientes, y el registro de las mismas en la base de datos computarizada.
- **Evaluación:** consiste en la valoración de los conocimientos de los empleados de la entidad, sobre los mecanismos de prevención del lavado de activos, mediante la aplicación periódica de pruebas escritas y orales, para determinar las necesidades de capacitación del personal.

La extensión de los procedimientos de revisión incluye el análisis de:

- Documentos soportes de las operaciones propias de la entidad, correspondiente a un período determinado.

- Los procedimientos para la prevención del lavado de activos, contenidos en el manual para la prevención del lavado de dinero y activos y financiamiento al terrorismo y la verificación de estos en relación a ser adecuados, efectivos y de calidad.
- La observancia por parte de los empleados de los principios del Código de Conducta, como plataforma ética y moral de la entidad.
- Las acciones correctivas emprendidas por la administración de la entidad para mejorar las deficiencias de los mecanismos de prevención que se hayan encontrado.
- El contenido del manual de funciones de los cargos existentes en la entidad y la asignación de responsabilidades específicas con respecto a la prevención del lavado de activos, de acuerdo con las funciones de cada cargo.

Código de Conducta

Una de las responsabilidades del oficial de cumplimiento es el establecimiento de la cultura de cumplimiento organizacional, a través de la ejecución de los programas de capacitación continua dirigidos a todo el personal de la entidad. Y es responsabilidad de la Junta Directiva o del Consejo de Administración de la entidad la adopción de políticas y directrices que preserven la integridad de la empresa y de sus empleados. Además, se debe realizar la formulación del plan anual de trabajo dentro de la función de planeación de la empresa con la asignación de recursos para desarrollar la política de reducir la exposición al riesgo del lavado de activos y arraigar la cultura de cumplimiento.

Informes dirigidos a las autoridades superiores de la entidad

Es responsabilidad del oficial de cumplimiento, mantener informado al Consejo de Administración o a la Junta Directiva, sobre lo adecuado, efectivo y la calidad de los mecanismos específicos para la prevención del lavado de activos, que han sido adoptados.

Dicho informe debe contener por lo menos los siguientes aspectos:

- Procedimientos de revisión empleados.
- Objetivos del informe.
- Período objeto de revisión de operaciones
- Grado de cumplimiento de los procedimientos por parte de los empleados.
- Deficiencias de control detectadas.

- Conclusiones.
- Recomendaciones.
- Compromisos de mejoramiento.
- Seguimiento a las acciones correctivas adelantadas.
- Evidencia de cumplimiento de compromisos.

Deberá, además, coordinar la ejecución del plan anual de trabajo. Dentro de las funciones de planeación y presupuesto de la entidad, se debe prever la asignación de recursos para implementar un plan anual de trabajo, que debe ser aprobado por Junta Directiva, y que contendrá las diferentes actividades sobre prevención y control del lavado de activos, que se estimen realizar periódicamente para proteger a la entidad y a sus empleados de dicho riesgo y para institucionalizar la cultura de cumplimiento.

El citado plan puede estar compuesto de las siguientes actividades:

- Programas de capacitación dirigidos a directivos y empleados.
- Programas de capacitación dirigidos al oficial de cumplimiento.
- Implementación de nuevos procedimientos de prevención y control del riesgo.
- Jornadas de sensibilización sobre protección al riesgo de lavado de activos.
- Programas de actualización del sistema de gestión de riesgo de lavado de activos.
- Programación de visitas de inspección a los diferentes agentes autorizados de proveer dinero electrónico, para evaluar lo adecuado y efectivo del sistema de gestión de riesgo de lavado de activos.
- Reuniones con las autoridades de control como la Auditoría Interna y la Auditoría Externa, la Policía Nacional Civil y la Fiscalía General de la República.
- La asistencia a eventos como seminarios, diplomados y encuentros en el ámbito nacional e internacional.
- Visitas a ciertos clientes para conocer su actividad económica y establecer el potencial de generación de ingresos operacionales y no operacionales.
- Programas que contemplen la investigación y el desarrollo de nuevos mercados para establecer agencias u oficinas de vinculación y atención de clientes, en el territorio nacional o internacional sin prescindir de mecanismos de conocimiento del mercado y del cliente, que permitan determinar el origen lícito de los recursos a transferir en dicha zona.

CAPITULO III

METODOLOGÍA DEL TRABAJO

Planeación del trabajo del Oficial de Cumplimiento

El oficial de cumplimiento durante el desarrollo de sus funciones debe elaborar planes de los trabajos que se pretenden efectuar. La formulación de planes de trabajo se utiliza para demostrar el orden y la buena utilización de los recursos con los que se cuenta para realizar el trabajo.

El plan de trabajo del oficial de cumplimiento en una entidad, desarrolla los siguientes aspectos:

- Adquirir un adecuado conocimiento de la misión, visión, políticas, principios, valores y procedimientos de la entidad y del medio ambiente donde ella opera.
- Definir claramente los objetivos del trabajo de cumplimiento.
- Determinar el grado de exposición al riesgo de lavado de activos.
- Diseñar una estrategia de cumplimiento.

Lo anterior significa que el oficial de cumplimiento, debe elaborar un plan anual de cumplimiento el cual describe las actividades a desarrollar, el responsable de la ejecución del trabajo, las dependencias afectadas, el tiempo de duración, el resultado obtenido, las acciones de mejoramiento emprendidas y el monitoreo para establecer el grado de cumplimiento de los objetivos trazados.

Evaluar el riesgo del lavado de activos

Una de las principales responsabilidades de la oficialía de cumplimiento, es evaluar el grado de exposición de los empleados y de la entidad, al riesgo de verse involucrados en un esquema de lavado de activos.

La medición del riesgo de lavado de activos, se efectúa a través de una matriz de riesgo, que consiste en determinar las variables, los factores y situaciones generadores de riesgo; valorar el riesgo; identificar las dependencias u oficinas mayormente expuestas; formular los procedimientos específicos para atenuar la exposición; y racionalizar los recursos de prevención y control interno.

La metodología de la matriz de riesgo, permite al oficial de cumplimiento, programar visitas de cumplimiento; diseñar programas de revisión adecuados; determinar el alcance de las revisiones; coordinar la frecuencia y alcance de las visitas de inspección con la auditoría y la auditoría interna; lograr un conocimiento del mercado de los servicios ofrecidos y de los clientes; entre otros aspectos.

Seguimiento a la implementación de procedimientos específicos de prevención del lavado de activos.

De igual forma, es competencia del oficial de cumplimiento, diseñar procedimientos específicos para la prevención y control del lavado de dinero y activos; con base en las siguientes directrices:

- **Políticas de Prevención y Código de conducta**

La entidad debe establecer un código de conducta el cual se constituye en la plataforma moral y ética institucional y desarrolla el siguiente contenido:

La declaración de principios de la entidad, inspirada en la lucha institucional contra el lavado de activos y en la colaboración con las autoridades.

Principios.

- Valores institucionales.
- Valores éticos.
- Sanciones impuestas ante incumplimientos al código de conducta.
- Resolución de situaciones generadoras de conflictos de interés.
- Cumplimiento de las leyes y los estatutos internos.
- Actuaciones prohibidas al personal.
- Manejo de información privilegiada.
- Relaciones con los clientes.
- Relaciones con los proveedores.
- Dedicación al trabajo.
- Conductas relacionadas con limitación de regalos y atenciones recibidas.
- Competencia profesional.
- Desarrollo del personal.

- **Conocimiento de los procedimientos operacionales**

Es indispensable que el oficial de cumplimiento conozca y entienda el ciclo operacional de la entidad. El diseño e implementación de procedimientos específicos para la prevención del lavado de dinero y activos, se efectúa sobre dichos procedimientos operacionales generales.

Conocimiento del mercado

- Diseño de perfiles de los clientes.
- Conocimiento del cliente.
- Segmentación de mercado.
- Detección y reporte interno de operaciones inusuales.
- Reporte de operaciones inusuales a la unidad que corresponda.
- Revisión de las operaciones inusuales y procedimiento para el reporte de operaciones sospechosas a las autoridades competentes.
- Consolidación de la información por cliente.
- Programas de capacitación continúa.
- Responsabilidades del "oficial de cumplimiento".
- Política para el "conocimiento del empleado".
- Desarrollo tecnológico.
- Determinación de señales de alerta.
- Procedimiento para el registro de las operaciones realizadas por la entidad.
- Estándares internacionales para la prevención del lavado de activos.
- Modelos para el reporte de información periódica a la Unidad de Investigación Financiera – UIF.
- Procedimientos para la atención a requerimientos formulados por las autoridades competentes.
- Procedimiento para la conservación y archivo de los documentos soportes de las operaciones.
- Procedimientos para el reporte de información periódica a las entidades de vigilancia y control o a las Unidad de Investigación Financiera (UIF).
- Metodología a ser empleada en las visitas de inspección a los diferentes agentes autorizados y oficinas de la entidad, por parte de los órganos de control interno.
- Funciones de la auditoría interna con respecto a la prevención de lavado de dinero y activos.
- Funciones de la auditoría externa con respecto a la prevención de lavado de dinero y activos.
- Régimen sancionatorio ante incumplimiento de los procedimientos específicos.

El oficial de cumplimiento debe revisar y estudiar el contenido del manual para verificar que se ajuste a las políticas de la entidad, y a los lineamientos generales que la Superintendencia del Sistema Financiero determine.

De la evaluación y análisis que hace de los procedimientos de control contenidos en el manual de procedimientos, determina si éstos son eficaces, si comprenden todas las operaciones de la entidad, y si son aplicados por los empleados de la entidad, así como el grado de eficacia de los mismos.

Debe sugerir a la administración efectuar las correcciones necesarias para mejorar el manual de procedimientos y su aplicación. En este sentido el oficial de cumplimiento tiene un papel de asesor frente a los directivos de la entidad, para que se adecuen a los lineamientos exigidos por las normas del país.

- **Establecimiento de una cultura de cumplimiento**

El oficial de cumplimiento debe velar por una cultura de cumplimiento institucional; basada en el convencimiento de los empleados al interior de la entidad, de asumir una actitud vigilante durante el desarrollo de las operaciones para evitar en todo momento que los funcionarios y la institución sean objeto de un esquema de lavado de activos.

Cuando el funcionario de cumplimiento, mediante estudio, análisis y seguimiento de las operaciones, establece algún grado de exposición de la entidad al riesgo de lavado, genera mecanismos de prevención y control suficientes, encaminados a preservar en todo tiempo y lugar la integridad individual e institucional.

El grado de responsabilidad que debe asumir el Oficial de Cumplimiento en la entidad, debe consistir en instruir a las personas que conforman la organización, en un comportamiento ético y responsable, encaminados al aseguramiento de la calidad en la ejecución de los procedimientos específicos de prevención y control, para mantener a salvo a la entidad, de la influencia de actividades delictivas.

- **Formulación y aplicación de programas de revisión y análisis**

Este procedimiento es un elemento importante dentro de las funciones del Oficial de Cumplimiento, el cual consiste en: implementar medidas de rutinas de revisión con el objeto de verificar el cumplimiento de las normas y reglamentaciones internas, en los procedimientos diseñados por la entidad para protegerse del lavado de activos y alcanzar metas institucionales.

Existen varias clases de medidas de revisión y análisis: revisión de operaciones, inspección a dependencias y oficinas de la entidad, inspección a clientes, verificación de cumplimiento de normas, análisis de razonabilidad de operaciones inusuales, revisión de segmentos de mercado, análisis estadístico de operaciones por cliente, cruce de clientes en listas OFAC narcóticos y terroristas, capacitación y análisis de viabilidad de reporte de operaciones sospechosas.

- **Conformación de la evidencia documental de las revisiones y análisis efectuados**

La evidencia documental, está contenida en los documentos elaborados por el Oficial de Cumplimiento, durante el período de revisiones:

- Plan anual de cumplimiento.
- Reportes de revisión y análisis de las operaciones.
- Reportes de inspección a dependencias y oficinas.
- Reportes de inspección a clientes.
- Reportes del análisis de razonabilidad de operaciones inusuales.
- Reportes de revisión de segmentos de mercado.
- Resultados de revisión y análisis de capacitación.
- Análisis de viabilidad de reporte de operación sospechosa.
- Fotocopias de documentos fuentes sobre los cuales se efectuó trabajo de revisión.
- Prueba escrita de conocimientos sobre prevención de lavado de activos aplicados a todo el personal de la entidad.
- Análisis estadístico de operaciones por cliente.
- Informe producto de las revisiones y análisis.

Los documentos relacionados anteriormente, deben estar debidamente archivados en legajos rotulados con la imagen visual corporativa de la entidad, el objeto de revisión y la fecha correspondiente.

- **Formulación de conclusiones y recomendaciones**

Toda revisión analítica efectuada por el Oficial de Cumplimiento, debe conducir a una conclusión sobre el estado en que se encuentra el objeto examinado y, eventualmente, a la formulación de recomendaciones tendientes a emprender acciones correctivas inmediatas por parte de los empleados indicados en coordinación con el Oficial de Cumplimiento o miembros de su grupo de apoyo.

En el informe de resultados de las revisiones y evaluaciones que periódicamente el Oficial de Cumplimiento efectúa y luego remite periódicamente a la Junta Directiva de la entidad, forma parte del mismo, las conclusiones y las recomendaciones correspondientes a cada objeto revisado.

Posterior a la presentación del informe ejecutivo a la Junta Directiva, el oficial de Cumplimiento en coordinación con la auditoría interna, adelantan el proceso de seguimiento a las recomendaciones formuladas, a los compromisos adquiridos por los empleados indicados y a las acciones correctivas aplicadas a efectos de corroborar que la acción de mejoramiento se llevó a cabo.

Si las acciones correctivas acordadas no se llevan a cabo en el tiempo establecido, serán materia de informe al máximo órgano directivo en el período correspondiente, a efectos de darle aplicación al régimen de sanciones pertinente.

CAPITULO IV

CONOCIMIENTO DEL CLIENTE

Este capítulo comprende la aplicación del principio de debida diligencia, cuáles pueden ser las diferentes medidas a implementar para conocer al cliente, su perfil de usuario, su número de operaciones realizadas, etc. Se detalla una serie de etapas que facilitan la aplicación de este principio y cuáles serán las decisiones a tomar en caso que se presenten operaciones sospechosas o inusuales.

- **Del Conocimiento del Cliente en General**

Existen muchas formas de conocer al cliente. Desde el punto de vista del comerciante, se puede conocer al cliente cuando se conocen sus hábitos de consumo, sus preferencias y las demás características que describen su posición relativa frente a los demás clientes. Desde el punto de vista social, es cuando se ha tenido algún tipo de relación con él, por ejemplo cuando el cliente es un conocido o un amigo.

Para efectos de la prevención al lavado de activos, el conocimiento del cliente desde el punto de vista del mercado y desde el punto de vista social es muy útil pero no suficiente. Las políticas de conocimiento del cliente en toda entidad deben ser un esfuerzo organizado para recolectar la información relevante que permita detectar y analizar operaciones sospechosas. Todo el esfuerzo de los sujetos obligados por conocer a sus clientes tiene dos propósitos generales:

- Servir de medida disuasiva para alejar a los lavadores de la entidad.
- Permitir la detección de operaciones inusuales y la determinación de operaciones sospechosas, que deben reportarse a las autoridades.

No obstante lo anterior, la entidad debe entender la política de conocimiento del cliente para efectos de la prevención al lavado de activos como parte integral de su negocio e integrarla a los demás esfuerzos que se hacen por conocer al cliente en otras áreas. De esta forma, el conocimiento del cliente desde el punto de vista del mercadeo sirve como guía para la política de prevención al lavado de activos y, a su vez, la labor de prevención al lavado de activos puede arrojar información valiosa que se traduce en un mejor servicio a los clientes.

- **Información relevante**

Se puede tener mucha información sobre el cliente sin que ésta sea relevante para efectos de prevenir y controlar el lavado de activos. La información relevante para este propósito es la que sirve para establecer los siguientes aspectos:

- Identificación completa.
- Actividad económica, procedencia u origen de los fondos.
- Volumen y características de las transacciones financieras.

- **Etapas del conocimiento del cliente**

El conocimiento del cliente no es simplemente una obligación puntual que se cumple con el diligenciamiento de unos formatos. Se trata de una política que implica una acción planeada y coordinada entre varias áreas de la entidad, labor que se desarrolla en cinco instancias: preparación y diseño, vinculación del cliente, análisis de la información, prestación del servicio y actualización de datos.

Para desarrollar una política de conocimiento del cliente eficaz, la entidad ha realizado una labor continua y organizada que puede ser descrita mediante las siguientes etapas:

Preparación y diseño

Bajo el criterio orientador de la legislación vigente, los sujetos vigilados deben establecer procedimientos para cumplir con la obligación de conocer al cliente. Al mismo tiempo, se deben diseñar y elaborar los formatos correspondientes y establecer los sistemas de almacenamiento, conservación y consulta de la información.

Vinculación del Cliente

El momento más importante en este proceso es la vinculación del cliente. Se trata de su primera relación con la entidad, en la cual el cliente presenta su documentación y la entidad decide sobre su vinculación. Esta oportunidad es muy valiosa para desarrollar la política de conocimiento del cliente y prevención del lavado de activos. Para efectos operativos y de controles propios del servicio, la entidad solicita información básica como registros de firmas, fotocopias de documentos de identidad, direcciones de correspondencia, referencias, etc. A su vez, la política de conocimiento del cliente conlleva la solicitud y análisis de información complementaria que tiene como único fin evitar que la entidad sea utilizada para lavar activos o legitimar capitales.

En todo caso, es importante tener en cuenta que cuando se analicen operaciones inusuales o sospechosas, la mejor fuente de información para realizar este estudio es aquella suministrada por el cliente al momento de vincularse a la entidad. En consecuencia, un mecanismo que permita la consulta fácil de esta información es fundamental para el ágil desarrollo de la política de prevención al lavado de activos.

Análisis de la información suministrada

El conocimiento del cliente no es una actividad pasiva, en la cual el sujeto obligado solicita la información y el cliente la suministra. Se asegura que esté completa, se solicita información adicional o explicativa, se verifica ciertos datos y, finalmente, se establece que toda la información tenga sentido y sea coherente.

Prestación del servicio

Una vez vinculado formalmente a la entidad, los clientes acuden a la entidad para realizar sus transacciones con diferentes propósitos y bajo muy diversas modalidades. En todos estos eventos, la entidad debe identificar a las personas que realizan estas operaciones, sin necesidad de repetir el proceso que se realizó a la hora de la vinculación del cliente.

Cuando se presta un servicio a un cliente ya vinculado, sobre el cual se ejerció la política de conocimiento del cliente, se pretende simplemente confirmar que la persona que realiza las transacciones es efectivamente el cliente de la entidad. Lo anterior con varios propósitos dentro de los cuales se encuentran:

- Comparar la operación con el perfil del cliente y el segmento del mercado.
- Consolidar las operaciones periódicas del cliente para efectos de análisis y control.
- Confrontar los listados especiales (Listas de clientes que no deben ser vinculados).

Actualización de datos

Es normal y necesario que los clientes cambien algunas de sus características personales y financieras durante la duración de la relación contractual con la entidad. Las personas naturales y las empresas cambian de actividad económica, de domicilio, etc. Por esta razón, es importante actualizar en forma periódica y sistemática los datos suministrados por los clientes. De lo contrario, la confrontación de las

operaciones realizadas con la información no actualizada del cliente puede inducir a creer que existen operaciones sospechosas donde no las hay o lo contrario.

- **Aspectos que implica el conocimiento del cliente**

Conocer al cliente implica recolectar y analizar información relevante sobre su identidad y su actividad económica. Esta información proviene de diferentes tipos de fuentes, los cuales pueden ser públicas y privadas, y conforman un conjunto de datos que le sirven a la entidad para conocer el riesgo relativo de cada uno de sus clientes frente a operaciones de lavado. A su vez, todos los documentos y los datos recolectados en desarrollo de esta política servirán de sustento para detectar operaciones sospechosas y encontrarle justificación a operaciones que aparecían como tal a primera vista. Por estas razones de peso, la entidad debe recaudar la información pertinente sobre sus clientes, de acuerdo con ciertas pautas que se describen a continuación. De esta labor depende el éxito del control que con dicha información se puede ejercer.

Los aspectos o labores que conforman el conocimiento del cliente son:

- Identificación del cliente.
- Diligenciamiento de formularios.
- Solicitud de documentos de soporte.
- Verificación de datos.
- Consulta de listas especiales.
- Asignación del perfil y ubicación en el segmento del mercado.
- Selección del cliente.
- Anticipación de servicios y movimientos.
- Solicitud de una declaración jurada.
- Conservación y organización de la información.
- Consolidación de operaciones.
- Actualización de datos y documentos.

Identificación del Cliente

Comúnmente las personas se identifican con el nombre y el número de documento de identidad. En términos sencillos, identificar es asegurarse que la persona que se acerca a la entidad no es otra, es decir no es suplantada o está actuando con una identidad falsa. La entidad emplea diversos métodos para

identificar a las personas y dejar constancia de que fueron efectivamente ellas quienes realizaron las operaciones o transacciones. Esta labor se basa, por lo general, en el cotejo o comparación de la firma, la fotografía y la huella dactilar en documentos que se presumen auténticos, frente a los documentos presentados por el cliente.

Para identificar las personas comúnmente se emplean algunos de los siguientes documentos: contratos sociales, estatutos, registro mercantil, documentos notariales, documentos de identificación tributaria, licencias o registros especiales.

Como mecanismo adicional se solicitan referencias personales, laborales, bancarias o comerciales que tienen el propósito de determinar la existencia real de la persona, vincularla con otros individuos o empresas, y facilitar la verificación de los datos básicos.

Diligenciamiento de formularios

No basta con identificar a la persona, es necesario consignar sus datos básicos y su información financiera en tal forma que ésta pueda ser utilizada cuando se requiera. Por esta razón, el agente autorizado establece formularios especialmente diseñados para consignar la información que permite obtener un conocimiento adecuado del cliente.

Normalmente estos formularios se diseñan y clasifican según los siguientes aspectos:

- Servicio (ejemplo: Formulario de apertura de cuenta electrónica)
- Tipo de cliente (ejemplo: Persona Natural)
- Etapa de la relación con el cliente (ejemplo: Formulario de actualización de datos)

Solicitud de Documentos de Soporte

Si bien existe el principio de buena fe, la información suministrada por los clientes debe ser verificada y soportada en ciertos casos. Por esta razón, los agentes autorizados deben solicitar ciertos documentos originales para comprobar la veracidad de la información suministrada. En ciertos eventos los agentes conservan copias u originales de algunos de estos documentos como formatos, declaraciones, contratos, etc.

Verificación de Datos

La obligación de verificar la información suministrada, de la cual se hizo referencia en el punto anterior, puede cumplirse de varias formas, según el riesgo que implique la transacción, la experiencia de la

entidad y las posibilidades prácticas. En algunos casos, basta con consultar información pública y fácilmente disponible. En otros casos, la entidad considera necesario tomar medidas adicionales y visitan al cliente en sus instalaciones para confirmar que la información suministrada es veraz. No es operativo ni pertinente visitar a todos los clientes de la entidad, como tampoco es prudente creer en toda la información suministrada por los clientes. Las entidades deben ejercer su buen juicio, conforme a la legislación aplicable, para determinar el alcance de su política de verificación de información.

Consulta de Listas Especiales

A criterio de la entidad, se pueden utilizar las listas que diferentes autoridades expiden con el propósito de alertar sobre los antecedentes de ciertas personas o empresas. Estas listas deben ser utilizadas con sumo cuidado, pues la existencia de homónimos puede generar inconvenientes en su aplicación. Para efectos del narcotráfico, es muy conocida internacionalmente las listas de la OFAC.

Selección del Cliente

Como se ha manifestado, el conocimiento del cliente al momento de la vinculación del mismo tiene varias ventajas. La más importante de ellas es que al no haberse realizado todavía ninguna transacción económica, la entidad está a tiempo para determinar si el cliente está dentro de su mercado objetivo. En algunos casos, los agentes autorizados pueden determinar que no es conveniente vincular al cliente, pues dentro de sus controles tienen un sistema de evaluación de factores de riesgo que les permite detectar desde el comienzo los clientes no deseados.

Anticipación de servicios y movimientos

Una de las herramientas más eficaces para la detección de operaciones inusuales es la anticipación de las operaciones que el cliente tiene posibilidad de realizar según su actividad económica. Se trata de analizar la información financiera suministrada para determinar las características y el monto dentro de los cuales se deben enmarcar las operaciones del cliente en el futuro cercano.

Solicitud de una declaración jurada

Es sumamente importante informar al cliente de la necesidad de contar con información verdadera y exacta sobre su identidad y su actividad económica. Muchas veces los clientes abordan los formatos de la política de conocimiento del cliente sin la debida atención, pues asumen que se trata de un trámite rutinario sin mayores consecuencias. Por esta razón, y como medida disuasiva frente a posibles casos de

lavado de activos, es costumbre solicitarles a los clientes que certifiquen la veracidad de la información mediante una declaración jurada en este sentido. El mismo texto debe mencionar las consecuencias en caso de suministrar información falsa o hacer uso indebido de los servicios prestados por la entidad.

Conservación y organización de la información

La información que se recopila en desarrollo de la política de conocimiento del cliente tiene como propósito servir de sustento para el análisis de operaciones sospechosas que la entidad debe realizar. Por esta razón, debe prestarse especial atención a la conservación tanto de los documentos físicos como de los datos que se tengan en medio electrónicos sobre los clientes.

En este sentido es importante tener en cuenta dos aspectos de la conservación de documentos: organización interna y tiempo de conservación. Se establecen procedimientos especiales para la organización de la información de los clientes, como el uso de carpetas que deben contener la información básica de cada cliente. Por otra parte, se deben atender plazos de conservación de los documentos del cliente, los cuales oscilan entre cinco y diez años.

Consolidación de operaciones

En algunos casos es suficiente una operación de un cliente para poder determinar que se trata de una operación sospechosa. No obstante, en la mayoría de los casos, es necesario apreciar la actividad del cliente en su conjunto para poder compararla con su perfil, el segmento del mercado al cual pertenece, las señales de alerta y los demás mecanismos de control establecidos por la entidad para determinar que la operación es sospechosa.

Por esta razón, corresponde al oficial de cumplimiento de la entidad consolidar el conjunto de operaciones de un cliente en un período fijo que normalmente corresponde a un mes calendario, para obtener una visión más completa de los movimientos del cliente y así poder analizarlos.

El informe de consolidación de operaciones contiene lo siguiente:

- Separación de movimientos de envío y recepción de dinero electrónico.
- Agrupación de información por servicio y región.
- Incluir el perfil del cliente y la fecha de asignación del mismo.
- Descripción del segmento del mercado en el cual se encuentra el cliente.

Actualización de Datos y Documentos

Algunos de los datos que el cliente suministra al momento de su vinculación tienen baja probabilidad de cambiar con el tiempo. Por el contrario, la información financiera es por esencia cambiante, y por lo tanto es necesario actualizarla constantemente para poder analizar las operaciones del cliente frente a su perfil real. Muchas operaciones que a primera vista aparecen como sospechosas, son el resultado de comparar operaciones de los clientes frente a perfiles desactualizados.

- **Objetivos de la política del conocimiento del cliente**

El conocimiento del cliente como parte de las políticas de la entidad no es un concepto nuevo, por el contrario, se trata de un aspecto fundamental de la actividad comercial de la misma. El establecimiento de procedimientos y mecanismos de identificación del cliente y determinación de su actividad económica para prevenir el lavado de activos son de los objetivos principales en estas políticas.

Principales objetivos

La política de conocimiento del cliente no debe mirarse como una actividad aislada que no cumple con los objetivos principales del negocio. Por el contrario, una política efectiva de conocimiento del cliente puede servir de base para una exitosa gestión comercial y de administración del riesgo.

Objetivos Comerciales

Conocer al cliente permite conocer sus características como consumidor de servicios, para ofrecer productos adicionales o novedosos. Los retos del mercado actual exigen que la entidad conozca las preferencias y los hábitos de consumo de sus clientes, toda esta información, debidamente analizada, permite personalizar y mejorar el servicio.

Objetivos preventivos o de control

Ejercer la política de conocimiento del cliente no solamente previene y controla la ocurrencia de operaciones de lavado de activos. La entidad se encuentra bien informada sobre la actividad económica de su cliente puede evitar otros delitos como el fraude.

Objetivo de administración del riesgo

La esencia de la entidad en el trabajo de la gestión de riesgos de lavado de dinero es la administración del riesgo. Un seguimiento constante de las operaciones de los clientes, en particular y en su conjunto, permite evaluar correctamente el riesgo y tomar acciones frente a este.

- **Resultado de la política de conocimiento del cliente**

Cuando la entidad ha logrado desarrollar su política de conocimiento del cliente en forma efectiva, no solamente está cumpliendo con una obligación legal, sujeta a sanciones por incumplimiento. Conocer al cliente, le aporta muchos beneficios a la entidad, entre los cuales vale la pena mencionar:

- Selección adecuada de clientes, basada en información confiable y análisis del riesgo de lavado de activos.
- Detección de operaciones inusuales cuando las operaciones del cliente se alejan de los parámetros de normalidad que se deducen de la actividad del cliente.
- Sustento para reportar como operaciones sospechosas, aquellas que una vez comparadas con la información suministrada por el cliente se consideran como sospechosas.
- Pruebas eficaces de que se ha actuado diligentemente en la aplicación de los controles al lavado de activos.
- Datos y documentos sobre el cliente para atender las solicitudes particulares de información que presenten las autoridades competentes.

- **Reporte de operaciones sospechosas**

Para poder reportar una operación como sospechosa, la entidad tiene que comparar el conjunto de operaciones del cliente con su perfil. Operaciones que resultan normales para determinados clientes pueden ser completamente sospechosas para otros.

- **Segmentación del mercado**

En términos simples, segmentar el mercado es agrupar a los clientes de acuerdo con las características básicas de sus operaciones (servicios, frecuencia, localización, etc.). La racionalidad de la entidad dicta que los clientes de un mismo segmento deben tener características económicas, contables y financieras similares. Es decir que los datos recolectados al momento de conocer a los clientes deben permitir asumir el segmento del mercado en el cual se situarán.

CAPITULO V

SEGMENTACION FACTORES DE RIESGO Y REPORTES

- **Informe o notificación de operaciones sospechosas**

Definición de operaciones sospechosas

La entidad debe verificar si las operaciones de sus clientes guardan relación con la actividad económica que se mantiene en los registros e informar a las autoridades competentes las transacciones que resulten sospechosas.

Cuando una operación se aparta del perfil del cliente o presenta una inconsistencia en el giro ordinario de sus negocios, en la frecuencia o volumen de los movimientos que el cliente realiza, o porque sus características particulares se salen de toda lógica, la operación debe ser considerada como una operación inusual. Cuando se está frente a una operación inusual o atípica la entidad debe proceder a realizar un análisis de la situación y en el evento en que dicha operación no refleje una respuesta lógica y razonable la operación se convierte en "sospechosa" y debe ser comunicada a la autoridad competente.

No toda operación inusual es sospechosa. Es el caso de aquellas operaciones atípicas en el giro de los negocios del cliente, que sí tienen una explicación lícita y razonable, las cuales no debe ser objeto de reporte.

El reporte de operación sospechosa es consecuencia de una cuidadosa revisión, gestión en la cual es recomendable el apoyo y participación del oficial de cumplimiento y decida por la Junta Directiva.

El informe de una operación sospechosa no es una denuncia penal de la existencia de un delito de lavado de activos. Con el reporte solo se cumple con el deber de colaboración con las autoridades de informar situaciones anormales. Se informa sobre las inconsistencias en el manejo de una cuenta o producto con respecto de la actividad y el perfil financiero que le conoce al cliente.

- **Consideraciones especiales sobre el reporte de operaciones sospechosas**

La entidad debe desarrollar un gran esfuerzo para analizar sus operaciones y determinar cuáles de éstas deben ser puestas en conocimiento de las autoridades bajo la modalidad de reporte de operaciones sospechosas. Este reporte materializa el resultado de la colaboración de la entidad en la lucha de la sociedad contra el lavado de activos.

El papel que cumple la entidad es muy importante, y por lo tanto debe ser asumido con mucho compromiso tanto por los directivos como por las personas encargadas de realizar los controles. A su vez, el cliente de la entidad puede verse afectado tanto en el desarrollo de los controles como en las investigaciones que realicen las autoridades, en consecuencia, los empleados que participen en los reportes deben manejar este tema con mucho profesionalismo y rectitud.

Hay que hacer énfasis en la naturaleza de la colaboración de la entidad y aclarar que se trata de un reporte de operaciones sospechosas, basado en la información parcial y fragmentada que tienen los sujetos obligados sobre la actividad de sus clientes. Corresponde a las autoridades iniciar las investigaciones pertinentes para determinar si se trata de actuaciones que pueden ser calificadas como delito. No le corresponde a la entidad entrar en consideraciones jurídicas, evaluar pruebas o pronunciarse sobre la legalidad de las conductas de sus clientes.

En relación con el reporte de operaciones sospechosas, se considera conveniente que la entidad tenga siempre en cuenta los siguientes comentarios sobre las características de dicho reporte:

Se reportan operaciones, no personas. Se reportan operaciones sospechosas, no clientes sospechosos. La entidad evalúa las operaciones realizadas por un cliente o un conjunto de clientes y si se salen de los parámetros de normalidad, las puede calificar como operaciones sospechosas. En ningún momento, la decisión de calificar una operación como sospechosa y reportarla a las autoridades implica una acusación o denuncia por parte de la entidad.

El reporte no implica denuncia. Al reportar una operación como sospechosa, la entidad le hace llegar una información útil y pertinente a las autoridades, en el entendido que solamente las autoridades judiciales pueden definir si se trata de una operación de lavado de activos. Por esta razón, la eficacia de una política de prevención al lavado de activos nunca debe medirse por el número de reportes o la proporción de estos que se traducen en condenas. Igualmente, la entidad no necesita definir el delito que se cometió ni otras circunstancias de las operaciones que son competencia de los investigadores judiciales.

El reporte no es infalible. El reporte que realiza la entidad se basa en la información disponible en la misma al momento de realizarlo. La entidad no posee toda la información sobre el cliente y sus negocios, tampoco tiene facultades para solicitar pruebas, por lo tanto su visión y su entendimiento sobre los negocios de sus clientes no son completos. Esto hace que algunas de las operaciones que se reportan como sospechosas no lo sean y que otras operaciones que nunca son detectadas puedan resultar siendo operaciones de lavado. Ni el más desarrollado sistema de prevención al lavado de activos puede

garantizar que una entidad no sea utilizada para el lavado de activos. Lo importante es que la entidad realice su mejor esfuerzo para detectar las prácticas de lavado conocidas y aquellas que por sus características pueden ser detectadas.

La obligación de detección de operaciones inusuales no recae sobre una sola persona en la entidad. Comúnmente se cree que el Oficial de Cumplimiento o el responsable de la política de prevención al lavado de activos es el responsable de descubrir y reportar las operaciones sospechosas. Esto no es cierto. La labor de analizar las operaciones y reportar aquellas que se consideran sospechosas es una labor de equipo que requiere del apoyo de todos aquellos funcionarios que dentro de sus funciones tienen contacto con los clientes y las operaciones.

El reporte no es subjetivo. Las autoridades de supervisión establecen unas guías generales para analizar y reportar las operaciones sospechosas. Entre otros aspectos se establece que la entidad debe conocer el cliente y el mercado para concluir que la operación es sospechosa. Además, la entidad debe contar con herramientas más complejas como señales de alerta, segmentos de mercado y perfiles de clientes para detectar las operaciones sospechosas. Por estas razones, cuando la entidad decide reportar una operación, debe hacerlo con argumentos y análisis, así éstos no tengan el rigor jurídico que exige la ley para probar el delito de lavado de activos.

Concepto de factores de riesgo

Los factores de riesgo son las circunstancias y características del cliente y la operación que hacen que exista una mayor probabilidad de corresponder con una operación sospechosa de lavado de activos.

Es importante aclarar que los factores de riesgo no constituyen una herramienta aislada para la determinación de operaciones sospechosas. Se trata simplemente de un instrumento que debe ser complementado con un estudio de las operaciones particulares, antes del reporte correspondiente.

La entidad al determinar y fijar la política de "conocimiento del cliente" debe evaluar los riesgos de los futuros clientes de conformidad con los diferentes "factores de riesgos" a los cuales pueden estar expuestos.

Ejemplos de factores de riesgo

Los principales factores de riesgo que se emplean en la entidad para controlar el lavado de activos son:

Según las contrapartes

- Actividad económica del cliente.
- Zona geográfica donde realiza las transacciones.

Según los servicios:

- Monto o valor de la transacción.
- Tipo de operación, servicio.
- Complejidad.

Actividad económica del cliente

Al estudiar las modalidades y los métodos de lavado de activos se observa que ciertas actividades son mejor fachada para el lavado que otras. Por esta razón, la entidad debe conocer actividades que por su poca supervisión, el uso de efectivo, u otros aspectos, implican mayor riesgo de lavado de activos.

Zona geográfica donde realiza negocios el cliente

La ciudad, la región y el país de donde provienen o terminan los recursos de los clientes pueden implicar riesgos particulares a los cuales la entidad debe prestar atención.

Tipo de operación, producto o servicio

Así como el negociante legítimo prefiere ciertos productos por ser más rentables o atractivos para su negocio, el lavador conoce los productos que le facilitan su labor y le aseguran sus objetivos criminales. Las remesas y transacciones electrónicas, son un ejemplo de productos que implican un mayor riesgo y por lo tanto deben ser catalogados como factores de riesgo.

Actividades y sectores vulnerables.

La entidad debe prestar atención a las operaciones con clientes y establecimientos cuyas actividades sean vulnerables de ser utilizadas para operaciones de lavado de activos.

Se trata de actividades legítimas y por ello debe tener especial cuidado para no estigmatizar personas o empresas que se dedican a la realización de tales actividades.

Identificación de zonas vulnerables para el lavado de activos

Una zona vulnerable es un área geográfica de alto riesgo para la realización de operaciones de lavado de activos.

La idea de las organizaciones criminales es buscar áreas menos controladas por las autoridades, para cumplir con su objetivo final de darle apariencia de legalidad a los recursos obtenidos en operaciones ilícitas.

De ahí, que existan zonas que de antemano presentan un riesgo superior que otras y que se pueden identificar como zonas vulnerables para el lavado de activos.

- **Análisis de las operaciones**

Existen muchas oportunidades para analizar las operaciones y detectar operaciones inusuales o sospechosas. Al momento de realizarse la operación, el agente autorizado que la tramita está en una posición privilegiada para analizar la información disponible y definir si se trata de una operación inusual. Sin embargo, este control no es suficiente. Las operaciones deben ser analizadas en su conjunto para poder tener una mejor visión de la actividad del cliente y poder definir si sus operaciones son realmente sospechosas. Por esta razón, la entidad, realiza un análisis posterior con información histórica para detectar operaciones inusuales. Este tipo de análisis implica consolidar la totalidad de operaciones de un cliente en un período determinado, por ejemplo un mes o un año, y analizar estas operaciones en su conjunto. Consolidar las operaciones de un cliente frente a todas las oficinas de la entidad permite detectar operaciones inusuales que en otras circunstancias pasarían inadvertidas.

Herramientas y técnicas empleadas para el análisis de operaciones para la detección de lavado de activos.

- Análisis centrados en las operaciones
- Análisis centrados en los clientes

Análisis centrados en las operaciones

Consolidación de operaciones

La forma más simple de consolidación es tomar todas las operaciones de un cliente en un período. No obstante, existen otras formas de consolidación más complejas, las cuales pueden servir para detectar operaciones de lavado más especializadas. Por ejemplo, se pueden consolidar las operaciones por cliente, por grupo familiar y por grupo económico. A su vez, cuando se tiene sospecha sobre vínculos secretos entre dos personas, es de mucha utilidad consolidar sus operaciones como si fueran una sola persona para investigar su comportamiento.

Comparación de las operaciones con las señales de alerta establecidas.

Una vez se tiene una idea general de las operaciones realizadas por el cliente, éstas deben ser comparadas con las señales de alerta preestablecidas por la entidad con el fin de descubrir si existe similitud entre el comportamiento del cliente y los mecanismos comúnmente usados por los lavadores.

De esta forma se puede hacer un segundo control frente a las operaciones que deben ser detectadas por las oficinas.

Estudio de clientes y perfiles

Una vez se conocen las operaciones realizadas por un cliente en un período determinado, se puede analizar si estas operaciones corresponden con la información que se tiene sobre el cliente, en especial el perfil.

Estudio de segmentos

Las operaciones realizadas por la totalidad de los clientes se pueden agrupar mediante el sistema de segmentos, según los criterios más relevantes: tipo de operación, localización geográfica, volumen y frecuencia. De esta forma, la entidad puede definir unos grupos o segmentos que describen mercados homogéneos.

Los segmentos permiten comparar la evolución de un cliente frente a los segmentos. Por ejemplo un cliente que siempre realiza operaciones en un segmento puede modificar su comportamiento y realizar operaciones en otros segmentos. Este cambio de comportamiento debe tener algún tipo de justificación, de lo contrario se está frente a una operación sospechosa.

Otro análisis muy interesante que se puede realizar es la comparación entre la información que se tiene sobre los clientes y los segmentos en los cuales se enmarcan las operaciones. De esta forma, se pueden encontrar clientes que realizan operaciones en un segmento contradictorio, según la información del conocimiento del cliente.

Factores de Riesgo

La entidad debe definir previamente las operaciones que constituyen un factor de riesgo de lavado de activos. Son operaciones que requieren un control adicional, según el conocimiento que la entidad tiene del negocio y de las modalidades de lavado de activos. Al analizar las operaciones realizadas por sus clientes, la entidad debe establecer los factores de riesgo que están presentes en algunas de ellas, para estudiarlas más detenidamente o ejercer los controles previstos.

Comparación con empresas similares

El conocimiento del cliente no solamente sirve para conocer clientes individuales, también brinda información muy útil sobre ciertos sectores de la economía. Esta información debe ser utilizada para determinar si las transacciones realizadas por un cliente tienen sentido desde el punto de vista del negocio.

Seguimiento a la evolución de las operaciones del cliente y su información financiera

Pocos clientes realizan operaciones en forma regular y predecible. Por el contrario, el comportamiento de los clientes se caracteriza por su irregularidad y su impredecibilidad. Entre otros factores, los clientes suelen tener ingresos y egresos variables o extraordinarios sobre los cuales la entidad no tiene información suficiente para anticiparlos.

Pese a que las transacciones de los clientes no son regulares, la entidad debe hacer un seguimiento periódico de las mismas con el fin de detectar tendencias o rangos que se salgan de los parámetros de normalidad.

CAPITULO VI

SEÑALES DE ALERTA Y MÉTODOS DEL LAVADO DE ACTIVOS

- **Señales de alerta**

Las señales de alerta no es lo mismo que operaciones sospechosas. Las señales de alerta ayudan a identificar o detectar comportamientos, conductas, actividades, métodos o situaciones atípicas que pueden encubrir operaciones de lavado. Pero la presencia de ellas no significa estar frente a una operación sospechosa que debe ser objeto de reporte inmediato.

Simplemente debe llamar la atención para proceder al análisis detallado de la situación.

El estudio de esos métodos permite una mayor comprensión de las formas que suelen emplear las organizaciones criminales para ocultar sus dineros ilícitos.

Concepto básico de señales de alerta

Las señales de alerta como su nombre lo indica, muestran los comportamientos particulares de los clientes y las situaciones atípicas que presentan las operaciones y que pueden encubrir operaciones de lavado de activos. Hay que tener en cuenta que no todas las operaciones que presentan comportamientos atípicos e inusuales son operaciones ilegales, por tal razón, el hecho de identificar señales de alerta no significa que la operación deba ser reportada de manera inmediata y automática a las autoridades como sospechosa.

La señal de alerta facilita el reconocimiento de una operación de lavado que corresponde a los procesos característicos de los diferentes métodos adoptados por la delincuencia para el lavado de activos.

Las señales de alerta permiten identificar operaciones que presentan situaciones inusuales y que en algunos casos son operaciones de lavado. Las señales de alerta se identifican gracias al conocimiento que se tiene de los métodos de lavado. A su vez, el método de lavado se refiere a la operación completa desarrollada por el delincuente, desde que empieza su actividad ilegal, pasa por la entidad, hasta que concluye la operación; con el resultado que busca de dar apariencia de legalidad a los bienes o fondos obtenidos ilícitamente.

Las normas que exigen a la entidad a adoptar sistemas de prevención de lavado de dinero, normalmente solicitan o recomiendan incluir en los manuales de procedimientos de prevención listas de señales de alerta, que les sirvan a los empleados para detectar operaciones inusuales o atípicas, o conocer

operaciones sobre las cuales deben tener especial prudencia y cuidado. Las señales de alerta deben ser delineados la entidad, teniendo en cuenta la naturaleza de las operaciones que realiza el mercado que atiende.

Listado de señales de alerta

a. Señales de Alerta frente al perfil del cliente

- Operaciones que no están de acuerdo con la capacidad económica del cliente.
- Operaciones que aisladas o vinculadas escapan al perfil previsible o ya definido del cliente en cuestión.
- De un momento a otro una persona, sin fundamento, aparece como dueño de importantes negocios.
- Cuentas que tienen un gran volumen de transferencias electrónicas, cuando el titular de la cuenta no justifica esta actividad.
- Realización de varios envíos en el mismo día o mes en forma inusual, respecto al comportamiento habitual del cliente.
- Transferencias electrónicas, sin aparente razón comercial ni consistencia con los negocios habituales del cliente.
- Recepción de varias transferencias de pequeñas cuantías, que se transfieren a otra ciudad, cuando esta actividad no es consistente con los negocios del cliente.
- Clientes cuyos ingresos reflejan resultados muy diferentes frente a los otros del mismo

Señales de Alerta relacionadas con las operaciones internacionales

- Frecuente envío o recepción de transferencias electrónicas.
- Depósitos de recursos en varias cuentas, usualmente por debajo del monto para el registro de transferencias, para luego ser consolidados en una cuenta maestra.

Ejemplos de señales de alerta relacionados con empleados

- Empleados con un estilo de vida que no corresponde con el monto de su salario.
- Empleados renuentes a disfrutar vacaciones.
- Empleados renuentes a aceptar cambios de su actividad o promociones que impliquen no continuar ejecutando las mismas actividades.
- Empleados que impiden que otros compañeros de trabajo atiendan a determinados clientes.

- **Responsabilidad de las entidades financieras y sus empleados**

Es importante destacar que la responsabilidad de identificar y verificar las señales de alerta recae en primera instancia sobre la entidad y a su vez, sobre los agentes autorizados que controlan las operaciones normales y que son los que tienen contacto permanente con el cliente. Lo anterior, no pretende liberar de responsabilidad a los demás miembros de la organización que deben estar igualmente capacitados para reconocer las señales de alerta. De conformidad con lo anterior, las responsabilidades de control y vigilancia dependerían de las funciones que desempeñe cada individuo en la organización.

La capacitación oportuna y adecuada compromete a todos los empleados de la entidad en los procesos de identificación de las señales de alerta.

- **Beneficios de conocer y detectar las señales de alerta**

El conocimiento e identificación de las señales de alerta por parte de la entidad y sus empleados, hace parte de los esfuerzos que las autoridades y la entidad vienen desarrollando para prevenir que sus servicios prestados sean utilizados por la delincuencia para sus operaciones de lavado de activos.

Beneficios:

- Las señales de alerta permiten identificar cuando una operación se sale de lo cotidiano y se debe clasificar como inusual.
- Las señales de alerta facilitan el trabajo de control de operaciones de los empleados responsables

- La identificación oportuna de las señales de alerta y el adecuado seguimiento a la operación permiten con un margen de seguridad confiable, establecer si la operación es o no inusual o atípica.
- Es importante conocer las señales de alerta y tener un equipo capacitado para identificarlas y hacerles el respectivo seguimiento en el momento en que se presentan.
- **Métodos para lavado de activos**

¿Qué son los métodos para el lavado de activos?

Los métodos de lavado son los procesos adoptados por los delincuentes para transformar sus fondos y bienes productos de actividades ilícitas en fondos y bienes con apariencia de legalidad, a través de la realización de operaciones que involucran a la entidad. Cuando los métodos usados son exitosos el lavador los adopta y los sigue utilizando frecuentemente en sus operaciones de lavado de activos.

Los lavadores de activos buscan adoptar comportamientos similares a los de los empresarios legales para no despertar sospechas entre los empleados de la entidad y así burlar el control de las autoridades competentes.

Importancia de conocer los métodos de lavado de activos

Conocer los métodos de lavados de activos, al igual que conocer y detectar las señales de alerta, es un compromiso de la entidad para prevenir que se involucren en operaciones de lavado de activos.

A continuación se exponen algunas de las razones más importantes de conocer los métodos de lavado de activos:

- Proteger el buen nombre de la entidad, ya que su prestigio está en juego si la delincuencia logra utilizarla para sus operaciones ilícitas. En la medida en que se conozcan los métodos de lavado de activos se hace más fácil detectar este tipo de operaciones.
- Evita complicaciones de tipo legal a la entidad
- Contribuye al reconocimiento internacional de cada país, como país cooperante en la lucha para la prevención del lavado de dinero y activos.

Plan Anual de Capacitación

ElectroniCash, S.A.



PLAN DE CAPACITACIÓN

a. Introducción

La base sobre la cual descansa un buen sistema de prevención contra el lavado de dinero y de activos y financiamiento al terrorismo es un adecuado y eficiente conocimiento del cliente y además lo acompaña un buen proceso de capacitación de inducción adecuado y constante especialmente del personal que tiene contacto directo con el cliente. Tal y como está establecido en la Ley de supervisión y regulación del Sistema Financiero, incorpora el plan de capacitación general de la entidad, jornadas de capacitación en prevención contra el lavado de dinero y activos.

Este plan de capacitación ha sido planteado partiendo de los perfiles del personal y funcionarios a los cuales será dirigido, definiendo el alcance de la temática para cada uno de ellos. El plan cuenta con tres grupos de perfiles: el primero orientado al personal operativo que tiene contacto directo con el cliente, es decir los agentes autorizados; el segundo grupo las jefaturas y gerencias, y el tercer grupo a la dirigencia. Así mismo, se propone un contenido mínimo para la formación del Oficial de Cumplimiento y el Auditor Interno, como responsables de la ejecución y supervisión del cumplimiento de la Ley respectivamente.

El riesgo de lavado de dinero y de activos y financiamiento al terrorismo es un aspecto que debe ser tratado de forma integral, es decir debe valorarse partiendo de la premisa que la prevención es tarea de todos los empleados al interior de la entidad, cada cual en su rol, por lo anterior la ejecución de este plan de capacitación deberá coordinarse con el departamento de Recursos Humanos y Gerencia General. El plan de capacitación está orientado a fortalecer las competencias del personal, en la gestión del lavado de dinero y de activos, el cual deberá ser ejecutado atendiendo la debida diligencia, comprometiéndose la administración a garantizar la asistencia del personal en las jornadas programadas. Tal como está establecido en el instructivo de la Unidad de Investigación Financiera de la Fiscalía General de la República, debiendo expedirse las respectivas constancias correspondientes sobre el proceso de capacitación e inducción, así como los compromisos que los empleados deben manifestar respecto del conocimiento y acatamiento de las disposiciones legales y normativas dictadas por la UIF en su instructivo, así como la normativa interna dispuesta por la oficina de cumplimiento de la entidad.

El plan además tiene incluidas las correspondientes jornadas de inducción al personal que está ingresando a la entidad con temas específicos especialmente orientados al cumplimiento de las disposiciones internas en materia de procesos y procedimientos de control que procuran minimizar de manera eficiente y eficaz el riesgo de LD/FT. Así mismo, bajo el formato de reuniones jornadas de

divulgación de los principales aspectos del entorno que afecten directa o indirectamente a la entidad en materia de prevención del lavado de dinero y de activos.

El plan no tiene especifico de ejecución, sino se prevé sea ejecutado conforme la disponibilidad de tiempo del personal y del presupuesto asignado por la alta dirección.

b. Justificación

A continuación se presenta la base legal que justifica la elaboración y ejecución del presente plan de capacitación:

En el artículo 10 literal c) de la Ley contra el lavado de dinero y de activos está establecido como obligaciones de las entidades sometidas al control de la misma capacitar al personal sobre los procesos o técnicas de lavado de dinero y de activos, a fin de que puedan identificar situaciones anómalas o sospechosas.

De la misma manera el Art. 4 literal e) del Reglamento de la Ley establece que para la aplicación y funcionamiento de la Ley las instituciones deberán: Recopilar documentación bibliográfica sobre el lavado de dinero y de activos, y establecer programas permanentes de capacitación para los miembros de su personal, tanto en lo relativo a procesos y técnicas de lavado de dinero y de activos, como en la forma de reportar oportunamente a quien corresponda, en forma razonada y documentada, los casos en que, en el desempeño de sus cargos, detecten situaciones irregulares o sospechosas.

En cuanto el capítulo VII capacitación y difusión del instructivo de la Unidad de investigación Financiera en la cláusula novena establece que: Las instituciones estarán obligadas a desarrollar programas de capacitación y difusión al personal responsable de la aplicación de las disposiciones, expidiendo las constancias correspondientes, para lo cual deberán:

- I. Efectuar una vez al año, con independencia de lo establecido en los incisos e) y f), cursos o reuniones de información especialmente cuando se modifique el contenido de las disposiciones o de los formatos de transacciones en efectivo y reportes de operaciones sospechosas;
- II. Elaborar instructivos para facilitar a su personal el llenado de los formularios de transacciones en efectivo y reporte de operaciones sospechosas;
- III. Difundir las presentes disposiciones entre los empleados y funcionarios responsables de su aplicación, así como el presente instructivo y las normas internas que emita el Oficial de Cumplimiento, para el debido cumplimiento de dichas disposiciones;

- IV. Identificar y difundir entre el personal, las prácticas de clientes o usuarios de las instituciones que se hayan considerado como sospechosas por el Oficial de Cumplimiento;
- V. Dar a conocer a los empleados y funcionarios de nuevo ingreso, a las áreas de relación con el público y manejo de recursos el contenido de las presentes disposiciones y las prácticas de las instituciones al respecto;
- VI. Incorporar a su programa de capacitación y difusión las observaciones y recomendaciones de la autoridad competente;
- VII. Los empleados y funcionarios deben manifestar por escrito su conocimiento de las disposiciones de este instructivo y de las prácticas de la institución en la materia, así como de la obligación que pueda representarles; y
- VIII. Las instituciones orientarán y brindarán el apoyo que requieran sus empleados, para que estos puedan cumplir con las obligaciones derivadas de este instructivo.”

c. Objetivos

- **Objetivo general**

Tener a total disposición un instrumento para gestionar la formación de competencias que se le debe impartir al personal en materia de prevención contra el lavado de dinero y de activos, a través de la ejecución programada de jornadas de capacitación e inducción, que contribuya a formar una cultura de cumplimiento y prevención en la entidad, así como a cumplir con las disposiciones legales y normativas vigente en El Salvador.

- **Objetivos Específicos**

- ✓ Promover una cultura de cumplimiento en la entidad, mediante la formación de los cuerpos gerenciales en materia de gestión de riesgo lavado de dinero y de activos, con el fin de asumir el compromiso de cumplimiento de la ley y sus instrumentos conexos.
- ✓ Potenciar las competencias del personal en materia de gestión del riesgo de lavado de dinero y de activos, a través de la divulgación de la normativa vigente, disposiciones internas, así como en técnicas y métodos de lavado de dinero y de activos, a fin de que el personal sea capaz de identificar y reportar oportunamente operaciones o transacciones irregulares o sospechosas.
- ✓ Fortalecer las competencias del personal y funcionarios responsables de la ejecución y supervisión de las disposiciones legales vigentes en la entidad, mediante un proceso de formación especializado en materia de prevención y gestión del riesgo de lavado de dinero y de

activos, a fin de garantizar el correcto y oportuno cumplimiento de la ley y sus instrumentos conexos.

d. Políticas de capacitación

Con el propósito de dar cumplimiento a lo establecido en el marco legal y normativo la alta gerencia acuerda las siguientes políticas en materia de capacitación e inducción sobre la prevención del lavado de dinero y de activos, que son de obligatorio cumplimiento para todo el personal y dirigencia:

- I. El Oficial de Cumplimiento de la entidad deberá presentar a Junta Directiva el plan de capacitación anual sobre prevención de lavado de dinero y de activos a más tardar el quince de diciembre de cada año a fin de que este pueda asignar el presupuesto necesario para su ejecución.
- II. Todo el personal y dirigencia de la entidad está en la obligación de asistir a las jornadas de capacitación incluidas en el presente plan, y las que se programen fuera de este por parte del Oficial de Cumplimiento de la entidad según sea necesario y previa aprobación de la Alta Gerencia.
- III. Toda inasistencia a una o varias jornadas de capacitación deberá ser justificada, estando el funcionario o empleado en la obligación de asistir a la próxima jornada sobre el tema impartido, solicitando previamente el material de la jornada pendiente para su estudio.
- IV. El Oficial de Cumplimiento es el responsable de ejecutar el presente plan en las fechas establecidas. Cualquier reprogramación deberá ser justificada con anticipación. El Oficial de Cumplimiento podrá hacer uso de expertos en la materia para impartir algunos temas que estén fuera de sus competencias, para lo cual deberá contar con la aprobación de la Alta Gerencia.
- V. La Junta de Directiva verificará el cumplimiento a cabalidad del presente plan, verificando que la asistencia a cada jornada sea requerida según el perfil de cada grupo.
- VI. El Oficial de Cumplimiento certificará cada jornada de capacitación y obtendrá el compromiso expreso de cada empleado sobre el conocimiento adquirido y de la aplicación de los procedimientos e instrucciones emitidas por la oficina de cumplimiento según sea el caso.
- VII. El Oficial de Cumplimiento hará la inducción correspondiente al personal de nuevo ingreso en la entidad, sobre los procesos y procedimientos de control establecidos en materia de prevención contra el lavado de dinero y de activos.
- VIII. El Oficial de Cumplimiento podrá dar a conocer entre los empleados los casos considerados y reportarlos como operaciones sospechosas a la UIF, mas sin embargo, deberá siempre guardar

la confidencialidad de los datos generales del cliente, para lo cual adecuará el material correspondiente para efectos didácticos. El Oficial de Cumplimiento informará trimestralmente la Junta Directiva sobre la ejecución del plan de capacitación.

e. Metodología de capacitación

Para el desarrollo del presente plan de capacitación el Oficial de Cumplimiento aplicará las siguientes modalidades de capacitación, según los objetivos trazados en cada jornada.

f. Reuniones focalizadas

Las reuniones forzadas tendrá como propósito divulgar las políticas, procesos, procedimientos, instructivos y demás disposiciones emitidas por el Oficial de Cumplimiento, así como las actualizaciones en la normativa emitida por la Unidad de Investigación Financiera, especialmente para las áreas que tiene contacto directo con el cliente, tanto en la oficina central como en las sucursales.

Estas jornadas se realizarán con programación y muy buena coordinación en el horario normal de trabajo. La característica principal es que son jornadas con propósitos específicos y unidades específicas. En cada jornada de capacitación es obligación la entrega del material de apoyo correspondiente, ejemplo: refuerzo de cumplimiento de lo establecido y llenado de declaraciones juradas.

g. Jornadas de capacitación

En el marco de esta modalidad deberán tratarse temas más integrales como por ejemplo: divulgación de la Ley contra el lavado de dinero y activos y su Reglamento, y del instructivo de la UIF, así como otras leyes relacionadas, como por ejemplo: Ley especial contra actos de terrorismo, Ley relativa a las drogas, entre otras, capacitación en aspectos generales del lavado de dinero (conceptos, características, instituciones internacionales de prevención, etc.), así como en tipologías de lavado y señales de alerta.

Las capacitaciones se realizarán en jornadas de dos horas, las cuales deberán ser impartidas por el Oficial de Cumplimiento o él debe de auxiliarse de un experto según el tema de agenda.

h. Talleres

Los talleres serán un medio para fortalecer las competencias del personal de atención al cliente, técnica, mercadeo y ventas, caja y todos aquellos que tienen contacto con el cliente en temas como tipologías de lavado de dinero y señales de alerta.

Los talleres podrán tener una duración de tres horas, los cuales estarán a cargo del Oficial de Cumplimiento o un experto en la materia. Para dichos talleres el Oficial de Cumplimiento podrá auxiliarse de casos reales ocurridos en la misma entidad. De medios de comunicación, o de los casos ya documentados por organismos internacionales como el GAFI, GAFISUD, GRUPO EGMONT, entre otros, en sus informes de tipologías.

i. Grupos de trabajo

La metodología de trabajo requiere gestionar la capacitación según los perfiles de cada puesto o nivel de responsabilidad según la estructura organizativa, de tal forma que por cada grupo se asignarán los temas necesarios para un mejor desempeño de las funciones y responsabilidades asignadas en el sistema de prevención.

j. Cronograma de actividades

Actividades a desarrollar	Metodología
<p>Aplicación de la Ley contra el lavado de dinero y activos.</p> <ul style="list-style-type: none"> • Generalidades • Antecedentes • Tipologías • Penalidades 	<p>El oficial de cumplimiento programara capacitaciones al personal de la empresa y a los agentes autorizados una vez al año.</p> <p>La capacitación durara tres días finalizando con una evaluación de los contenidos aplicados.</p>
<p>Financiamiento al terrorismo.</p> <ul style="list-style-type: none"> • Antecedentes históricos • ¿Cómo identificarlo? • Medidas a seguir 	<p>El oficial de cumplimiento impartirá un capacitación anual para los empleados y Agentes Autorizados la cual tendrá una duración de un día al finalizar se realizara una evaluación sobre el tema</p>
<p>Políticas y procedimientos para la prevención de lavado de dinero y financiamiento al terrorismo.</p>	<p>La oficialía de cumplimiento brindara una capacitación anual al personal involucrado en la gestión de los riesgos sobre cómo aplicar las políticas y procedimientos, se realizara una evaluación con casos prácticos.</p>
<p>Rol del Oficial de Cumplimiento</p> <ul style="list-style-type: none"> • Generalidades 	<p>El oficial de cumplimiento brindara una capacitación anual al nuevo personal de entidad sobre las funciones</p>

Actividades a desarrollar	Metodología
<ul style="list-style-type: none"> • Funciones 	y la importación del oficial de cumplimiento en la entidad
<p>Debida diligencia</p> <ul style="list-style-type: none"> • Conceptos • Procedimientos para llevar a cabo la debida diligencia • Penalidades 	La oficialía de cumplimiento prepara una capacitación dinámica donde se muestren los procedimientos de debida diligencia y la importancia de estos. Con una evaluación
<p>Taller de casos de lavado de dinero</p>	Al final de las capacitaciones antes mencionadas se llevara a cabo un taller en el que aplicaran todo lo aprendido en casos reales y se evaluara su desempeño ante las situaciones presentadas.

PARTE III.III – PERSONAS RELACIONADAS <input type="checkbox"/> NO SE ENCONTRARON PERSONAS RELACIONADAS EN ESTA ENTIDAD		
Tipo De Relación: (*)		
F. Nacimiento / Insc. Cnr:	Primer Nombre (**):	
Segundo Nombre:	Apellidos (**):	
Apellido De Casada:	Tipo De Persona (*): <input type="checkbox"/> Natural <input type="checkbox"/> Jurídica	Sexo: <input type="checkbox"/> M <input type="checkbox"/> F
Razón Social (***):	Estado Civil: <input type="checkbox"/> Casado(a) <input type="checkbox"/> Soltero(a) <input type="checkbox"/> Divorciado(a) <input type="checkbox"/> Viudo(a)	
Tipo De Documento 1(*):	No. De Documento 1 (*):	F. Exp. 1:
Tipo De Documento 2:	No. De Documento 2:	F. Exp. 2:
Tipo De Documento 3:	No. De Documento 3:	F. Exp. 3:
Tipo De Documento 4:	No. De Documento 4:	F. Exp. 4:
Actividad: (*)	Lugar De Nacimiento:	
Nacionalidad:	País De Nacimiento:	
Residencia:	No. Permiso Residencia:	
Método De Identificación De Identidad: <input type="checkbox"/> Cliente Conocid <input type="checkbox"/> Empresa O Sociedad Conoc <input type="checkbox"/> Se Examinó Documento		
Observaciones:		

PARTE III.III – PERSONAS RELACIONADAS <input type="checkbox"/> NO SE ENCONTRARON PERSONAS RELACIONADAS EN ESTA ENTIDAD		
Tipo De Relación: (*)		
F. Nacimiento / Insc. Cnr:	Primer Nombre (**):	
Segundo Nombre:	Apellidos (**):	
Apellido De Casada:	Tipo De Persona (*): <input type="checkbox"/> Natural <input type="checkbox"/> Jurídica	Sexo: <input type="checkbox"/> M <input type="checkbox"/> F
Razón Social (***):	Estado Civil: <input type="checkbox"/> Casado(a) <input type="checkbox"/> Soltero(a) <input type="checkbox"/> Divorciado(a) <input type="checkbox"/> Viudo(a)	
Tipo De Documento 1(*):	No. De Documento 1 (*):	F. Exp. 1:
Tipo De Documento 2:	No. De Documento 2:	F. Exp. 2:
Tipo De Documento 3:	No. De Documento 3:	F. Exp. 3:
Tipo De Documento 4:	No. De Documento 4:	F. Exp. 4:
Actividad: (*)	Lugar De Nacimiento:	
Nacionalidad:	País De Nacimiento:	
Residencia:	No. Permiso Residencia:	
Método De Identificación De Identidad: <input type="checkbox"/> Cliente Conocid <input type="checkbox"/> Empresa O Sociedad Conoc <input type="checkbox"/> Se Examinó Documento		
Observaciones:		

NOTA

(*) Campo obligatorio
 (**) Campo obligatorio para personas naturales
 (***) Campo obligatorio para personas jurídicas
 (día/mes/año) Formato para fecha

No. Cta Orig:	No. Cta Dest:	Monto En Moneda Local:
Monto: (*)	Monto Destino:	Fecha Operación:
Beneficiario:		

Tipo De Instrumento: (*)		No. De Operación:
Moneda: (*)	Entidad Origen:	Entidad Destino
Suc. Origen:	Suc. Destino:	Relación: <input type="checkbox"/> Directa <input type="checkbox"/> Indirecta
No. Cta Orig:	No. Cta Dest:	Monto En Moneda Local:
Monto: (*)	Monto Destino:	Fecha Operación:
Beneficiario:		

Tipo De Instrumento: (*)		No. De Operación:
Moneda: (*)	Entidad Origen:	Entidad Destino
Suc. Origen:	Suc. Destino:	Relación: <input type="checkbox"/> Directa <input type="checkbox"/> Indirecta
No. Cta Orig:	No. Cta Dest:	Monto En Moneda Local:
Monto: (*)	Monto Destino:	Fecha Operación:
Beneficiario:		

Tipo De Instrumento: (*)		No. De Operación:
Moneda: (*)	Entidad Origen:	Entidad Destino
Suc. Origen:	Suc. Destino:	Relación: <input type="checkbox"/> Directa <input type="checkbox"/> Indirecta
No. Cta Orig:	No. Cta Dest:	Monto En Moneda Local:
Monto: (*)	Monto Destino:	Fecha Operación:
Beneficiario:		

Tipo De Instrumento: (*)		No. De Operación:
Moneda: (*)	Entidad Origen:	Entidad Destino
Suc. Origen:	Suc. Destino:	Relación: <input type="checkbox"/> Directa <input type="checkbox"/> Indirecta
No. Cta Orig:	No. Cta Dest:	Monto En Moneda Local:
Monto: (*)	Monto Destino:	Fecha Operación:
Beneficiario:		

NOTA

Se deberán completar con las transacciones que se relacionen con la operación reportada. En caso de ser necesario se deberá continuar en otra página, completando en todos los casos el número de página y el total de estas y si no tiene operaciones dentro de esta entidad marcar el cuadro que esta en la parte superior derecha.

(*) Campo obligatorio
 (**) Campo obligatorio para personas naturales
 (***) Campo obligatorio para personas jurídicas
 (día/mes/año) Formato para fecha