UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

“GESTIÓN DE RIESGOS PARA PREVENIR OPERACIONES ILÍCITAS EN LAS SOCIEDADES PROVEEDORAS DE DINERO ELECTRÓNICO UBICADAS EN EL DEPARTAMENTO DE SAN SALVADOR”

TRABAJO DE INVESTIGACIÓN PRESENTADO POR:

ÁLVAREZ DOMÍNGUEZ, NYREE EUNICE

FLAMENCO GARCÍA, JOSÉ DANIEL

GODÍNEZ MORALES, RAÚL ALFREDO

PARA OPTAR AL GRADO DE:

LICENCIADOS EN CONTADURÍA PÚBLICA

MARZO 2019

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA

AUTORIDADES UNIVERSITARIAS

Rector	:	Msc. Roger Armando Arias Alvarado.
Secretario General	:	Lic. Cristóbal Hernán Ríos Benítez.
Decano de la Facultad de Ciencias Económicas	:	Lic. Nixon Rogelio Hernández Vásquez.
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 de Hernández.
Coordinador General del Seminario de Graduación	:	Lic. Mauricio Ernesto Magaña Menéndez.
Coordinador del Seminario de Graduación de la Escuela de Contaduría Pública	:	Lic. Daniel Nehemías Reyes López.
Docente Director	:	Lic. José Gustavo Benítez Estrada.
Jurado Examinador:	:	Lic. Daniel Nehemías Reyes López. Lic. José Gustavo Benítez Estrada. Lic. Carlos Nicolás Fernández Linares.

Marzo 2019.

San Salvador, El Salvador, Centroamérica.

AGRADECIMIENTOS

Felizmente agradecido con Dios por haberme brindado salud, sabiduría, fortaleza y perseverancia para poder culminar mi carrera profesional.

A mi madre por su amor, apoyo incondicional, esfuerzo, y la confianza depositada en mí. A mi abuela Margarita por todo su amor. A mis hermanos: David, Claudia, César, Norma y Regina, porque de distintas formas me han apoyado durante toda esta etapa. A mi novia Angélica por su apoyo y comprensión en los momentos más difíciles de esta carrera y su motivación para seguir siempre adelante. A toda mi familia y amigos, por la confianza, sus palabras de ánimo y por cada ayuda que me brindaron. A mis compañeros de trabajo de graduación Raúl y Eunice, por todo su esfuerzo y dedicación para poder culminar con éxito este proceso. A todos, que Dios los bendiga.

José Daniel Flamenco García.

Doy gracias especialmente a mi madre, a mi padre que me observa desde los cielos y mis hermanos Fannye y Ángel por todos sus esfuerzos para guiarme y ayudarme en la finalización de mi carrera profesional. Además, doy gracias a mi esposo Raúl y a mi hija Arianna que en este último año se convirtieron en mi inspiración y a todas aquellas personas que conocí y que me ayudaron en momentos difíciles para seguir adelante durante mi carrera como: Daniel, Rony, Katherine, Yuri, Arely, Marcela, Joaquín y Olivia.

Nyree Eunice Álvarez Domínguez.

Al Creador y señor de todo lo que conozco y lo que me falta por descubrir, por regalarme la oportunidad de estar acá, después vivir tantas experiencias desde aquel momento en que decidí emprender este viaje, permitiéndome coincidir con tantas personas que han hecho de mi vida una experiencia extraordinaria, iniciando por mi padre Raúl Godínez (El médico de la familia), por regalarme de él, todo lo que es; a mi madre Eleonora Morales de quien estaré eternamente enamorado; a mi esposa Nyree Álvarez por aceptarme como soy, junto a quien quiero envejecer y por último a Arianna, nuestra princesa, quien con solo su existencia complementa todo lo que necesito para ser feliz.

Raúl Alfredo Godínez Morales

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN EJECUTIVO

Los avances tecnológicos y su papel en las formas de realizar el comercio dieron origen a la creación de las plataformas de dinero electrónico, éstas ayudarían a simplificar los procesos de pago, adquisición de bienes y/o servicios y se realizarían de una forma más segura para los usuarios. Sin embargo, con el paso del tiempo, estos canales electrónicos fueron objeto de aprovechamiento por grupos de personas criminales para cometer ilícitos; a raíz de esa situación se estudió la problemática de cómo afecta a los proveedores del servicio de dinero electrónico no contar con un modelo que ayude a la prevención de operaciones ilícitas en sus plataformas.

Debido a lo expuesto anteriormente, el trabajo de investigación tiene por objetivo diseñar un modelo de gestión de riesgos que contribuya a prevenir operaciones ilícitas en las Sociedades Proveedoras de Dinero Electrónico, con la finalidad que éstas puedan tener un guía para mitigar los riesgos relacionados al lavado de dinero y activos y financiamiento al terrorismo.

La indagación fue realizada en base al enfoque no experimental longitudinal, el cual se centra básicamente en la tendencia del problema dentro del periodo seleccionado, para el que fue necesario emplear un estudio de tipo descriptivo en el que se utilizaron técnicas e instrumentos como entrevista y recopilación bibliográfica de la problemática, los cuales permitieron identificar riesgos, evaluarlos y medir su probabilidad de ocurrencia como de impacto, y a su vez permitieron establecer las siguientes conclusiones:

Si bien es cierto se cuentan con parámetros para determinar que una operación en los medios electrónicos pueda ser catalogada como inusual y posteriormente sospechosa, existe el riesgo que estos sean burlados por empleados o personas ajenas a la empresa que tengan conocimiento de ellos.

Las empresas proveedoras de dinero electrónico deben realizar capacitaciones constantes en materia de prevención de lavado de dinero y financiamiento al terrorismo, ya que, al no ser periódicas, los empleados se vuelven vulnerables de caer en complicidad al conocer los procesos de operación de las plataformas electrónicas.

Se considera de importancia documentar todas las transacciones que se realizan a través de estos medios, ya sea física o electrónicamente, con el fin de dar cumplimiento a los requerimientos que en determinados momentos pueda realizar la Superintendencia del Sistema Financiero o la Fiscalía General de la República, en relación a la prevención de lavado de dinero y financiamiento al terrorismo.

A partir de las conclusiones mencionadas, es recomendable implementar un modelo de gestión de riesgos que ayude en la prevención de operaciones ilícitas en cada una de las áreas involucradas en las empresas proveedoras de dinero electrónico.

INTRODUCCIÓN

En El Salvador las Sociedades Proveedoras de Dinero Electrónico han ido ampliando la gama de operaciones que pueden realizar a través de sus diferentes plataformas, desde enviar dinero hacia otra parte del territorio, realizar el pago de diferentes colectores y hasta recibir remesas internacionales únicamente con el uso de un dispositivo móvil. Sin embargo, este tipo de servicios requiere de un sistema de control eficiente que permita mitigar los riesgos a los cuales están expuestos, por medio de herramientas que ayuden a mitigarlos.

El presente trabajo se estructuró en cuatro capítulos, los cuales se describen a continuación:

El capítulo I describe el planteamiento de la problemática a través de sus antecedentes y las características de ésta.

Posteriormente en el capítulo II, se analizó el estado actual de las empresas proveedoras de dinero electrónico, así como la operatividad de éstas y su funcionamiento, se evaluó además las ventajas y desventajas de este tipo de servicios.

Asimismo, se referenció al marco legal, técnico y normativo de la investigación para dar una respuesta a la problemática objeto de estudio.

En el capítulo III se estableció la metodología de investigación, el tipo de la misma, las unidades de análisis, universo y muestra, los instrumentos y técnicas utilizadas en la indagación, así como el análisis de los resultados obtenidos, finalizando con un diagnóstico del control interno de las empresas proveedoras de dinero electrónico.

En el capítulo IV, se planteó una propuesta de solución de la problemática que, para este caso, es un modelo de gestión de riesgos que facilite la prevención de operaciones ilícitas en las operaciones realizadas por las Sociedades Proveedoras de Dinero Electrónico.

Finalmente se establecieron las conclusiones y recomendaciones de los resultados obtenidos de la investigación, la bibliografía y los anexos de este estudio.

CAPÍTULO I

1. PLANTEAMIENTO DEL PROBLEMA

1.1. Situación problemática

El dinero electrónico y las plataformas de este servicio han sido de aceptación en diferentes partes del mundo debido a la facilidad para realizar transacciones financieras, tales como pagos, cobros y transferencias de dinero.

Su origen data del año 2001, en Japón, donde se implementó por primera vez en el sistema de transporte, creándose tarjetas de pago electrónicas que reducían el volumen de dinero físico manejado, y el cual, posteriormente se extendió en diferentes comercios de todo ese país.

La inclusión al mercado financiero de entidades dedicadas a otros sectores, como las de telefonía, dieron un paso importante al implementar plataformas digitales capaces de realizar operaciones de pago y transferencias de dinero de forma electrónica, dando con ello el origen a las primeras formas de lo que hoy en día conocemos como *Dinero Electrónico*.

Uno de los principales pioneros en Europa, fue España, y en Latinoamérica las primeras implementaciones se dieron en Ecuador, Colombia y Uruguay. De igual forma en Centroamérica, la aceptación fue rápida, esto debido a la facilidad con la que se manejaba el efectivo y se realizaban diferentes operaciones financieras, constituyéndose en El Salvador, la primera sociedad dedicada a este rubro, en el año 2011, trayendo consigo una serie de beneficios a la población que no tenía acceso al sistema bancario.

Este trabajo de investigación se realizó con la intención de dotar de procedimientos de control y así prevenir operaciones ilícitas en las plataformas virtuales, propiedad de las Sociedades Proveedoras de Dinero Electrónico radicadas en el departamento de San Salvador. Dicho

problema, básicamente consiste en utilizar estos medios, por personas o el crimen organizado, para cometer ilícitos de diferente índole.

Esta práctica ha obligado a las sociedades proveedoras de este tipo de dinero a que implementen nuevas prácticas y controles mucho más eficaces.

Desde que se detectó este problema en El Salvador, fue abordando interés por parte de la Fiscalía General de la República, iniciando un proceso que garantizaría mejor el control y la detección de este tipo de ilícitos. Pero por ser un tema relativamente nuevo, aún se siguen evaluando e implementando controles.

1.1.1. Caracterización del problema.

Las sociedades cuyo giro es el de proveer dinero electrónico, como cualquier otra, son vulnerables a riesgos, es por ello que es necesaria la dotación de controles que permitan prevenir operaciones ilícitas.

Partiendo de esto, la Superintendencia del Sistema Financiero, como ente supervisor y regulador de este tipo de empresas, en su afán de preservar una cultura financiera estable y transparente, supervisa la actividad individual y consolidada de estas sociedades, y fomenta la inclusión al sistema financiero de las micro y pequeñas empresas que no tenían acceso a los servicios bancarios, este escenario fue la base sobre la cual, posteriormente aprobó la Ley para Facilitar la Inclusión Financiera (Asamblea Legislativa, 2015) que ayudaría a dichos comercios a introducirse al conglomerado del sistema.

Pero la situación delincuencial existente en el país provocó que las plataformas de dinero electrónico se volvieran atractivas para cometer ilícitos.

Un refuerzo a los controles y la generación oportuna de informes pueden coadyuvar a la prevención de esa clase de operaciones dentro de estas plataformas.

Algunas de las características que describen el problema se mencionan a continuación:

- **Falta de guías de orientación:** Al no contar con un modelo de gestión de riesgos que ayude a la prevención de operaciones ilícitas, las plataformas de dinero electrónico se vuelven vulnerables, por lo que es necesario implementar una guía de control interno para orientar a las empresas proveedoras de este tipo.
- **Uso de medios legales**: la finalidad del delincuente es utilizar las plataformas de dinero electrónico para poner en circulación dinero ilícito dentro del sistema financiero, o utilizarlos solamente para hacer efectivo el cobro de una actividad delincuencial previa.
- **Monitoreo constante:** Por el fácil acceso y registro de usuarios, se vuelve atractivo este método de pago para cometer ilícitos, puesto que basta con tener un teléfono celular inteligente con acceso a la red de la compañía para operar en ella y hacer transacciones, algunos usuarios pueden perfectamente operar con movimientos ilegales, lo que conlleva a mantener un monitoreo básicamente siempre.
- **Seguridad en las tecnologías de la información:** los constantes avances de las Tecnologías de la Información (TI) requieren que las plataformas electrónicas garanticen la seguridad de los usuarios, por lo que se vuelve determinante prevenir cualquier riesgo que pueda afectar el buen uso de dichas plataformas.
- **Apoyo por parte de entidades vigilantes**: actualmente la Superintendencia del Sistema Financiero se encarga de autorizar y supervisar las operaciones realizadas por las Sociedades Proveedoras de Dinero Electrónico, pero ello por sí solo, no garantiza

que los controles sean aplicados adecuadamente, tanto en el registro de las sociedades proveedoras, como en la regulación de sus operaciones.

- **Desinformación generalizada**: El poco desarrollo y explotación de este mercado que según el Grupo de Acción Financiera de Sudamérica (GAFISUD) en su "Guía sobre los nuevos métodos de pago: tarjetas prepagas, pagos por telefonía móvil y pagos por internet" publicada en junio de 2013, considera que "(…) existe una carencia de información" respecto al tema que está directamente relacionada con el aún poco desarrollo mercado de los nuevos métodos de pago (NMPs)", esto puede traducirse en temor en la población o dudas sobre si su dinero está verdaderamente seguro en esta plataforma hasta lo que podría pasar en un escenario de calamidad o desabastecimiento energético.

Como respuesta se optó por un modelo que involucre el total de las variables objeto de estudio de manera separada, ya que no se encontraron antecedentes de investigaciones previas como referencia para abordar la temática.

1.1.2. La inclusión Financiera y el Dinero Electrónico – Década de 2000.

En Centroamérica, la inclusión financiera se ha venido discutiendo desde que tuvo aceptación en otros países de Latinoamérica como un sistema viable, económico e impulsador de la economía.

En este contexto, un estudio realizado por la Federación Latinoamericana de Bancos (FELABAN) publicado en su página oficial en octubre de 2016, refleja algunas situaciones puntuales sobre la situación financiera y el crecimiento del Sistema Bancario en El Salvador, que aunque lo cataloga como lento, considera que "(…) está avanzando en este camino"; señala que

"(…) los principales obstáculos que impiden la Inclusión Financiera son las barreras de tipo legal y de supervisión" (p.58); pudiendo traducirse este último, como la ausencia de un organismo que vigile el proceso.

La investigación reflejó, además, que "El Salvador se situaba, en el 2015, en el sexto lugar entre los países que menos saldo de cartera y de depósitos había percibido en su Sistema Financiero, con menos de 40 millones de dólares" (p.18).

1.1.3. Las operaciones ilícitas por medio del dinero electrónico.

Durante los años 2011, 2012 y 2013 la Fiscalía General de la República (FGR) y la Policía Nacional Civil (PNC) reportaron los primeros casos de operaciones ilícitas, los autores eran estructuras delictivas que, a través de este sistema, hacían efectivo el cobro de extorsiones, en ese entonces, poco o nada se hacía por las empresas proveedoras de dinero electrónico, quienes inicialmente eran ajenas al problema que se generaba.

Como antecedente en este contexto, se hizo importante mencionar el estudio realizado por el Consejo Nacional de la Pequeña Empresa en El Salvador (CONAPES, 2013), donde puntualizaba que "(…) el 40 % de las Pymes, lamentablemente eran víctimas de extorsión".

Cronológicamente, otro estudio realizado por "InSight Crime" (2015), fundación dedicada al estudio de la principal amenaza para la seguridad nacional y ciudadana en América Latina y El Caribe: El Crimen Organizado, señaló que solo ese año, "(…) los salvadoreños pagaron alrededor de unos US$400 millones al año por este delito, seguido por los hondureños, con unos US$200 millones, y los guatemaltecos, con alrededor de US$61 millones".

Según sus datos, "(…) el Triángulo del Norte (El Salvador, Guatemala y Honduras) constituía, para ese año, el epicentro mundial de la extorsión.

"InSight Crime" afirmaba que "los sectores más golpeados por este delito son, el transporte público, y las pequeñas empresas y enfatizaba en la importancia de este sector para la economía nacional", sosteniendo que "(…) más del 98 % de los negocios; alrededor del 47 % de las ventas nacionales, y aproximadamente 36 % del empleo en El Salvador, son generados por las micro y pequeñas empresas".

En este contexto, ese mismo año, el Estado salvadoreño aprobó la Ley para Facilitar la Inclusión Financiera, la cual regula las transacciones con dinero electrónico, así como a las sociedades proveedoras de este servicio, con el objeto de propiciar la inclusión financiera y fomentar la competencia en el Sistema Financiero.

Otra investigación realizada por el Instituto de Estudios Estratégicos y Políticas Públicas (IEEPP, 2015), refleja de nuevo que los países miembros del llamado "Triángulo Norte", siguen siendo los que más golpeados por el delito de extorsión, reiterando una vez más que, donde más se paga, sigue siendo en El Salvador, seguido por Guatemala y en el tercer lugar está Honduras.

Los estudiantes Catota, Cortez y Escobar (2017) de la Universidad de El Salvador, por medio de la Escuela de Contaduría Pública de la Facultad de Ciencias Económicas, en su trabajo de pregrado, en relación a este problema, sugieren un modelo de control interno que apoye a estas sociedades para advertir, prevenir y detectar el delito de Lavado de Dinero. Esa investigación, forjaba un precedente importante en la historia del Dinero Electrónico y su vinculación con el crimen organizado, centrándose exclusivamente en el origen de los fondos, pero dejaba fuera otros aspectos considerados también críticos, como es el destino y el movimiento de los mismos una vez dentro de la plataforma electrónica, lo cual constituye el escenario clave para el desarrollo de esta investigación.

1.2. Enunciado del problema

Dada las condiciones actuales del problema y el contexto en que se ha venido generando, se formuló la siguiente interrogante:

¿Cómo afecta a las Sociedades Proveedoras de Dinero Electrónico del departamento de San Salvador no contar con un modelo de gestión de riesgos para prevenir operaciones ilícitas?

1.3. Justificación de la investigación

Son muchas las razones para llevar a cabo esta investigación, la presencia en la vida cotidiana de los salvadoreños y el daño que las extorsiones ocasionan a las víctimas, son motivo para estudiar de manera profesional dicho problema. Y en base a los estándares propios de una investigación, se justificó tomando en cuenta los siguientes aspectos:

1.3.1. Novedoso.

El estudio se consideró novedoso, ya que si bien es cierto existe un trabajo relacionado al dinero electrónico, aquel se centró exclusivamente en el origen de los fondos (Lavado de dinero), a diferencia de éste el tema principal está enfocado al destino y movimiento de éstos una vez dentro de la plataforma electrónica, lo cual constituye un nuevo escenario que no ha sido abordado en ninguna investigación de la Universidad de El Salvador, ni en otras universidades del país y de ninguna otra fuente en particular, aparte los espacios noticiosos y demás medios de comunicación.

1.3.2. Factibilidad.

La investigación se consideró viable, tomando en que cuenta que, los recursos económicos que supone, los elementos técnicos implementados, la bibliografía consultada, así como los

equipos informáticos utilizados, se consideraron al alcance y disponibles cuando se necesiten, por lo que no fue un punto significativo que pudiera impedir la investigación.

Sumado a esto, se contó con el prestigioso apoyo de la Universidad de El Salvador, a través de la Escuela de Contaduría Pública, con el soporte y la orientación técnica, mediante la asignación de facilitadores que, desarrollando seminarios, contribuyen a la orientación metodológica de esta investigación.

El desarrollo de la investigación se realizó con recursos propios, financieros y tecnológicos.

1.3.3. Utilidad social

El estudio se consideró de importancia, pues además sumar al conocimiento actual relacionado con el tema y de ser aplicado, contribuye a reducir las operaciones ilícitas por medio de las plataformas de dinero electrónico.

Además, servirá como material didáctico para estudiantes de Licenciatura en Contaduría Pública y carreras afines, así como de complemento para la labor docente.

1.4 Objetivos de la investigación

1.4.1. Objetivo general.

Diseñar un modelo de gestión de riesgos que contribuya a prevenir operaciones ilícitas en las Sociedades Proveedoras de Dinero Electrónico del departamento de San Salvador.

1.4.2. Objetivos específicos.

- Obtener información sobre la existencia de controles en los puntos de entrega del dinero, para prevenir riesgos que contribuyen a que el dinero electrónico y su plataforma sean utilizados para realizar operaciones ilícitas.
- Identificar los factores que han originado cada riesgo en particular, para atender por separado las causas y las consecuentes manifestaciones.
- Determinar las características predominantes, mediante análisis de los riesgos identificados, como punto de partida para comprenderlos y abordarlos de manera acertada.
- Sugerir técnicas de diagnóstico y propuestas de mitigación, en respuesta a los riesgos identificados.
- Prevenir los riesgos que contribuyen a que el dinero electrónico y su plataforma sean objeto de operaciones ilícitas.

1.5 Hipótesis

1.5.1 Hipótesis de trabajo.

H_1. La implementación de un modelo de gestión de riesgos contribuirá a la prevención de operaciones ilícitas en los servicios prestados por las Sociedades Proveedoras de Dinero Electrónico.

1.5.2 Determinación de variables.

- Independiente: La implementación de un modelo de gestión
- Dependiente: Prevención de operaciones ilícitas en las Sociedades Proveedoras de Dinero Electrónico.

1.6 Limitaciones de la investigación

1.6.1 Teórica.

La investigación fue orientada a prevenir aquellas áreas de las Sociedades Proveedoras de Dinero Electrónico que tienen mayor riesgo, con el objeto de evaluar sus fortalezas y prevenir las posibles causas que las podrían volver vulnerables y que pudieran ser usadas para cometer ilícitos.

Para ello, se tomó como referencia, la normativa técnica vigente aplicable como guía y la legal como marco regulatorio aplicable a las empresas proveedoras de dinero electrónico, tanto las normas emitidas por el Banco Central de Reserva de El Salvador (BCR), así como la Ley para Facilitar la Inclusión Financiera, asimismo se aplicaron los lineamientos sugeridos por las Normas Prudenciales de Bancos respecto a la gestión de los riesgos como las “Normas para la Gestión Integral de Riesgos de las Entidades Financieras” (NPB4-47), “Normas de Gobierno Corporativo” (NPB4-48) y “Normas para la gestión de riesgo operacional de las entidades financieras” (NPB4-50).

1.6.2 Temporal.

La investigación comprendió el periodo a partir del cual, la problemática nació y se desarrolló (2011), debido a que, si bien es cierto, las operaciones sospechosas ya existían, es en

ese año donde se involucró en ellas el dinero electrónico. Además, se escogió tal periodo, para enmarcar la creación y entrada en vigencia de la Ley para Facilitar la Inclusión Financiera, aprobada en septiembre de 2015 y evaluar si esta contribuirá en reducir el problema; se estableció como fecha límite, la fecha actual (2018).

1.6.3 Geográfica.

El estudio abarcó específicamente a las Sociedades Proveedoras de Dinero Electrónico que, a la fecha (2018), se encuentran aprobadas o en proceso de aprobación y reguladas por la "Ley para Facilitar la Inclusión Financiera" de El Salvador la cual entró en vigencia en el año 2015, y radicadas en el departamento de San Salvador.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Estado actual

Los intermediarios financieros juegan un papel muy importante en la captación de dinero del público, pero con la globalización y la influencia de éste en el comercio se ha ampliado su papel, proporcionándole al dueño de los fondos, no solo su resguardo, sino además la posibilidad de realizar operaciones financieras nuevas como pagos a sus proveedores, recibir cobros de sus clientes, hacer transacciones de fondos entre cuentas propias y ajenas, incluso invertirlo para que gane intereses, con la sola apertura de una cuenta de ahorros.

Debido a los grandes avances tecnológicos, los sistemas financieros se han renovado, permitiendo el surgimiento de nuevas empresas, las cuales fueron creadas con el fin de facilitar a

sus diferentes usuarios el acceso a servicios modernos a través de plataformas electrónicas, dando como resultado la virtualización del comercio y el dinero.

El dinero electrónico es una nueva forma de pago, equivalente a utilizar dinero físico, simplificando las formas de realizar las operaciones y de una forma más segura; está orientado, principalmente a aquella población que, por su situación económica o localización geográfica, habían sido excluidas del sistema bancario.

En El Salvador, fue conocido por la población, apenas a inicios de la segunda década del tercer milenio, constituyéndose como un medio de pago informal, ya que a su entrada en vigencia aún no existía un marco regulatorio para las empresas que brindaban estos servicios, y su gran aceptación se debió a la misma que históricamente tuvo en otros países de la región.

El dinero electrónico fue tomando relevancia en la economía nacional a tal grado que el Estado se vio obligado a regular las operaciones y las empresas que prestaban este servicio, y en el año 2015 se aprobó la primera propuesta de Ley que controlaría su uso, dándole un carácter legal.

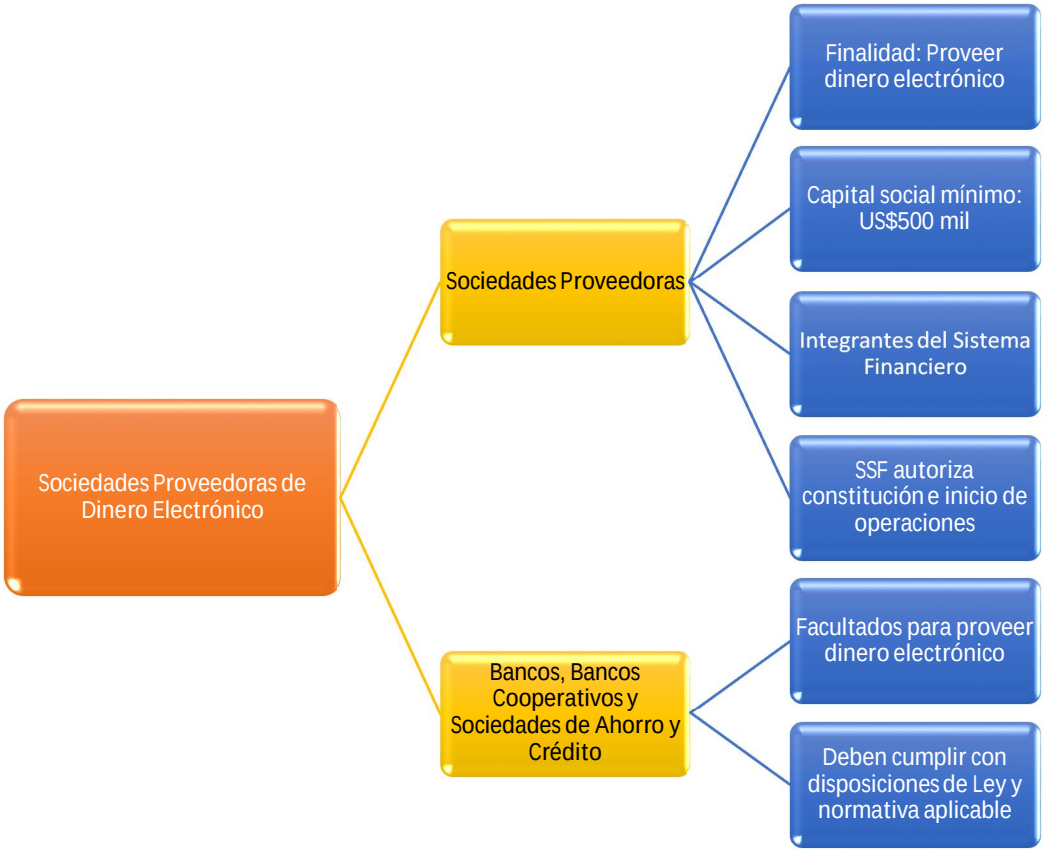
El Grupo de Acción Financiera Internacional (GAFI) ente internacional que vela por combatir prácticas financieras ilegales y el lavado a escala mundial, marca una diferencia entre el dinero electrónico y moneda virtual, definiendo esta última como "(…) una representación digital del valor que puede ser comercializada digitalmente y funciona como un medio de cambio; y/o una unidad de cuenta; y/o un depósito de valor, pero no tiene curso legal (cuando se ofrece a un acreedor, es una oferta válida y legal de pago) en ninguna jurisdicción. Ninguna jurisdicción emite o garantiza las monedas virtuales y cumple con las funciones antes mencionadas por común acuerdo de la comunidad de sus usuarios" distinta del dinero fiduciario (moneda legal, real o legal)

que es emitido por cada país como medio de pago legal, convirtiéndose en una representación digital de este.

Actualmente solo existe una sociedad proveedora de dinero electrónico legalmente autorizada en El Salvador, según consta en acta de sesión del Consejo Directivo de la Superintendencia del Sistema Financiero número CD-23/2018 celebrada el 21 de junio de 2018, en la cual autorizan a la Sociedad Proveedora de Dinero Electrónico Mobile Cash, Sociedad Anónima, a partir del día 1 de agosto de 2018, y en la misma instruyen a dicha sociedad a trasladar los fondos a la cuenta de depósitos en el Banco Central de Reserva de El Salvador, el cual respaldará el cien por ciento del dinero electrónico en circulación al inicio de sus operaciones.

Con la creación de la Ley para Facilitar la Inclusión Financiera se establecieron los requisitos, autorización y operación de las sociedades y bancos interesados en proveer dinero electrónico. (p.6)

Actualmente no existe ninguna institución bancaria que realice este servicio, sin embargo, pueden solicitar la autorización para proveer dinero electrónico, siempre y cuando cumplan con lo establecido en la Ley para llevar a cabo ese giro. En la Figura 1 se muestra quiénes son las proveedoras de dinero electrónico.



Fuente: *Banco Central del Reserva de El Salvador*

Figura 1. Esquema de las Sociedades Proveedoras de Dinero Electrónico en El Salvador. **Fuente especificada no válida.**

Según esta Ley, proveer dinero electrónico consiste en administrar los valores monetarios que reciben las sociedades que brindan este servicio, por medio de sus puntos de atención, y se almacenan en una plataforma informática para que estos sean aceptados como medio de pago por diferentes comercios, que a su vez están asociados por medio de contratos con los demás titulares que intervienen en el proceso.

Estas plataformas, como toda aplicación informática, deben cumplir con los principios de seguridad informática, para el resguardo de los fondos de cada usuario, aparte de esto, es importante mencionar que un ilícito puede llevarse a cabo, aun cumpliendo un protocolo de

seguridad informática, es decir, valerse de otros medios tradicionales para intimidar y obtener dinero de una víctima, utilizando una plataforma legal exclusivamente para hacer efectivo el cobro. Prevenir estas y otras posibles operaciones ilícitas que puedan afectar a los usuarios es el tema central de esta investigación.

2.2 Marco teórico

2.2.1 Inclusión financiera.

El Banco Mundial, define la Inclusión Financiera como "(…) el acceso que tienen las personas y las empresas a una variedad de productos y servicios financieros", catalogándolo además como "clave" para reducir la pobreza y e impulsar la prosperidad.

Su fin es, precisamente, incluir a aquellos sectores alejados de las urbes, cuyos miembros no tienen acceso a usar el Sistema Financiero, ya sea por tener un empleo informal o por el difícil acceso al Sistema.

2.2.2 Monedas virtuales.

Las monedas virtuales son definidas, según el Grupo de Acción Financiera Internacional – GAFI (2014) como: "Una representación digital del valor que puede ser comerciada digitalmente y funciona como (1) medio de cambio; y/o (2) unidad de cuenta; y/o depósito de valor, pero no tiene curso legal". Estos indican que el carácter legal de la misma lo determina el Gobierno de cada país, de acuerdo a ciertos criterios propios.

Monedas Virtuales no reguladas legalmente.

El GAFI (2014), divide las monedas virtuales no reguladas en dos partes:

- Convertibles: llamadas también abiertas, tomando esta calidad siempre y cuando participantes privados las oferten y otros la acepten, ya que la "convertibilidad" no está garantizada en lo absoluto por la ley, pero pueden ser intercambiadas, una y otra vez, por dinero real; como, por ejemplo: Bitcoin, e-Gold (fuera de uso), Liberty reserve, (fuera de uso), Second Life Linden Dollars y WebMoney. (p.5)
- No convertibles: llamadas también cerradas, y puede ser específica de un dominio o mundo virtual particular, como los videojuegos de rol multijugador excepcionales en línea (MMORPG, por sus siglas en inglés), o Amazon.com, en virtud de las normas que regulan su uso, no se puede cambiar por dinero real. Algunos ejemplos incluyen: Proyect Entropia Dollars, Q Coins y World of Warcraft Gold. (p.5)

De igual manera, el GAFI describe que todas las Monedas Virtuales no convertibles son centralizadas, es decir, tienen una autoridad administrativa única (administrador) que controla el sistema; mientras que las convertibles pueden ser tanto centralizadas como descentralizadas.

> "Las monedas descentralizadas (también conocidas como criptomonedas) son monedas virtuales de código abierto fundamentadas matemáticamente que funcionan en una red de pares distribuida, sin autoridad central administradora, de vigilancia o de supervisión". (GAFI, 2014, p.5)

Riesgos de Monedas Virtuales no reguladas legalmente.

La utilización de una moneda virtual no regulada legalmente, según el informe de la Autoridad Bancaria Europea (2013) trae consigo riesgos, destacando seis de ellos:

- Perder el importe depositado en las casas de intercambio por no disponer estas de un respaldo económico de los saldos.

- Robos o pérdidas de saldos depositados en monederos digitales, por ataques o por extravío de las claves o las contraseñas.
- Carecer de protección como medio de pago.
- El valor de las divisas cambia rápidamente y puede caer a valor nulo.
- Las transacciones con divisas virtuales pueden respaldar actividades ilícitas o blanqueo de capitales.
- Se puede incurrir en responsabilidades fiscales.

Los Nuevos Métodos de Pagos (NMPs)

El Grupo de Acción Financiera de Sudamérica (GAFISUD) en su "Guía sobre los nuevos métodos de pago: tarjetas prepagas, pagos por telefonía móvil y pagos por internet", publicado en junio de 2013, considera que "Los NMPs abarcan una amplia gama de productos que van desde meras extensiones del alcance de los sistemas de pago tradicionales a métodos totalmente nuevos. Acorde con la línea de trabajo del GAFI al respecto, este informe se centra en los siguientes NMPs: **Tarjetas Prepagas, Servicios de Pago Móvil y Servicios de Pago por Internet"** (p.6)

Tarjetas Prepagas

La mencionada guía se refiere a las Tarjetas Prepagas "(…) como una alternativa a las tarjetas de crédito y/o débito. Esta nueva modalidad de tarjeta mantenía las mismas prestaciones y funcionalidades que las tradicionales, pero sin necesitar una cuenta bancaria o una verificación de solvencia crediticia".

Las tarjetas prepagas pueden clasificarse en dos categorías principales: de ciclo abierto y de ciclo cerrado. En lo que concierne al LA/FT, son las tarjetas de ciclo abierto las que más nos interesan puesto que su gran funcionalidad comporta mayores riesgos.

La modalidad de ciclo cerrado abarca a las generalmente conocidas como “tarjetas regalo”; la mayor parte de estas tarjetas suele tener un menor alcance de uso, reduciéndose éste a un comercio. Las tarjetas regalo son anónimas, no están asociadas a una cuenta bancaria, y no permiten extraer efectivo ni realizar transacciones. Sin embargo, es preciso apuntar, que no por el hecho de tener un uso limitado están exentas del riesgo de ser utilizadas ilícitamente para operaciones de LA/FT. (p.7)

Servicios de Pagos por Internet

Según el GAFISUD, en su informe define que un servicio de pago por Internet “(…) es un STDV (servicio de Transferencia de Dinero o Valores) que permite a sus usuarios realizar operaciones en línea con el dinero virtual que previamente ha sido comprado o cargado en una cuenta prepaga. La estructura de un sistema de pago de este tipo requiere al cliente o usuario que se registre con el proveedor del sistema de pago antes de que el sistema efectúe cualquier transacción. Normalmente el proceso de registro suele requerir—aunque no en todos los casos—la introducción y verificación de alguna información del cliente (E-mail, teléfono, código postal, entre otros) para poderlo dar de alta y proporcionarle un usuario y contraseña para que se conecte y haga uso del sistema. La información requerida dependerá del producto, del tipo de negocio o de la regulación dispuesta en la jurisdicción donde se encuentre.” (p.13, párrafo 2)

2.2.3. Dinero electrónico.

Como herramienta tecnológica para lograr la Inclusión Financiera, los gobiernos están implementando un sistema de Dinero Electrónico, el cual, según el Banco Central de Reserva de El Salvador, "(…) es la cantidad de dinero que una persona puede manejar a través de un dispositivo móvil, aceptado como medio de pago en comercios afiliados y convertible a dinero en efectivo".

Las Sociedades Proveedoras de Dinero Electrónico, son sociedades anónimas de capital fijo, cuya finalidad se limitará a proveer dinero electrónico, pero también podrán administrar sistema de pagos móviles, es decir, compensar y liquidar pagos con otros proveedores de su naturaleza, previa autorización del Banco Central de Reserva de El Salvador (BCR).

El capital mínimo para que una Sociedad proveedora pueda constituirse, no deberá ser inferior a quinientos mil dólares de los Estados Unidos de América, el cual deberá ser totalmente suscrito y pagado en efectivo; este deberá ser acreditable con depósito en el BCR y ajustado por el Consejo Directivo de la Superintendencia del Sistema Financiero cada dos años en consideración a las variaciones del Índice de Precios al Consumidor (IPC) (Art 2, Inc. 2).

La plataforma electrónica es un sistema que permite operar las transacciones y movimientos realizados con dinero electrónico, dando a los usuarios la posibilidad de acceder a ellas a través de dispositivos móviles.

El GAFISUD en su "Guía sobre los nuevos métodos de pago: tarjetas prepagas, pagos por telefonía móvil y pagos por internet", publicado en junio de 2013, distingue cuatro categorías de servicios financieros a través del teléfono móvil:

a) Servicios de información financiera móvil: en este caso los clientes tienen un acceso extendido a su información financiera a través de sus celulares, pero no tienen la posibilidad de realizar operaciones, como por ejemplo transacciones. (p.10, párrafo 5)

b) Banca móvil: son servicios que ofrece la entidad financiera a sus clientes a través de sus celulares. No son servicios estrictamente nuevos, sino que la entidad financiera ahora facilita una gestión del mismo, pero de forma remota. Entre las operaciones realizables se encuentran: consultas de saldo, transferencia entre cuentas, solicitud de chequeras, suspensión de cheques, pago de facturas, pago de préstamos o la consulta del historial de transacciones. (párrafo 6)

c) Monedero móvil: Funciona como una alternativa al dinero en efectivo. Los clientes pueden almacenar valor en sus celulares, y pueden usar su crédito o tiempo aéreo como método de pago o transferencia. En el momento de la compra, bastará con pasar el código de barras que aparecerá en el teléfono por el lector que tiene instalado el establecimiento. Esta modalidad puede suponer riesgos dependiendo de su funcionalidad y otras medidas mitigadoras que aplique. (párrafo 7)

d) Servicios de pagos móviles: permiten a personas que disponen de cuentas, ya sea con bancos u otras entidades financieras no bancarias, realizar operaciones con teléfonos celulares (pagos en comercios, compras desde el móvil, transferencias entre cuentas, pago de facturas, etc.). Cuando los proveedores de servicios son las entidades financieras bancarias se aplican medidas ALA/CFT homogeneizadas, sin embargo, en muchos casos, los proveedores de estos servicios son instituciones financieras no bancarias y pueden no disponer de medidas de control y supervisión adecuadas. (párrafo 8)

Tipos de pago que permite el sistema.

Entre los pagos que pueden realizarse, con esta tecnología incluyen:

- De individuo a individuo.
- De individuo a empresa, por compra de bienes y servicios.
- De empresa a individuo, como salarios.
- De empresa a empresa.
- De gobierno a individuos.
- De individuo a gobierno.

Ventajas

La mayor parte de las ventajas y desventajas a mencionar, corresponden al proyecto de investigación de pregrado “Ventajas y desventajas del uso de Dinero Electrónico en la ciudad de Guayaquil”, Ecuador (2017), realizado por Shigla, A. y Villavicencio, K.

- No es necesario llevar dinero físico para realizar transacciones.
- La seguridad es con clave personal.
- Las tarifas por el uso del servicio son notablemente económicas.
- Permite realizar pagos de manera rápida y segura.
- Disponibilidad las 24 horas.
- No es necesario saldo de aire ni plan de datos activo. Solamente cobertura.
- Se lleva un mayor control de las operaciones y gastos realizados.
- No se requiere necesariamente de un teléfono inteligente. El servicio funciona por medio de mensajes de texto.

Desventajas

- No todas las personas están de acuerdo a usar este tipo de servicio, por consiguiente, no será aceptado por unos, como método de pago.
- El servicio dejaría de funcionar con interrupciones del servicio de energía, ya sea eléctrica o producto de batería del móvil.
- Dependencia del proveedor del servicio.
- Falta de privacidad de los fondos personales.
- Vulnerabilidad a ataques informáticos.

Lavado de Dinero y Financiamiento al Terrorismo (LD/FT)

Los riesgos fueron abordados tomando en cuenta las leyes actuales vigentes en El Salvador, principalmente la Ley Contra el Lavado de Dinero y de Activos y su Reglamento, la NRP-08 denominada “Normas técnicas para la gestión de los riesgos de lavado de dinero y de activos, y de financiamiento al terrorismo”, las Normas Prudenciales NPB 4-47 “Normas para la gestión integral de riesgos de las entidades financieras”, NPB 4-50 “Normas para la gestión del riesgo operacional de las entidades financieras”, así como “Los Estándares Internacionales sobre la Lucha Contra el Lavado de Activos y el Financiamiento del Terrorismo y la proliferación, emitidos por el Grupo de Acción Financiera de Sudamérica (GAFISUD), en enero de 2012.

2.3 Marco Legal

Como base legal se tomó en cuenta las normativas emitidas por El Banco Central de Reserva de El Salvador con relación a las Sociedades Proveedoras de Dinero Electrónico y sus regulaciones; también se consideraron las normativas emitidas por la Fiscalía General de la

República (FGR) a través de Unidad de Investigación Financiera (UIF) relacionadas al delito de lavado de dinero y activos y financiamiento al terrorismo.

Tabla 1

Análisis de las leyes que regulan el dinero electrónico en El Salvador.

Ley	Análisis
Ley para Facilitar la Inclusión Financiera. Vigencia: 2015 (Art. 1)	Señala las condiciones para el desarrollo del dinero electrónico: Constitución, operación, autorización, capital, garantías y causales de revocatoria de las Sociedades Proveedoras de Dinero Electrónico; y los depósitos en cuentas de ahorro con requisitos simplificados (Artículo N° 1). Adicionalmente la Ley establece que las Sociedades Proveedoras de Dinero Electrónico deben contar con políticas internas en materia de gestión de riesgos, códigos de conducta y otro tipo de requisitos exigidos por formar parte del sistema financiero, como los mencionados en la Ley de Supervisión y Regulación del Sistema Financiero (Artículo N° 7).
Ley de Supervisión y Regulación del Sistema Financiero. (Art. 3 y Art. 7 y Articulo N°35, literales “c” y “d)	Aplicable a las Sociedades Proveedoras de Dinero Electrónico debido a que forman parte del Sistema Financiero. En ella se establece las obligaciones de los integrantes y la responsabilidad de la Superintendencia de supervisar sus operaciones; a continuación, se hace mención a los más relacionados al tema de investigación (Articulo N°35, literales “c” y “d”): · La adopción y actualización de políticas sobre estándares éticos de conducta, manejo de conflictos de interés, uso de información privilegiada, prevención de conductas que pueden implicar la manipulación o abuso del mercado, así como el cumplimiento de principios, reglas o estándares en el manejo de los negocios que establezcan para alcanzar los objetivos corporativos · La adopción y actualización de políticas y mecanismos de gestión de riesgos, debiendo entre otras acciones, identificarlos, evaluarlos, mitigarlos y revelarlos acordes a las mejores prácticas internacionales.
Ley Contra el Lavado de Dinero y de Activos.	El objetivo de esta ley es “prevenir, detectar, sancionar y erradicar el delito de lavado de dinero y de activos, así como de su encubrimiento”; la misma establece aquellos sujetos obligados, entre los cuales hace mención específica en su artículo número dos de “Toda Sociedad, Empresa o Entidad de cualquier tipo, nacional o extranjera, que integre una institución, grupo o conglomerado financiero supervisado y regulado por la Superintendencia del Sistema Financiero”, que para fines de esta investigación se consideran las Sociedades Proveedoras de Dinero Electrónico como parte de esas instituciones obligadas ya que se encuentran dentro de aquellas que son supervisadas y reguladas por la mencionada Superintendencia del Sistema Financiero.
Reglamento de la Ley Contra el Lavado de Dinero y de Activos.	La finalidad única de este es facilitar y asegurar la aplicación de la Ley Contra el Lavado de Dinero y de Activos, el cual para objeto de la investigación es la base para interpretar de manera correcta la mencionada Ley, así como aclarar de manera más específica las obligaciones de las instituciones y las características de aquellas operaciones que se puedan considerar como irregulares o sospechosas.
Instructivo de la Unidad de Investigación Financiera para la Prevención del Lavado de Dinero y de Activos.	Este Instructivo establece las obligaciones que deben cumplir las entidades financieras en cuanto a la prevención del lavado de dinero y de activos, a través de medidas como identificación y conocimiento de los clientes, elaboración de formularios de transacciones en efectivo, de reportes de operaciones sospechosas, con el fin de evitar que personas o agrupaciones de personas oculten o encubran el origen ilícito del dinero que entra al sistema financiero.
NRP-08 “Normas técnicas para la gestión de los riesgos de lavado de dinero y de	El objetivo de éstas es brindar una dirección a los integrantes del Sistema Financiero, para la adecuada gestión del riesgo de lavado de dinero y de activos y de financiamiento al terrorismo, para prevenir y detectar de forma oportuna las operaciones relacionadas

activos, y de financiamiento al terrorismo”	a dichos riesgos, así como también la adopción de políticas y procedimientos de metodologías para la gestión del riesgo mencionado.
NRP-12 “Normas técnicas para el registro, obligaciones y funcionamiento de entidades que realizan operaciones de envío o recepción de dinero”	El objetivo de esta norma es regular el registro, operaciones, obligaciones y funcionamiento de las entidades que realizan operaciones de envío o recepción de dinero en forma sistemática o sustancial por cualquier medio a nivel nacional e internacional. Establece los lineamientos para la implementación de políticas de auditoría interna, gestión de riesgos y manual para la prevención de lavado de dinero y activos y financiamiento al terrorismo; Además, establece los formularios que deben ser completados por las entidades para reportar al Banco Central de Reserva sobre operaciones de envío o recepción de dinero.
NASF-04 “La Norma Técnicas para la Constitución de las Sociedades Proveedoras de Dinero Electrónico”. Vigencia: 2016	Estas Normas tienen como objeto regular los requisitos y el proceso para la autorización de constitución de las Sociedades Proveedoras de Dinero Electrónico, de conformidad a lo dispuesto en la Ley para Facilitar la Inclusión Financiera, estableciendo su naturaleza, finalidad, cuantía del capital social.
NASF-05 “Normas Técnicas para el inicio de operaciones y funcionamiento de los proveedores de dinero electrónico”. Vigencia: 2016	Para conocer el inicio de operaciones y funcionamiento de los proveedores de dinero electrónico, estas Normas tienen como objeto regular los requisitos y el proceso para la autorización de inicio de operaciones y registro de los Proveedores de Dinero Electrónico, así como disposiciones aplicables a la operatividad de éstos en el territorio nacional, conforme a la Ley para Facilitar la Inclusión Financiera. El ajuste de los límites máximos establecidos en la Ley para Facilitar la Inclusión Financiera para Registros de Dinero Electrónico y Depósitos en Cuentas de Ahorro con requisitos simplificados, de acuerdo al reciente aumento de salario mínimo del 2017, se contempla en Circular de fecha 9 de marzo del mismo año, en donde se establece un máximo por cada usuario de trescientos dólares por transacción; mil doscientos acumulados en transacciones durante un mes y esta misma cantidad en saldo acreditable en un mismo mes.
NASF-06 “Catalogo contable para Sociedades Proveedoras de Dinero Electrónico” Vigencia: 2016	Como su nombre lo dice, esta norma establece un Catálogo Contable para uso de estas sociedades en específico.
NPB 4-47 “Normas para la gestión integral de riesgos de las entidades financieras”	Las presentes Normas tienen como objeto establecer los elementos mínimos que deben observar las entidades para la gestión integral de riesgos de conformidad con las leyes aplicables y estándares internacionales en la materia, acordes con la naturaleza y escala de sus actividades. Establece los procedimientos a seguir para la identificación, medición, evaluación y control de riesgos, de manera simplificada, así como su monitoreo y seguimiento.
NPB 4-48 “Normas de gobierno corporativo para las entidades financieras”	El objeto de estas Normas es establecer las bases mínimas que deben adoptar las entidades para fortalecer sus prácticas de gobierno corporativo dentro del proceso de gestión de riesgos financieros, operacionales y otros, conforme a estándares internacionales en la materia y acordes con la naturaleza y escala de sus actividades. El gobierno corporativo es el sistema por el cual las sociedades son administradas y controladas; su estructura deberá establecer las atribuciones y obligaciones de los que participan en su administración, supervisión y control, tales como los accionistas, la Junta Directiva, miembros de la Alta Gerencia, Comités y Unidades de control; asimismo, debe proporcionar un marco adecuado de transparencia de la organización y la protección de los intereses de los depositantes, asegurados y demás usuarios de las entidades. (p. 1)
NPB 4-50	El objeto de las presentes Normas es proporcionar lineamientos mínimos para una adecuada gestión del riesgo operacional y criterios para la adopción de políticas y

"Normas para la gestión del riesgo operacional de las entidades financieras"	procedimientos relacionados con el desarrollo de metodologías para la gestión del riesgo, acordes con la naturaleza, tamaño, perfil de riesgo de las entidades y volumen de sus operaciones. Estas Normas complementan a las disposiciones establecidas en las Normas para la Gestión Integral de Riesgos de las Entidades Financieras (NPB4-47) y las Normas de Gobierno Corporativo para las Entidades Financieras (NPB4-48). (p.1)

El marco legal en El Salvador aún está en proceso de formación, la Ley para Facilitar la Inclusión Financiera aún no cuenta con su reglamento, por lo que deja cabida a confusiones al momento de ser aplicada, pero es evidente que el mercado de dinero electrónico también es nuevo.

2.4 Marco técnico y normativo

Tabla 2

Análisis de la normativa técnica aplicable a las Sociedades Proveedoras de Dinero Electrónico en El Salvador

Norma	Análisis
ISO 31000 Vigencia: 2018	Para el desarrollo de la investigación se implementan los principios sugeridos por la ISO 31000, con sus actualizaciones más recientes del 2018, como guía para la gestión de riesgo, mediante el entendimiento, la planificación y el actuar con un mapa de riesgo que permite monitorear áreas vulnerables dentro de las organizaciones. En base a esta Norma también se evaluarán los riesgos que se encuentren, mediante estimados de la probabilidad e impacto; y que además en su versión más reciente, incluye la elaboración de un reporte mensual de riesgo.
Las Recomendaciones del GAFI Publicadas en febrero de 2012 y junio de 2015.	Se abordan las recomendaciones del Grupo de Acción Financiera Internacional (GAFI), ente intergubernamental que tiene por objetivo promover políticas legales, regulatorias y operativas para proteger el sistema financiero mundial contra el lavado de activos y financiamiento al terrorismo. En ese sentido, se consideran los Estándares Internacionales sobre la Lucha contra el Lavado de Activos y el Financiamiento del Terrorismo y de la Proliferación (Las Recomendaciones del GAFI) publicados en febrero de 2012, así como las "Directrices para un enfoque basado en riesgo para monedas virtuales" publicadas en Junio de 2015, para abordar de manera más amplia los ilícitos a los cuales se hace referencia en esta investigación, así como la evaluación de los riesgos y su forma de gestionarlos adecuadamente. De esa misma forma, se analizan cada una de las medidas preventivas que considera el GAFI, tanto para los usuarios, así como para las instituciones financieras, y los servicios que estas brindan, haciendo énfasis en las nuevas tecnologías y las monedas virtuales.
Guía del GAFI sobre Medidas Antilavado de Activos y contra el Financiamiento al Terrorismo e Inclusión Financiera. (Publicada en 2013)	Esta Guía proporciona un marco general para ayudar a las jurisdicciones en la implementación de un sistema ALA/CFT consistente con el objetivo de la inclusión financiera. Su objetivo es apoyar a las autoridades competentes en el desarrollo de un conjunto medidas ALA/CFT integrales y equilibradas basadas en el entorno de riesgo de LA/FT en el que sus sistemas financieros operan. También tiene como objetivo promover el desarrollo una comprensión común de las Recomendaciones del GAFI que son relevantes al promover la inclusión financiera y calificar la flexibilidad que ofrecen. en particular, a través del enfoque basado en el riesgo. Por último, el documento contiene las iniciativas de países para hacer frente a la Inclusión Financiera en el contexto ALA/CFT. (p.142 párrafo 7, p. 143, párrafo 1).
Guía del GAFISUD sobre los nuevos Métodos de	El objetivo de GAFISUD es entender en su totalidad las características, funcionamiento, modalidades y riesgos de estos métodos de pago, así como identificar

pago: tarjetas Prepagas, pagos por telefonía Móvil y pagos por internet. Publicado en junio de 2013	aquellos elementos que puedan funcionar como mitigadores de esas amenazas. Pretende mantener un enfoque que preserve la viabilidad de los productos y servicios promoviendo por un lado la inclusión financiera, y por otro, el cumplimiento de requisitos razonables de control, supervisión y seguridad. En una etapa posterior, GAFISUD se compromete en esta guía a proporcionar toda la asistencia que los países miembros necesiten al respecto para revisar su situación nacional y traerla a los máximos niveles de efectividad cumpliendo con los principales estándares internacionales. - Los Capítulos 1 y 2 ofrecen una visión detallada de cada uno de los métodos de pago, su evolución, características y funcionamiento; - Los Capítulos 3, 4 y 5 se centran en la identificación de riesgos y en las formas de mitigarlos acorde con los estándares internacionales. Este módulo incluye también una selección de casos de explotación de NMPs por criminales para operaciones de LA. Finalmente, en el Capítulo 5 se hace hincapié en la compatibilidad del cumplimiento de las recomendaciones del GAFI y la inclusión financiera. - El Capítulo 6 concluye con una visión general de la situación del subsector de pagos en la región latinoamericana. - El Capítulo 7 describe tres casos de productos particulares. Los dos primeros casos confirman la viabilidad de productos de pago de bajo riesgo y en cumplimiento de los estándares internacionales. El tercer caso describe un esquema de moneda virtual multiuso, no regulado y de posible alto riesgo. - El Capítulo 8 recoge brevemente las principales conclusiones del informe.
El acuerdo de Basilea I, firmado en 1988,	Como información complementaria, se consultaron algunos tratados internacionales que abonan a los lineamientos de cómo deben constituirse y funcionar las empresas pertenecientes al sistema financiero, como es el caso de los Tratados de Basilea. El Comité de Basilea, creado en 1975, por los bancos centrales del llamado Grupo Los 10 y conformado por un grupo de once (no diez) naciones industriales: Bélgica, Canadá, Francia, Alemania, Italia, Japón, Países Bajos, Suecia, Suiza, Reino Unido, y los Estados Unidos; los acuerdos de Basilea, se encargan de fijar coeficientes de caja y niveles de riesgo asumibles. El primer acuerdo, estableció principios básicos en los que debía fundamentarse la actividad bancaria. Los más importantes fueron el capital regulatorio, el requisito de permanencia, la capacidad de absorción de pérdidas y la de protección ante quiebra. Este capital debía ser suficiente para hacer frente a los riesgos de crédito, de mercado y de tipo de cambio. El acuerdo establecía también que el capital mínimo de la entidad bancaria debería constituir el 8 % del total de los activos de riesgo (crédito, mercado y tipo de cambio sumados).
El acuerdo Basilea II Firmado en 2004	Aunque en España no se llegó a aplicar hasta el 2008, desarrollaba, de manera más extensa, el cálculo de los activos ponderados por riesgo. De esta forma, permitía que las entidades bancarias aplicasen calificaciones de riesgo basadas en sus modelos internos, siempre que estuviesen previamente aprobadas por el supervisor. Este acuerdo incorporaba, por lo tanto, nuevas tendencias en la medición y el seguimiento de las distintas clases de riesgo. Se hizo énfasis en las metodologías internas, la revisión de la supervisión y la disciplina de mercado. El acuerdo Basilea II, fue aprobado en 2004, aunque en España no se llegó a aplicar hasta el 2008. Desarrollaba, de manera más extensa, el cálculo de los activos ponderados por riesgo. De esta forma, permitía que las entidades bancarias aplicasen calificaciones de riesgo basadas en sus modelos internos, siempre que estuviesen previamente aprobadas por el supervisor.
El acuerdo Basilea III. Firmado en diciembre de 2010	Intentó adaptarse a la magnitud de la crisis económica. Trataba de atender a la exposición de gran parte de los bancos de todo el mundo a los “activos tóxicos” en sus balances y en los derivados que circulaban en el mercado. El temor al efecto dominó que pudiera causar la insolvencia de los bancos, hizo que se establecieron nuevas recomendaciones como: Endurecimiento de los criterios y aumento de la calidad del volumen de capital para asegurar su mayor capacidad para absorber pérdidas.

	Modificación de los criterios de cálculo de los riesgos para disminuir el nivel de exposición real. Constitución de colchones de capital durante los buenos tiempos que permitan hacer frente el cambio de ciclo económico. Introducción de una nueva ratio de apalancamiento, como medida complementaria al ratio de solvencia.

El marco normativo en El Salvador está dado principalmente por su Banco Central de Reserva de El Salvador (BCR) y supervisado por la Superintendencia del Sistema Financiero (SSF), y es una selección especial de las Normas aplicables al sistema bancario. Internacionalmente existen Organismos como el Grupo de Los 10 (G10) y el Grupo de Acción Financiera Internacional (GAFI) que dictan estándares sobre Lavado de Dinero e Inclusión Financiera aplicables a las Sociedades Proveedoras de Dinero Electrónico (SPDE).

CAPÍTULO III

3. METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Enfoque y tipo de investigación

Lo que se buscó fue estudiar la gestión de riesgo implementada por las Sociedades Proveedoras de Dinero Electrónico para prevenir operaciones ilícitas. Para ello, se eligió el tipo de estudio no experimental longitudinal, centrándose básicamente en la tendencia del problema dentro del periodo seleccionado; los resultados, posteriormente fueron analizados.

3.2. Delimitación temporal y espacial

Es importante mencionar que se analizó únicamente una sociedad debido a que, a la fecha de la investigación era la única entidad autorizada para proveer dinero electrónico, haciendo énfasis en la ubicación de la misma, la cual se desplazó del departamento de San Salvador a La Libertad.

Referente al tiempo, se consideraron fundamentales los años siguientes:

a) Año 2011: Constitución e inicio de operaciones de la sociedad en cuestión, la cual fue constituida el 03 de marzo de 2011.

b) Año 2015: Creación de la Ley para Facilitar la Inclusión Financiera e inicio del proceso de autorización como Sociedad Proveedora de Dinero Electrónico por parte de la Superintendencia del Sistema Financiero, Decreto No. 72 de la Asamblea Legislativa de la República de El Salvador de fecha trece de agosto de dos mil quince.

c) Año 2018: Autorización oficial como primera Sociedad Proveedora de Dinero Electrónico en El Salvador según acta de sesión del Consejo Directivo de la Superintendencia del Sistema Financiero No. CD-23/2018 romanos I, II y III celebrada en el año 2018.

3.3. Universo y muestra

La muestra es específica, ya que se consideró el cien por ciento del universo, tomando en cuenta que, actualmente en nuestro país, solo existe una empresa autorizada para brindar el servicio de dinero electrónico que no corresponde directamente al Sistema Bancario.

3.4. Sujeto y objeto de estudio

La unidad de análisis es la única Sociedad Proveedora de Dinero Electrónico autorizada en El Salvador y el objeto es conocer la gestión de riesgos y la efectividad de ésta.

3.5. Técnicas, materiales e instrumentos

Para la recolección de información se utilizó, tanto la técnica de observación directa y entrevistas con preguntas concretas para lograr los objetivos.

a) ***Testeo del Servicio:*** se realizaron visitas a los corresponsales en calidad de "Cliente Misterioso" con el fin de obtener información sobre los controles aplicados y se abrió cuenta de usuario Tigo Money para testear el funcionamiento del sistema y experimentar

de primera mano la comodidad y seguridad que percibe el usuario al momento de realizar una transacción con su billetera móvil.

b) Entrevistas: se realizó entrevista con el Director de Auditoría Interna de la primera sociedad, la cual nos permitió tener un contacto más directo y obtener información más específica de los controles utilizados por éstas para resguardarse para que las plataformas que brindan el servicio electrónico sean más eficientes y seguras.

3.6 Procesamiento y análisis de la información

- Se revisó y organizó la información recabada, y luego fue transformada a texto para comprenderla mejor.
- Se clasificaron y compilaron los datos para poder ser analizados y detectar riesgos latentes que pudieran estar cubiertos o no cubiertos totalmente.
- Se han agregado tablas, graficas, flujogramas y cualquier otra técnica que se necesaria para su mejor comprensión del funcionamiento y esquematización de las funciones dentro de la organización.

Los análisis se realizaron partiendo de la hipótesis planteada, la cual se llevó a comprobación, para su respetiva aceptación o refutación; llevando a cabo la respectiva medición de las variables, todo esto en función de los objetivos propuestos.

Al finalizar las encuestas y entrevistas, se efectuó un diagnóstico general de cada una de las preguntas con el fin de establecer un diagnóstico de cada una y que este sirva para crear medidas de control o ya sea mejorar las ya existentes.

3.7. Cronograma de actividades

Tabla 3

El cronograma de actividades está en función de los avances presentados.

AÑO 2018																																							
MES	**MAR**				**ABR**				**MAY**				**JUN**				**JUL**				**AGO**				**SEPT**				**OCT**				**NOV**				**DIC**			
SEMANA	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
PLANIFICACIÓN DE INVESTIGACIÓN																																								
Selección del tema																																								
Aprobación del tema a investigar																																								
Caracterización de la problemática																																								
Formulación de la investigación																																								
Delimitación de la investigación																																								
Justificación y objetivo de la investigación																																								
Primera entrega avance de anteproyecto																																								
Marco teórico, legal, técnico																																								
Elaboración de diseño metodológico, hipótesis y operacionalización																																								
Entrega de anteproyectos																																								
Evaluación del anteproyecto																																								
Elaboración de cuestionarios																																								
Recolección de la información																																								
Procesamiento y análisis de la información																																								
Entrega de Capítulo I																																								
ELABORACIÓN DE CAPÍTULOS I, II Y III																																								
Elaboración de Capítulo II																																								
Entrega de CAPÍTULO II																																								
Elaboración de Capítulo III																																								
Elaboración de conclusiones y recomendaciones																																								
Entrega de Capítulo III																																								
Entrega de trabajo final																																								
Revisiones y Correcciones																																								

3.8. Presentación de los resultados

Se presentan los resultados de la encuesta, en donde se hace un análisis individual de cada una de las respuestas obtenidas, con el objeto de detectar vulnerabilidades en los controles y dar así una respuesta a los riesgos detectados.

Tabla 4.
Resultados de la entrevista realizada al Auditor Interno de la Sociedad Proveedora entrevistada.

No	Pregunta	Respuesta	Análisis
1	¿Cuenta la empresa con un sistema de control interno que ayude a prevenir operaciones ilícitas en las plataformas virtuales de dinero electrónico?	Si. La empresa cuenta con un sistema de control interno, que abarca todas las áreas de la compañía, tanto operativas, financieras, legales, etc. Para detectar operaciones inusuales se cuenta con una herramienta informática de nombre SYS-HELP, que determina operaciones que sobrepasan los límites establecidos a las cuales se les da seguimiento de acuerdo a las regulaciones legales.	Es evidente que la empresa cuenta con herramientas informáticas vanguardistas muy funciónales al momento de detectar operaciones inusuales, las cuales son detectadas a través patrones de comportamiento que cada usuario presenta, tales como: montos, horarios, frecuencia de transacciones y otros. También es evidente que no todas las transacciones que cuentan con estos patrones son riesgos latentes, por otra parte, existe la posibilidad que empleados que conocen dichos patrones de evaluación, se valgan de ello para burlarlos o las confíen a terceros.
2	¿Cuál es la base técnica sobre la que ha sido elaborado su sistema de Gestión de Riesgos?	En base a las normas emitidas por el Banco Central de Reserva (BCR) para tal efecto y el marco de control interno está montado sobre el modelo COSO (Committee of Sponsoring Organizations) para los controles financieros y COBIT (Control Objectives for Information and Related Technology) para los controles no financieros. COSO es un modelo de gestión de riesgo integral de importante aceptación por un gran número de empresas a nivel mundial, su actualización 2017 consta de 23 principios organizados en 5 componentes y cubre desde El Gobierno Corporativo hasta el monitoreo del riesgo. En cuanto COBIT es un marco aceptado también mundialmente pero se centra en el control de la información, Tecnologías de la Información (TI) y los riesgos que estos conllevan.	Se considera que la base sobre la que está montado el control interno de la compañía esta implementado de manera adecuada tomando en cuenta la complejidad de ésta. Es importante mencionar que la base técnica es establecida legalmente por el Banco Central de Reserva y supervisada por la Superintendencia del Sistema Financiero, y los marcos técnicos COSO y COBIT son de aceptación general en muchos países del mundo debido a la eficacia en la gestión de riesgos y tecnologías de la información.

3	¿Qué mecanismos de control significativos han sido implementados para prevenir operaciones ilícitas y que resultados han obtenido?	El sistema de monitoreo de alertas es una de las herramientas más eficiente con la que cuenta la empresa, porque detecta cualquier operación inusual que se realice en la plataforma.	Aunque esta herramienta promete ser eficiente, ya que genera alertas basadas en patrones de las operaciones que puede realizar un cliente de acuerdo a su giro o actividad económica, pero como se mencionó anteriormente, estos patrones de riesgos pueden ser burlados por empleados u otras personas ajenas a la empresa que tenga conocimiento de ellos.
4	¿Se han detectado actividades sospechosas con los procesos implementados?	Si, en la empresa las llamamos inusuales ya que por términos legales no podemos clasificarlas como sospechosas.	Son detectadas en base a ciertos controles que posee la entidad; sin embargo, existe el riesgo de fuga de información confidencial a través de un empleado que conozca el sistema y se preste para este tipo de operaciones y de esa forma atentar contra la seguridad de la plataforma.
5	¿De qué forma se documentan los procesos cuando se detecta una operación sospechosa?	Primeramente, le llega un correo como una alerta al usuario, luego se le da seguimiento por parte de las áreas correspondientes, y por último se cierra el caso. El flujo de trabajo se llama Ciclo Compartido (Share Point), en el queda documentado el caso para cualquier persona que necesite ver cuál fue la atención al caso por una alerta.	Aunque el sistema genera un reporte de cada operación inusual, solo toman en cuenta factores internos, dejando a un lado aspectos externos como la ubicación desde donde el usuario realiza la transacción, como el caso de zonas con alto índice de delincuencia.
6	¿Cuáles son los riesgos más significativos que han sido cubiertos desde la implementación de su sistema de control interno para prevenir operaciones inusuales?	Esta situación es previsible en el manejo de operaciones de la empresa ya que cualquier sistema de control puede tener vulnerabilidades, sin embargo, se trabaja para prevenir riesgos de cualquier índole.	Aunque la Auditor Interno no profundizó por motivos confidenciales, el riesgo a posibles eventualidades de parte de personas propias y ajenas a la empresa siempre existe, por lo que la empresa trata de cubrir todas las áreas que en un determinado momento puedan considerarse críticas.
7	¿El proceso de gestión de riesgos de lavado de dinero y activos y financiamiento al terrorismo se hace de forma integral hasta que este es mitigado?	Si. Se hace de forma integral, desde la identificación de riesgos hasta la respuesta a estos, todo de acuerdo a lo regulado en la Normas Técnicas para la Gestión de los Riesgos de Lavado de Dinero y de Activos, y de Financiamiento al Terrorismo (NRP 08)	Este aspecto se considera cubierto por la compañía, gracias a la intervención de entes reguladores y de supervisión como el Banco Central de Reserva (BCR) y la Superintendencia del Sistema Financiero (SSF) respectivamente.
8	¿Cuál es el perfil que deben cumplir el o los encargados de la gestión de riesgos de la empresa?	Hay una estructura que previamente ha sido revisada por Junta Directiva y la Superintendencia del Sistema Financiero dio el visto bueno, pero el perfil de debe poseer conocimientos financieros y técnicos. El encargado del área de Gestión de Riesgos es Gerente de Riesgos y éste tiene un equipo de personas	Los perfiles del personal que gestiona los riesgos son avalados por la Superintendencia del Sistema Financiero, por lo que el riesgo de contratar personas no aptas o no idóneas se reduce, ya que se realiza la debida diligencia para evitarlo.

		encargado de gestionar, capacitar y dar cumplimiento a los planes de acción para mitigarlos.	
9	¿Tiene el área de gestión de riesgos un presupuesto adecuado para el desarrollo de sus funciones?	La palabra “adecuado” es subjetiva, esto tiene mucho que ver con el tipo y la cantidad de riesgos y la probabilidad de ocurrencia. Los riesgos son algo que constantemente estamos evaluando, pero se cuentan con los recursos necesarios para ello.	Es evidente que el presupuesto asignado no está en correspondencia con el volumen de riesgos y la complejidad de estos, por lo que es necesario una determinación adecuada de los gastos en que se pudiera incurrir y la existencia de un presupuesto específico para esta área.
10	¿Con qué periodicidad se capacita al personal encargado de la gestión de riesgos de la empresa?	Los jefes de Gestión de Riesgos tienen la obligación de participar en las formaciones de las diferentes áreas, pero al personal, como tal, se capacita una vez al año. Ellos tienen doble tarea, reciben la enseñanza y transmiten el conocimiento adquirido.	Aunque el personal es debidamente capacitado se considera que estas formaciones son poco frecuentes, ya que para el nivel tecnológico que el sistema de dinero electrónico supone, estas deberían ser con mayor periodicidad.
11	¿Qué tipo de informes emite la Unidad de Gestión de Riesgo, a quién se comunica y con qué periodicidad se informa?	Los informes son por escrito y se informa una vez al mes. El Comité encargado informa de los riesgos ya sea si son nuevos o el nivel de progreso que llevan y como se está cumpliendo el plan de acción para mitigarlos. Una vez son identificados y escalados en comité, son presentados en Junta Directiva una vez cada tres meses, según las Normas de Gobierno Corporativo para las Entidades Financieras (NPB 04-48).	Los riesgos son reportados con una periodicidad prudente y dentro del tiempo establecido por el ente normativo.
12	¿Cómo se evalúa la comunicación entre los encargados de la gestión del riesgo y los obligados de rendir cuentas de cada área?	Los riesgos se comunican al Comité y estos se hacen del conocimiento a Junta Directiva.	Se considera que debe haber una comunicación efectiva entre todos los niveles jerárquicos y de esta forma dar respuesta a los riesgos.
13	¿Cuenta la empresa con un Comité de Riesgos y quienes lo integran?	Los informes se emiten de acuerdo a la Normas de Gobierno Corporativo para las Entidades Financieras (NPB 04-48), la cual establece que debe haber tres comités, uno de Gestión de Riesgo, otro de Prevención contra el Lavado de Dinero y el otro de Auditoría. La Junta Directiva determina quién va a integrar cada comité, estos se reúnen una vez al mes.	La empresa ha constituido los comités tal como lo sugiere el Banco Central de Reserva a través de las Normas de Gobierno Corporativo para Entidades Financieras, por lo que la empresa cuenta con el soporte técnico adecuado en sus funciones de supervisión y control interno y su buen funcionamiento.
14	¿Cómo se asegura la empresa que las	Mediante la capacitación. La compañía las divulga las políticas y	A través de capacitaciones, la empresa realiza un control sobre el nivel de

	disposiciones para gestionar riesgos son claramente comprendidas y puestas en práctica?	luego realiza test al personal para evaluar la comprensión de las mismas.	comprensión que tiene el personal en la materia, sin embargo, no se mencionan evaluaciones prácticas para asegurar que la teoría sea bien aplicada en casos puntuales.
15	¿Cuenta el sistema generador de transacciones electrónicas con las medidas de seguridad necesarias establecidas por la Ley de Inclusión Financiera?	Si, cada empleado con acceso al sistema posee su propio usuario y contraseña para el manejo del sistema de acuerdo a las actividades delegadas a cada miembro.	Los requerimientos legales en temas de seguridad informática son de vital importancia para el buen funcionamiento de las plataformas electrónicas, así como para el resguardo de los usuarios que hacen uso de ellas; la empresa cuenta con medidas de seguridad de la información adecuadas para garantizar el correcto uso de la plataforma por parte del personal.
16	¿Los empleados del departamento de informática pueden acceder al sistema fuera de la empresa?	No, todo se genera desde adentro, hay un área de seguridad donde cada usuario que tiene acceso a la plataforma está documentado en una descripción de funciones y no se le da acceso, más de los que requieran sus actividades laborales. Esos accesos son previamente evaluados por los jefes y por el área de riesgo y está delimitado desde la consulta hasta hacer transacciones que afecten una billetera de dinero electrónico.	El ingreso al sistema desde fuera de las instalaciones de la empresa podría volverse vulnerable sino se cuenta con las medidas de seguridad de información, para garantizar el adecuado manejo por parte del empleado; la empresa mitiga este riesgo a través de no permitir el ingreso a ningún empleado que esté fuera del espacio físico de sus instalaciones.
17	¿De qué forma la empresa comprueba la autenticidad de los documentos y el origen de los ingresos de las personas que van a registrarse en el sistema?	Mediante el uso de la debida diligencia establecida por La Ley Contra el Lavado de Dinero y el Instructivo de la Unidad de Investigación Financiera de la Fiscalía General de la República que establece la política “Conozca a su cliente”, a través del cual se llena un formulario con información personal de cada cliente que se registra en el sistema.	La Ley Contra el Lavado de Dinero y de Activos, obliga a la empresa a establecer una política interna de debida diligencia para la identificación de sus usuarios o sus clientes, así como conservar esa documentación y de sus operaciones con el fin de tenerla disponible cuando así lo requieran las autoridades competentes, de esa forma la empresa no puede comprobar autenticidad de documentos a la hora de registrar usuarios, pero si presentar la documentación a las autoridades encargadas para ello.
18	¿Cómo determina la empresa los límites de saldo y de transacciones con los comercios, sus puntos de atención, colectores y usuarios de las plataformas electrónicas con dinero electrónico?	Mediante la parametrización del sistema, cuando algún usuario sobrepasa los límites de las “billeteras electrónicas”, este envía una alerta en forma de correo electrónico o mensaje de texto, para informarle al cliente sobre ese exceso, pero la plataforma siempre está sujeta al error humano, por lo que podrían darse casos que ésta permita sobrepasar alguno de los parámetros establecidos.	Si bien existen parámetros para controlar los límites de los montos de las operaciones con dinero electrónico, existe la posibilidad que el sistema permita realizar transacciones superiores de esas cantidades, por lo cual emitirá una alerta para informar al cliente de dicha inconsistencia.

19	¿La empresa verifica que los corresponsales financieros cumplan con las regulaciones en materia de prevención de lavado de dinero y financiamiento al terrorismo y con qué periodicidad se verifica?	Se verifican según lo establecido en la Ley Contra el Lavado de Dinero y de Activos. Aunque la empresa no puede estar pendiente de cada corresponsal, por ejemplo, un banco local o un corresponsal de dinero del exterior. La compañía se asegura mediante el monitoreo que realiza y tiene herramientas para hacer su evaluación de riesgo para saber por ejemplo cuándo un empleado o una institución financiera ha caído en degradación por un tema de lavado de dinero, entonces la compañía hace su valoración de riesgo y consulta con la Superintendencia del Sistema Financiero (SSF) y el Banco Central de Reserva (BCR) para ver hasta dónde llegan con esa institución, lo mismo sucede con empresas aquí en El Salvador que están vinculadas con noticias y sospechas de operaciones inusuales, porque el riesgo reputacional es el más dañino que puede haber y la empresa se cuida mucho en ese aspecto.	La empresa verifica dentro de sus posibilidades a través de monitoreo que los corresponsales financieros debido a que, por tratarse de empresas con sede internacional instaladas en el país, se cuidan de transgredir las leyes del país donde radican.
20	¿Cuáles son los cambios más significativos en materia de prevención de riesgo que experimentó el plan de control interno de la empresa una vez autorizada oficialmente para proveer dinero electrónico y dar cumplimiento a las leyes aplicable?	La compañía siempre ha contado con un sistema de control interno desde que nació, siempre se han mantenido auditorías, uno de los cambios fue el ente regulador y el único cambio del plan fue que las guías de control se pasaron del inglés al idioma español, porque la Ley para Facilitar la Inclusión Financiera pide que la Guía de Control de Interno se maneje en idioma castellano.	La empresa en un inicio operaba sin una legislación que le fuera aplicable, lo que significaba que realizaba sus operaciones de acuerdo a políticas y procedimientos con estándares internacionales que únicamente se encontraban en idioma inglés, al aprobarse la Ley para Facilitar la Inclusión Financiera fue de carácter obligatorio que dichas guías de procedimientos se realizaran en español para adecuarlo al idioma del país.
21	¿La empresa cuenta con un archivo de todas las operaciones que se realizan con dinero electrónico a fin de cumplir con los requerimientos de la Unidad de Investigación Financiera de la Fiscalía General de la República?	Si, todas las operaciones quedan documentadas para cualquier requerimiento de parte de la Fiscalía General de la Republica (FGR).	Documentar las transacciones que se realizan en la plataforma de dinero electrónico le sirve a la empresa para respaldarse en caso de algún requerimiento de actividades inusuales o sospechosas de parte de la FGR, debido a ello, la empresa lleva un respaldo de todos los casos de operaciones inusuales en forma de bitácoras.
22	¿La empresa tiene nombrado un oficial de cumplimiento para	Si, la empresa cuenta con un oficial de cumplimiento, el cual fue nombrado por la Junta Directiva y	La Ley Contra el Lavado de Dinero y de Activos obliga a la empresa a “nombrar y capacitar a un oficial de cumplimiento”,

	cumplir con la Ley Contra el Lavado de Dinero y de Activos?	con la evaluación de la Superintendencia del Sistema Financiero (SSF).	que deberá "reportar diligencias u operaciones financieras sospechosas que superen el umbral de la Ley", de esa forma brindar información en el momento que la requiera ya sea la Superintendencia del Sistema Financiero o la Fiscalía General de la República a través de la Unidad de Investigación Financiera para demostrar el origen lícito de las transacciones que se realicen con dinero electrónico.
23	¿Cuál es la relación entre el oficial de cumplimiento con el departamento encargado de la gestión de riesgos?	Son áreas independientes, porque uno ve la previsión de Lavado de Dinero y el otro ve la Gestión de Riesgo, o sea, el segundo gestiona el Riesgo Operacional. Comparten información, pero no tienen dependencia jerárquica, el departamento de Auditoría Interna, el Oficial de Cumplimiento y el Gerente Riesgo se reportan a la Junta Directiva, las tres son áreas completamente independientes, sino hubiera conflicto de intereses.	El Art. 14 de la Ley Contra el Lavado de Dinero y de Activos, establece que los oficiales de cumplimiento deberán gozar de independencia en el desarrollo de sus funciones, así como tienen la facultad para la toma de decisiones, por lo que, con el fin de garantizar esa independencia dentro de la estructura organizativa de la empresa, tanto el oficial de cumplimiento como el departamento de auditoría interna son cargos que no dependen el uno del otro.

3.9 Diagnóstico de la investigación

Según los resultados de la entrevista se puede apreciar escaso interés por atender factores externos que son potencialmente considerados como posibles generadores de riesgos, y aunque si se cuenta con un sistema de control interno, este se centra más puntualmente en los factores internos.

Por otra parte, las Sociedades Proveedoras de Dinero Electrónico no cuentan con una guía que les ayude a gestionar este tipo de riesgos de operaciones ilícitas, cuya cobertura es exigida por las Superintendencia del Sistema Financiero y se encuentran contenidas en las Normas Técnicas aplicables a entidades financieras y en la Ley Contra el Lavado de Dinero y de Activos.

Actualmente no existe un marco normativo exclusivo para las Sociedades Proveedoras de Dinero Electrónico, puesto que las existentes son propias del sistema bancario, las cuales a la fecha de su creación no consideraban este rubro.

A esto se suman ciertas limitaciones en la aplicación de algunas leyes como la Ley para Facilitar la Inclusión Financiera la cual aún no cuenta con su respectivo reglamento, lo que contribuye a dificultar su interpretación; y otras como las adaptaciones de normativa técnica propia del sistema bancario cuya aplicación es parcial, como es el caso de la NPB4-47, la cual habla de gestión integral de riesgos de las entidades financieras, de los cuales los riesgos de crédito, de liquidez y de mercado no son aplicables al tipo de sociedades en estudio.

Tomando en cuenta lo anterior, se consideró necesario proponer un Modelo de Gestión para prevenir operaciones ilícitas en las Sociedades Proveedoras de Dinero Electrónico basado en la Ley para Facilitar la Inclusión Financiera, las Normas emitidas por el Banco Central de Reserva, especialmente las Normas Prudenciales 4-47, 4-48 y 4-50 y Normas Técnicas para la Gestión de Riesgos de Lavado de Dinero y de Activos y de Financiamiento al Terrorismo NRP-08, así como las Guías del GAFI: “Directrices para un Enfoque Basado en Riesgo – Monedas Virtuales”, “Medidas Antilavado de Activos y contra el Financiamiento al Terrorismo e Inclusión Financiera” “Guía del GAFISUD sobre los nuevos métodos de pago: tarjetas prepagas, pagos por telefonía móvil y pagos por internet”.

CAPITULO IV

"PROPUESTA DE UN MODELO DE GESTIÓN DE RIESGOS PARA SOCIEDADES PROVEEDORAS DE DINERO ELECTRONICO PARA PREVENIR OPERACIONES ILÍCITAS"

4.1 Planteamiento del Modelo de Gestión

La propuesta se basó básicamente en diseñar un modelo de control interno que sirva de apoyo a las Sociedades Proveedoras de Dinero Electrónico (SPDE) en proceso de ser autorizadas y las nuevas en constitución para apoyarlos en la elaboración de su sistema de gestión de riesgos para prevenir operaciones ilícitas, tanto provenientes del personal dentro de la entidad como de los usuarios de sus servicios.

El modelo fue elaborado en concordancia con las exigencias legales vigentes, así como la implementación de controles para gestionarlos de manera íntegra, se ha tomado como referencia la Ley para Facilitar la Inclusión Financiera, las Normas Técnicas para la Gestión de los Riesgos de Lavado de Dinero y de Activos, y de Financiamiento al Terrorismo (NRP-08), las Normas para la Gestión Integral de riesgos de las entidades Financieras (NPB4-47), las Normas de Gobierno Corporativo (NPB4-48), las Normas para la Gestión de Riesgo Operacional de las entidades financieras (NPB4-50), , las Normas Técnicas para el inicio de operaciones y funcionamiento de los proveedores de dinero electrónico (NASF-05), las Recomendaciones del GAFI así con los Acuerdos de Basilea. Se adopta la premisa que las áreas de Gestión serán similares en Sociedades Proveedoras de dinero electrónico constituidas en el país, debido a que estas son reguladas por la ley desde el primer momento del proceso de constitución.

El Modelo de Gestión de riesgos para prevenir operaciones ilícitas en las Sociedades Proveedoras de Dinero Electrónico se compone de las siguientes fases:

Fase 1. Generalidades de una sociedad proveedora de dinero electrónico. Esta fase comprendió la adopción de una sociedad ficticia como ejemplo, cuyo propósito fue la mejor comprensión de las demás fases.

Fase 2. Objetivos y alcance del modelo. Comprende el propósito para el cual el modelo fue elaborado y los aspectos y tipos de riesgos que abarcó, centrándose especialmente en la prevención de ilícitos.

Fase 3. Gestión integral de riesgos. Supone la fase central del modelo y por consiguiente abarca las etapas de identificación, evaluación, valoración, mitigación y monitoreo de los riesgos dentro de una sociedad proveedora, todas ellas basadas en las disposiciones legales vigentes exigidas por la Superintendencia del Sistema Financiero (SSF).

Fase 4. Conclusiones y recomendaciones. Luego de gestionar los distintos riesgos se concluyó sobre éstos y los factores que los originan y se propusieron algunas recomendaciones que consideradas pertinentes y que podrían coadyuvar en disminuirlos o mitigarlos.

4.2 Objetivo

Con el modelo propuesto se buscó fortalecer las capacidades de prevención y respuesta de las Sociedades Proveedoras de Dinero Electrónico ante operaciones ilícitas en sus plataformas; disminuir la probabilidad de ocurrencia y de impacto de posibles operaciones sospechosas, y responder de manera rápida y efectiva ante cualquier transacción de ese tipo tomando como

referencia experiencias y modelos probados en los distintos países de Latinoamérica donde se han implementado algunos similares.

4.3 Alcance

El presente modelo de gestión de riesgos cubre a aquellos sectores que están vulnerables de ser utilizados para cometer ilícitos, con el fin de prevenirlos con anticipación y a la vez proporcionar un marco de referencia para las Sociedades Proveedoras de Dinero Electrónico en proceso de constitución.

4.4 Prólogo

Los conceptos empleados y la estructura de este documento y su contenido, están basados en las Normas emitidas por El Banco Central de Reserva de El Salvador (BCR) y lineamientos de control sugeridos por la Superintendencia del Sistema Financiero (SSF), con el fin de proveer una guía basada en dichas Normas para contribuir con las Sociedades Proveedoras de Dinero Electrónico -En adelante: SPDE- en proceso de constitución y/o autorización, a adaptar dicha normativa a su estructura, y de esa manera cumplir con los requerimientos que la Ley establece para poder funcionar como tales.

4.5 Índice de la propuesta

4.5.1 Índice de Figuras

4.5.2 Índice de Tablas

DESARROLLO DEL MODELO PROPUESTO

Inicia: *Modelo de Gestión de Riesgo para SPDE*

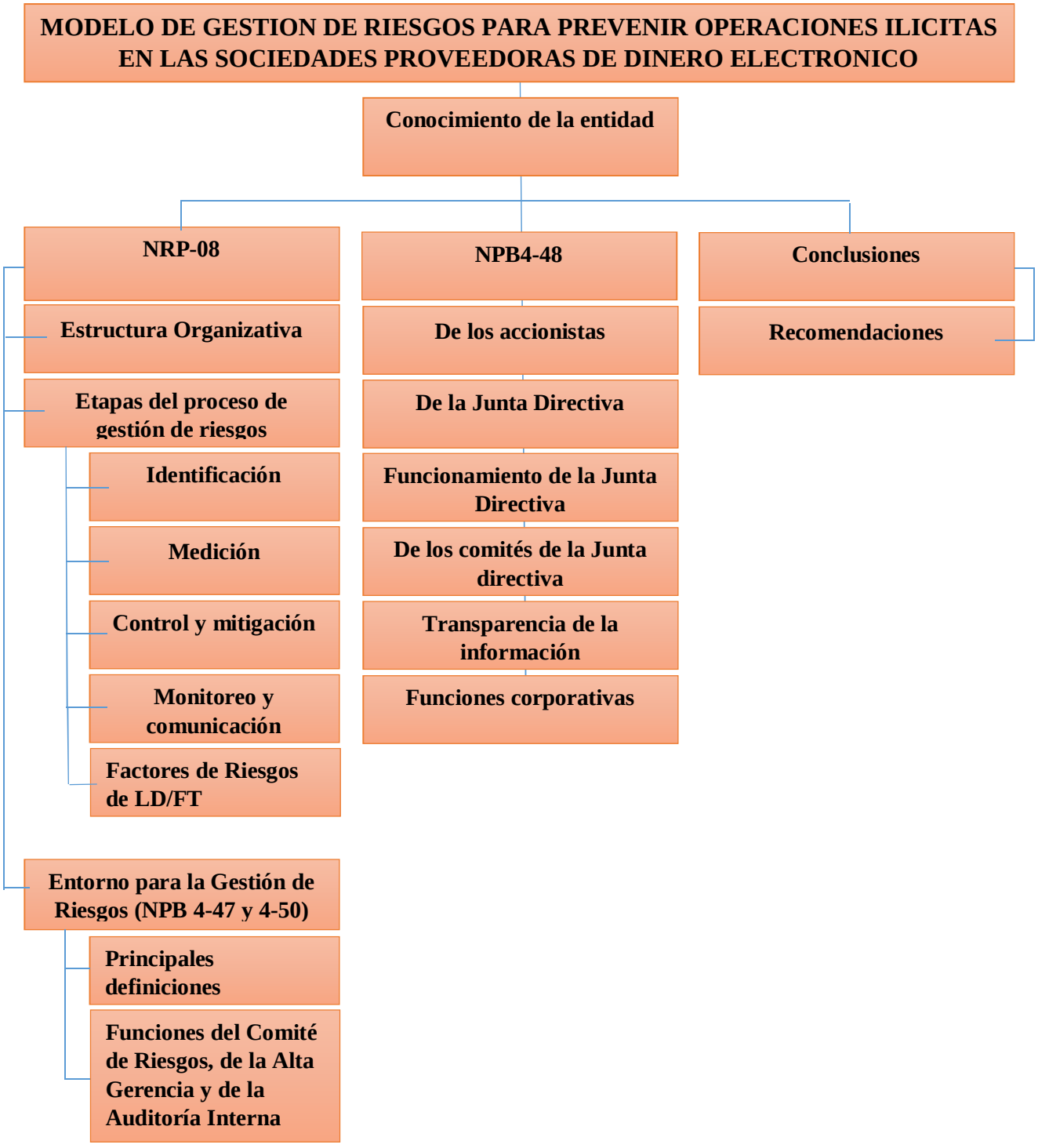
Propuesta de un modelo de gestión de riesgo para Sociedades Proveedoras de Dinero Electrónico.

Elaborado por:

Raúl Godínez
Nyree Álvarez
Daniel Flamenco

Presentado como parte del Trabajo de Graduación para optar al grado de Licenciados en Contaduría Pública.

Esquema del modelo propuesto



Fuente: *Elaborado por el grupo de trabajo*

Figura 1. Estructura basada en las "Normas Técnicas para la Gestión de los Riesgos de Lavado de Dinero y de Activos, y de Financiamiento al Terrorismo" (NRP-08), la Normas para la Gestión Integral de Riesgos de las Entidades Financieras (NPB4-47), Normas de Gobierno Corporativo (NPB4-48) y Normas para la Gestión de Riesgo Operacional de las Entidades Financieras (NPB4-50).

Conocimiento de la entidad

MON-E S.A. es una Sociedad Proveedora de Dinero Electrónico (SPDE) que opera desde el año 2012, brindando a sus usuarios una plataforma tecnológica vanguardista en la que pueden realizar pagos de servicios, recargas móviles, envíos de dinero, y hasta recibir remesas internacionales. Contando a la fecha con más de 100 comercios afiliados y 250 mil de usuarios, siendo un referente de compromiso y entrega en las operaciones que realizan.

Pero la sociedad no está autorizada oficialmente aún por la Superintendencia del Sistema Financieros como Sociedad Proveedora de Dinero Electrónico, la Junta Directiva decide iniciar dicho proceso de autorización, lo que conlleva cumplir con ciertos requisitos, y dando cumplimiento a los requerimientos establecidos por la Superintendencia del Sistema Financiero (SSF) y a las normativas emitidas por el Banco Central de Reserva de El Salvador (BCR) -respecto a la gestión de riesgos, inicia dicho proceso un año después de haber entrado en vigencia la Ley para facilitar la inclusión Financiera. Cabe mencionar que para el año que comenzó a operar aún no existía un marco legal ni normativo que regulara las operaciones de este tipo sociedad por lo que sus servicios eran prestados de acuerdo a lineamientos internacionales que regían a su casa matriz y referente locales y/o regionales de actividad económica similar.

En este sentido, resultó necesario conocer los aspectos generales de mayor relevancia de la empresa que podrían convertirse más fácilmente en factores de riesgos en el cometimiento de ilícitos, para gestionarlos o prevenirlos.

Los datos generales de la sociedad son importantes para entender mejor la propuesta y los mismos se detallan en la ficha técnica siguiente:

- Nombre de la empresa: Mon-E, Sociedad Anónima
- Actividad principal: Proveer dinero electrónico

- Dirección: 87 avenida norte, Calle al mirador, Complejo World Trade Center, Torre Futura, No. 1010
- Áreas a evaluar: Operaciones, Legal e Informática
- Número de Identificación Tributaria: 0614-230215-101-0
- Número de Registro de Contribuyente: 10250-7
- Tipo de Gobierno: Junta Directiva

Misión y Visión

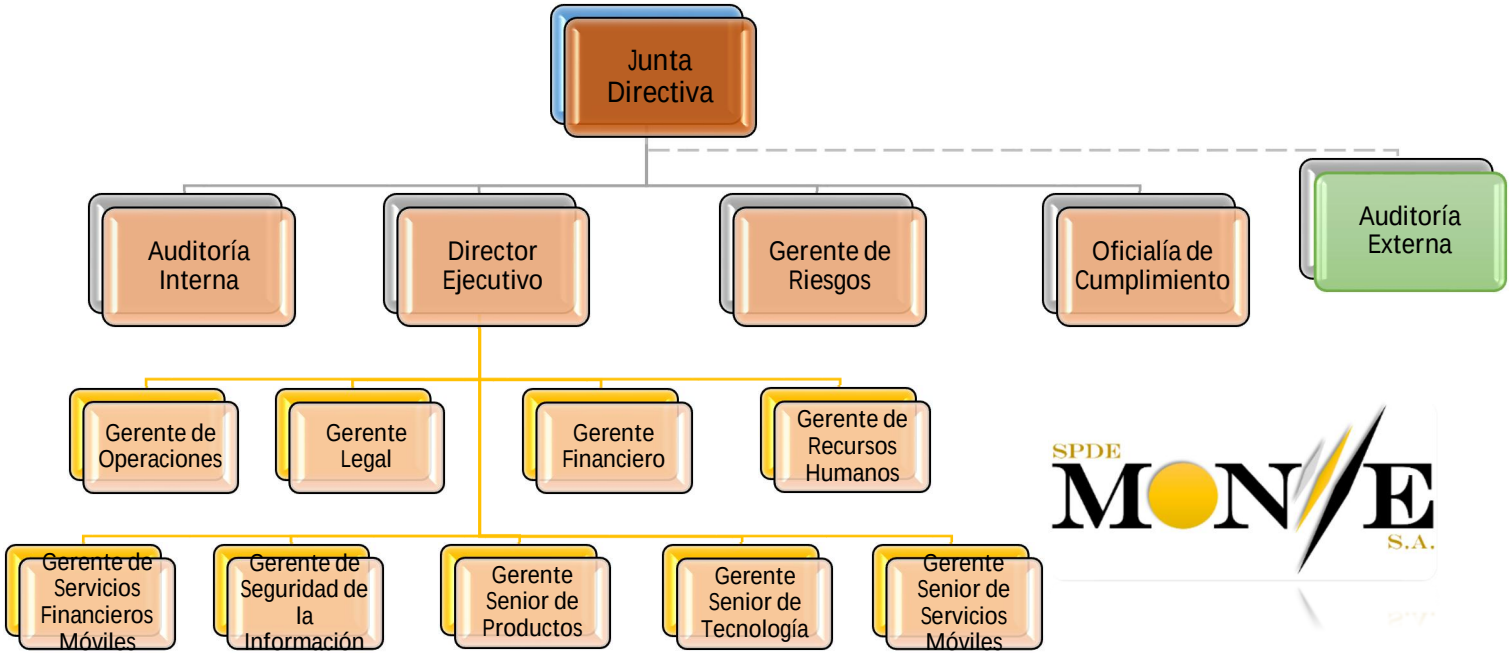
Misión de la entidad:

Proveer dinero electrónico de la manera más simple y segura.

Visión de la entidad:

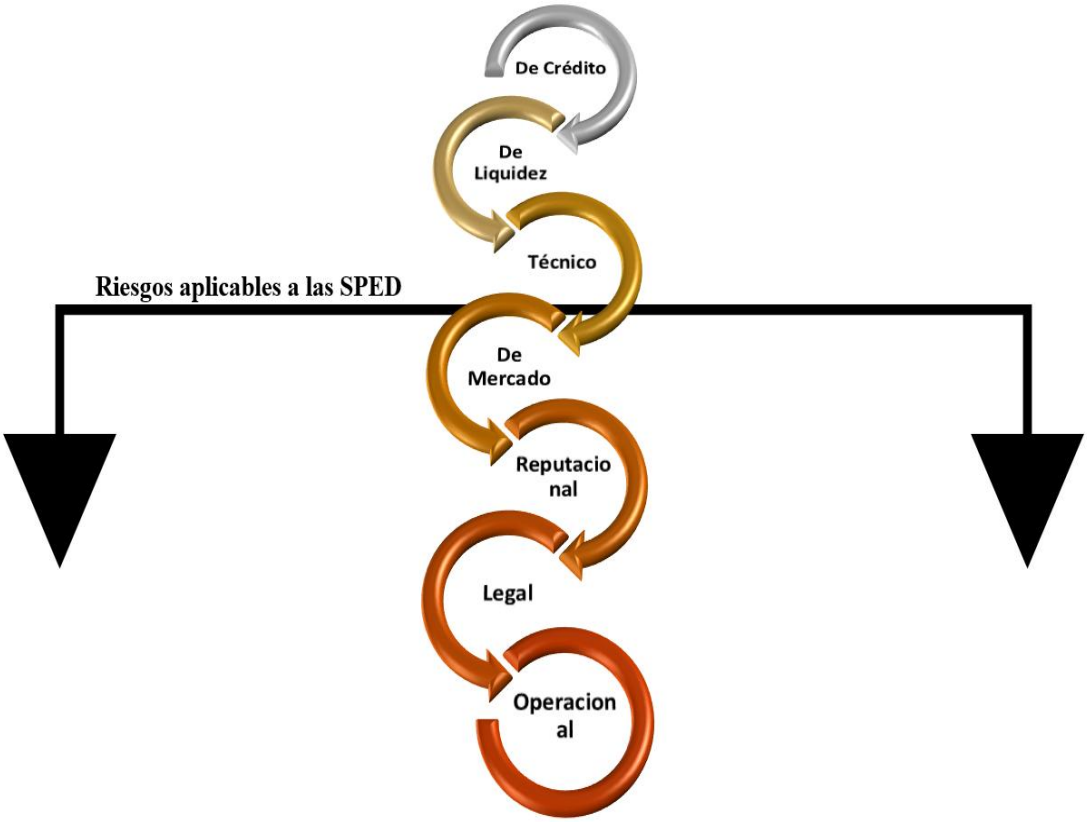
Ser la empresa líder a nivel regional en el servicio de proveer dinero electrónico, basándonos en los estándares más altos de calidad y de atención al cliente.

Estructura organizativa



Fuente: *Elaborado por el grupo de trabajo*

Figura 2. Ejemplificación de las áreas que intervienen en el funcionamiento de una Sociedad Proveedora de Dinero Electrónico; se puede apreciar la importancia que juegan los departamentos de segundo nivel, los cuales deben relacionarse estrechamente y compartir información para poder operar correctamente.



Fuente: Elaboración Propia

Figura 3. Según la clasificación hecha por las Normas para la Gestión Integral de Riesgos de las Entidades Financieras (NPB4-47), entre otros existen siete áreas en las que puede presentarse el riesgo para las instituciones del sistema bancario del El Salvador. Las Sociedades Proveedoras están obligadas a tomar en cuenta esta Norma, pero adaptándola a los riesgos aplicables para su giro.

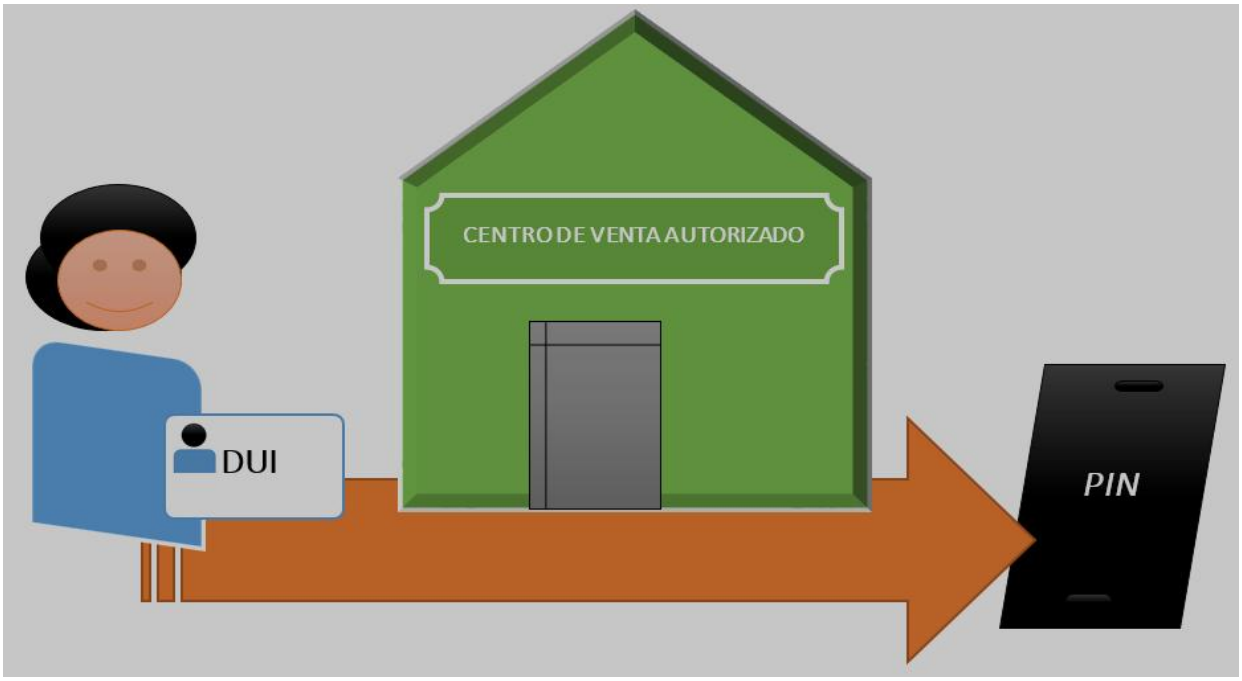
4.6 Definiciones y funcionamiento

4.6.1 Definiciones.

Para facilitar la asimilación se hace necesaria la definición de los siguientes términos:

Billetera Electrónica:

Las billeteras electrónicas son servicios de pago en línea que surgieron como resultado de la digitalización del comercio, y constituyen bienes monetarios propiedad de un individuo y que es equivalente al dinero físico, cuyo uso es de manera virtual pudiendo materializarse de acuerdo a



Fuente: *Equipo de trabajo.*

Figura 4. El proceso para recargar una billetera electrónica es acercarse a un centro de venta autorizado por la Sociedad Proveedora de Dinero Electrónico para tal efecto; presentar su DUI, el punto de venta transferirá la cuantía de dinero electrónico al móvil por el valor equivalente al importe del dinero físico recibido y una vez el dinero en el móvil ya puede hacerse uso de él, utilizando un código de seguridad propio de cada propietario.

ciertas condiciones del sistema que lo regula. Por ejemplo, una billetera electrónica solo puede realizar transacciones hasta un monto máximo semanal de un salario mínimo mensual del sector comercio y servicios (US$300.00 a la fecha) y el monto máximo de transacciones acumuladas en el mes, así como el saldo límite que pueden acreditar, no debe superar los cuatro salarios mínimos del sector mencionado según lo regula la más reciente circular, de fecha 9 de marzo de 2017, emitida por el Banco Central de Reserva al respecto.

Comercio Afiliado:

Persona Natural o Jurídica que cumpla con las condiciones contractuales previamente establecidas referente a la aceptación de dinero electrónico como medio de pago para que los usuarios puedan gastar, canjear o transferir el dinero contenido en sus billeteras electrónicas.

Usuario:

Persona Física dueña de una billetera electrónica.

Prevención:

Son las acciones orientadas a mitigar o evitar la ocurrencia de operaciones inusuales con impacto a los sistemas informáticos o a la Sociedad Proveedora en sí, son actividades de carácter permanente y con visión de largo plazo, como la investigación, promoción de prácticas adaptativas y capacitación.

Mitigación de Riesgo:

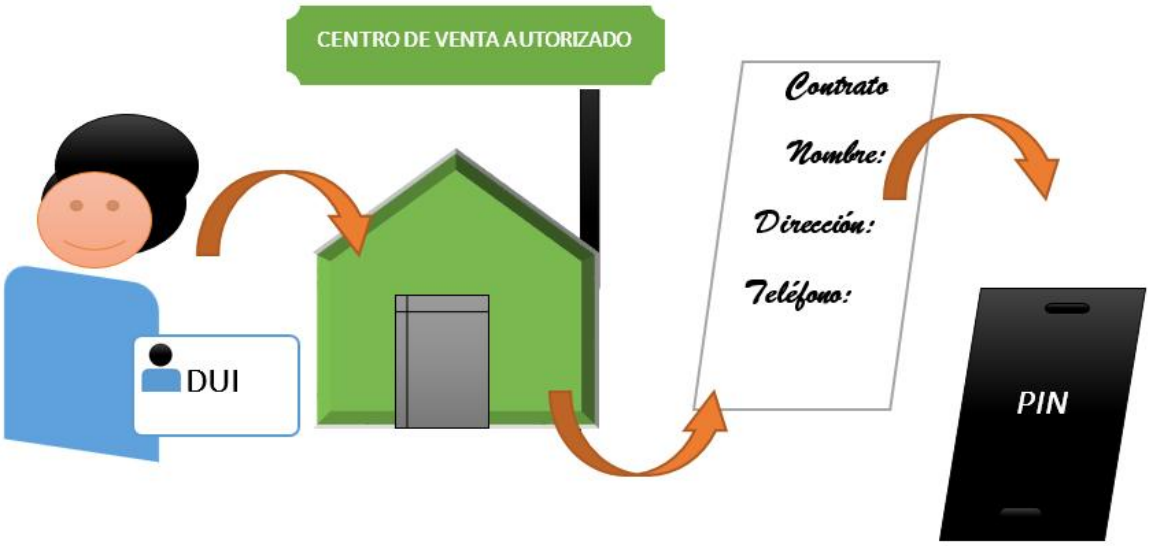
Son las medidas tendientes a reducir o mitigar el impacto de una operación ilícita o no usual.

Alerta:

Consiste en un estado de monitoreo permanente de la situación u operación ilícita y la correspondiente difusión cuando se advierte la probable y cercana ocurrencia de cualquier evento. Para ello, se requiere de comprensión del riesgo mediante capacidades científicas, técnicas e institucionales para observar, registrar, analizar, modelar y predecir las amenazas climáticas.

Preparación:

Son las medidas y acciones previas a un desastre cuya ocurrencia ha sido declarada como probable, así como la organización de procedimientos, de personal y los equipos de enfrentamiento.



Fuente: **Equipo de trabajo**

Figura 5: Los datos generales incluyen, entre otros, el Nombre de la persona titular de la cuenta, número de móvil, numero de DUI, etc. Todas estas formalidades deberán ser aceptadas por el nuevo usuario si desea utilizar una Billetera electrónica.

Respuesta:

Acciones que se llevan a cabo inmediatamente planes de acción propios de atención ante el evento, su objetivo es salvaguardar los sistemas informáticos y disminuir el impacto a nivel de organizacional, regional y nacional si corresponde.

Reconstrucción:

Consiste en el proceso de reparación del daño a un sistema informático, llevándolo a un nivel de desarrollo igual o superior al existente antes del evento.

Desarrollo y Adaptación:

Es la promoción de prácticas que contribuyan al incremento de la resiliencia de los sistemas informáticos de modo que puedan enfrentar y manejar de mejor manera los riesgos futuros. Incluye

la incorporación de la Gestión de Riesgo Administrativa en la planificación de mediano y largo plazo.

Riesgo de Crédito:

Es la probabilidad de pérdida debido a incumplimiento contractual de un prestatario a quien previamente se le otorgó un préstamo. (No aplica a las SPDE)

Riesgo de Liquidez:

Es la probabilidad de pérdidas por incumplimiento por no disponer de los fondos para con sus obligaciones asumidas con terceros. (No aplica a las SPDE)

Riesgo Técnico:

Es la probabilidad de pérdidas por inadecuadas bases técnicas o actuariales empleadas en el cálculo de primas y de las reservas técnicas de los seguros, insuficiencia en la cobertura o el aumento inesperado de gastos y de la distribución en el tiempo de los siniestros. (No aplica a las SPDE)

Como SPDE los riesgos en los que nos enfocamos en mitigar son los siguientes:

Riesgo de Mercado:

Es la probabilidad de pérdidas, producto de movimientos en los precios de mercado que generan un deterioro de valor en la posición dentro y fuera del balance o en los resultados financieros. (Puede aplicar a las SPDE).

Riesgo Legal:

Es la probabilidad de incumplir específicamente con las leyes locales del país en el que opera la entidad, que podría ocasionarle daños a la imagen. (Aplica a las SPDE)

Riesgo Reputacional:

Es la probabilidad de incurrir en pérdidas producto del deterioro de la imagen de la entidad, debido a incumplimientos de leyes, normas internas, códigos de Gobierno Corporativo, de conducta, lavado de dinero, entre otros. (Aplica a las SPDE).

Riesgo Operacional:

Es uno de los más comunes y por tanto uno a los que mayor cuidado y recursos debe proporcionarle la entidad; es la probabilidad de incurrir en pérdidas debido a fallos en los procesos, el personal, los sistemas informáticos y a causa de factores de riesgos externos como el Lavado de Dinero y Activos (LD/FT) abordados en la NRP-08. (Aplica a las SPDE)

4.6.2 Funcionamiento de la plataforma.

La SPDE brinda sus servicios por medio de una plataforma virtual que almacena cada billetera electrónica de su cliente, estas son administradas por cada propietario, y con el afán de garantizarle una experiencia grata al momento de realizar transacciones y efectuar sus pagos con la mayor sencillez posible, se explica a detalle el funcionamiento de esta.

Registro de usuario:

Para darse de alta como usuario de Dinero Electrónico es necesario crear un usuario y una contraseña, además de llenar la información general solicitada, una vez terminados todos los

campos, es recomendable leer los términos y condiciones para luego aceptarlos.

Pagos electrónicos

Estos pueden realizarse de tres formas:

a) Por medio de la aplicación ingresando a la sección de pagos, y eligiendo entre las distintas opciones desplegables el que más se adapte al pago a realizar (NPE, número de teléfono o código de cliente), introducir el monto y luego confirmar. Se recibirá un mensaje de confirmación del pago realizado.

b) Por medio del comando USSD[1]. Marcando *1111#[2] y elegir entre las opciones disponibles que más se adapte a la necesidad del usuario, luego ingresar el monto y el destinatario y confirmar.

c) En punto autorizado. Si por alguna razón el usuario no tuviera acceso a las dos opciones anteriores, puede acercarse al punto autorizado más cercano y realizar el trámite con la portación única del Documento Único de Identidad y llenando un formulario detallando el tipo de transacción a realizar.

Transferencias:

Para transferir dinero electrónico es básicamente el mismo uso anterior con las variantes que el usuario seleccionara la opción Transferencias en las primeras dos modalidades o solicitar al encargado del punto autorizado que realice la transacción llenando el formulario proporcionado por este, elegir el monto y listo.

[1] USSD son siglas en ingles de Unstructured Supplementary Service Data – Datos de Servicio Suplementario no Estructurados, un servicio interactivo de comunicación GSM que permite un servicio fácil de usar y al que puede accederse desde cualquier equipo aun sin acceso a internet y tenerse una respuesta casi instantánea. A diferencia de un Mensaje de texto tradicional, la comunicación USSD no se almacena en la memoria del teléfono, lo que lo convierte en información sensible. (www.infobip.com)

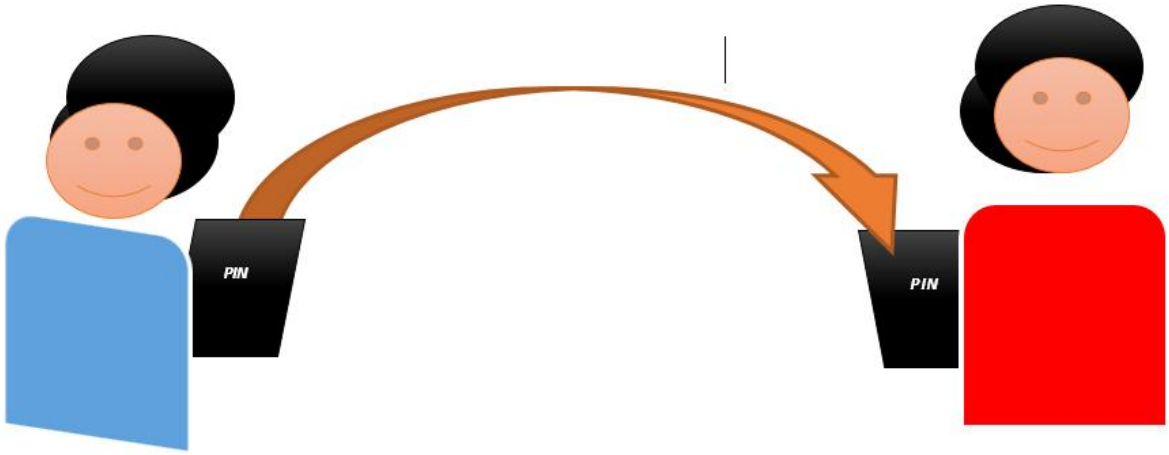
Abonar o retirar dinero electrónico:

Para abonar saldo a tu billetera electrónica solamente es de acercarse a un punto autorizado y solicitarla como una recarga normal de saldo aire, especificando el número telefónico ligado a la billetera virtual, se recibirá un mensaje de confirmación y listo.

Para retirar dinero es importante acercarse a un punto autorizado, llenar formulario con la opción retiro en efectivo y exhibir el Documento Único de Identidad (DUI), confirmar la cantidad a retirar y recibirá una confirmación en el móvil de la cantidad de dinero que se descontará de la billetera electrónica.

Costo por retiros de dinero:

El retiro de dinero propio o envíos tiene un costo del 4 por ciento, para recibos internacionales (remesas internacionales) o proveniente de salarios no tiene costo alguno.



Fuente: *Equipo de trabajo.*

Figura 6. Las transferencias, pagos o recibos de dinero electrónico suponen la utilización rigurosa de un código de seguridad el cual es introducido por el que envía los fondos y de igual manera es necesario que el receptor lo acepte.

4.7 Gestión integral de riesgos (NRP-08 y NPB 4-47)

4.7.1 Clasificación de Riesgos según las Normas para la Gestión Integral de riesgos de las entidades Financieras (NPB 4-47)

Uno de los primeros pasos en la Gestión de Riesgo en SPDE MON-E, S.A. es segmentarlos para poder ser tratados por separado de acuerdo a su origen, características y diseño estructural e impacto. La figura 2 muestra la clasificación de riesgos a la que puede estar expuesta generalmente una SPDE de acuerdo con su naturaleza.

4.7.2 Sistema de gestión integral de riesgos

En base a lo señalado por las Normas Técnicas para la Gestión de los riesgos de Lavado de Dinero y de Activos, y de Financiamiento al Terrorismo (NRP-08), las cuales señalan que “las entidades deberán establecer un sistema de gestión integral de riesgos, que deberá entenderse como

un proceso estratégico realizado por toda la entidad, mediante el cual identifican, miden, controlan y monitorean los distintos tipos de riesgos de LD/FT.

Identificación de Riesgos

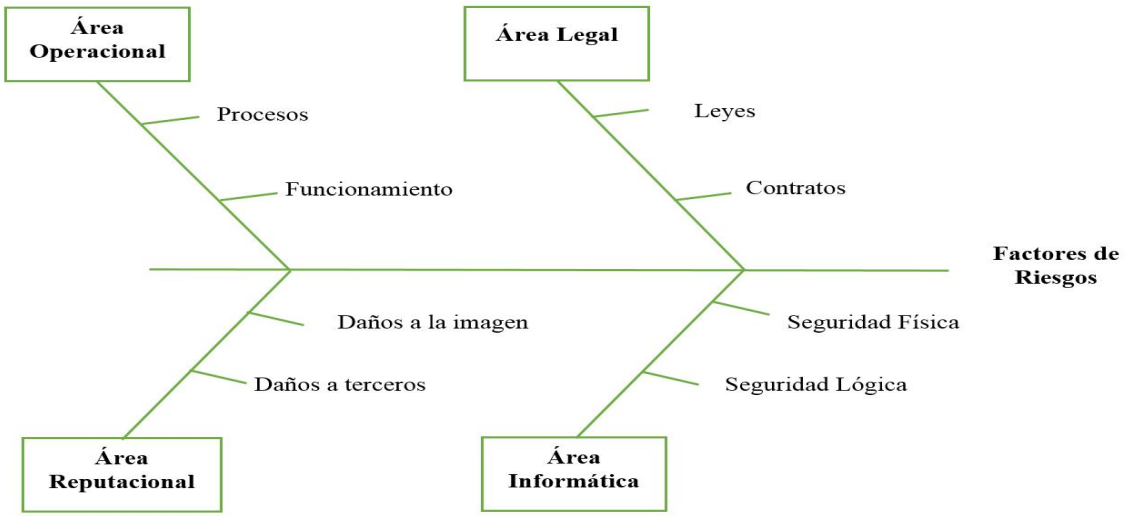


Figura 7. Esquema tipo espina de pescado, se representa los cuatro bloques en los cuales se agrupan los factores de riesgo identificados:

a que se encuentran expuestas y las interrelaciones que surgen entre estos, para proveer una seguridad razonable en el logro de sus objetivos. Dicha gestión deberá estar acorde a la magnitud de sus actividades, negocios y recursos de la entidad". (pg. 1 - Art. 3)

Asimismo con base a lo señalado por las Normas Técnicas para la Gestión de los Riesgos de Lavado de Dinero y de Activos, y de Financiamiento al Terrorismo (NRP-08) que establecen que las "entidades financieras adoptarán políticas, reglas, y mecanismos de conducta (…) desarrollarán y ejecutarán programas, normas, procedimientos y controles internos para prevenir las actividades relacionadas con el delito de lavado de dinero y de activos.", SPDE MON-E, S.A. se centra en gestionar, de manera especial, los riesgos de mercado, reputaciones, legal y operacional (los señalados en la figura 4).

CUESTIONARIO DE CONTROL INTERNO
Aplicado a Sociedades Proveedoras de Dinero Electrónico (SPDE)

Referencia: CCI

Fecha de Auditoría de Gestión al 31 de diciembre de 2017

Objetivo general:

- Conocer los controles que ejecuta el área de operaciones para la prevención de riesgos de transacciones ilícitas.

Objetivos específicos:

- Identificar los procedimientos de control interno implementado en las operaciones de la SPDE.
- Obtener información sobre los controles aplicados por el área relacionados a la prevención de operaciones ilícitas según NRP-08.

Indicaciones:

Marque la respuesta que considere correctamente a la aplicabilidad de los controles.

No.	Pregunta	Si	No	Comentario
ASPECTOS OPERATIVOS				
1	¿El área de operaciones cuenta con un manual de procedimientos por escrito?	✓		
2	¿El manual de procedimientos se actualiza periódicamente?	✓		
3	¿Se informa a todo el personal involucrado en el área cuando hay cambios en el manual de procedimientos?	✓		
4	¿El manual de procedimientos posee controles para mitigar los riesgos para prevenir operaciones ilícitas?	✓		Solo para operaciones internas
5	¿Existen parámetros para determinar que una operación es ilícita?	✓		Solo para operaciones internas
6	¿Se gestionan los riesgos de actividades ilícitas mediante el uso de las plataformas electrónicas de dinero?		✓	
7	¿Se capacita al personal en la identificación de operaciones ilícitas?	✓		Solo para operaciones internas
8	¿Se elabora un control de las operaciones catalogadas como ilícitas?	✓		Solamente en función a movimientos sospechosos no así en función de los usuarios y zonas de donde se realizan
9	¿Se verifican los procedimientos de registro de usuarios a la plataforma electrónica?		✓	No se le ha dado la importancia que amerita
10	¿Se realizan inspecciones de los documentos utilizados en el registro de usuarios?		✓	No se le ha dado la importancia que amerita
11	¿Se ha identificado zonas de alto riesgo más expuestas al cometimiento de ilícitos relacionados al lavado de dinero y activos?		✓	No se le ha dado la importancia que amerita
12	Pueden aperturarse corresponsales en zonas de alto riesgo delincuencial?		✓	No se le ha dado la importancia que amerita

13	¿Se realizan evaluaciones periódicas a los corresponsales sobre la efectividad de los controles para prevenir operaciones ilícitas?		✓	No se le ha dado la importancia que amerita
14	¿Existe un control en la plataforma para evitar exceder los montos de las transacciones legalmente establecidas?	✓		Solamente por medio de parametrización del sistema
15	¿El área cuenta con políticas para evitar la fuga de información por parte de los empleados?		✓	No se han establecido políticas
16	¿El sistema se actualiza periódicamente?	✓		Depende del proveedor del software
17	¿El sistema está delimitado geográficamente únicamente en el territorio nacional?			En función alcance y cobertura de la red telefónica.
18	¿El área de operaciones cuenta con controles por escrito en caso de caídas del sistema?		✓	
ASPECTOS LEGALES				
19	¿El área legal cuenta con un manual de procedimientos por escrito?		✓	Se depende de las necesidades que surgen
20	¿El manual de procedimientos se modifica periódicamente en base a cambios en las regulaciones normativas y legales?		✓	No hay manual
21	¿Se informa a todo el personal involucrado en el área cuando hay cambios en el manual de procedimientos?		✓	No hay manual
22	¿El personal cuenta con capacitaciones periódicas en materia legal y normativa?		✓	
23	¿Los contratos con clientes y acreedores se actualizan en la medida surgen cambios que les son aplicables?		✓	Una vez firmados no se modifican
24	¿Se verifica el fiel cumplimiento de obligaciones de todos los contratos realizados?	✓		
25	¿Existen procedimientos establecidos en caso de incumplimiento de contratos?	✓		
26	¿Están debidamente registrados todos los derechos de marcas y distintivos comerciales?	✓		
27	¿Se cuenta con procedimientos para ejercer el derecho de la buena imagen de la empresa?	✓		
ASPECTOS REPUTACIONALES				
28	¿Existen controles para identificar la suplantación de identidad de un usuario en la plataforma electrónica?		✓	No se ha tomado en consideración
29	¿Se realizan encuestas para percibir la opinión de los usuarios del dinero electrónico?		✓	
30	¿Se realizan esfuerzos para identificar posibles operaciones sospechosas relacionadas al cobro de extorciones?	✓		
ASPECTOS INFORMATICOS				
SEGURIDAD FÍSICA				

31	¿El área de informática cuenta con un manual de procedimientos por escrito?		✓	
32	¿El manual de procedimientos se actualiza periódicamente?		✓	
33	¿Se informa a todo el personal involucrado en el área cuando hay cambios en el manual de procedimientos?		✓	
34	¿El manual de procedimientos posee controles para mitigar los riesgos para prevenir operaciones ilícitas?		✓	
35	¿Se destinan recursos suficientes a las actividades de investigación y desarrollo?	✓		
36	¿Cuenta con Cámaras de Video vigilancias en los lugares físicos donde se encuentran los equipos tecnológicos utilizados?	✓		
37	¿Solo personal autorizado ingresa al centro de cómputo y se hace uso de la bitácora del centro de cómputo?	✓		
38	¿El personal ingresa con comida o bebida al centro de cómputo?		✓	
39	¿Se cuenta con tecnología detectora de humo en lugares ocupados por equipo tecnológico?	✓		
40	¿Los equipos están fuera del alcance de tuberías y desagües?	✓		
41	¿Están protegidos contra el polvo?	✓		
42	¿Las habitaciones están equipadas con aire acondicionado?	✓		
43	¿Los Gabinetes están anclados al piso y techo?	✓		
44	¿Los equipos están instalados en un aproximado de 20 cm de la superficie de suelo?	✓		
45	¿Existen fuentes de energía propias que no dependan de la corriente eléctrica general?	✓		
46	¿Cuenta con equipos UPS (Suministro de Energía Ininterrumpida), conectados a los equipos informáticos?	✓		
47	¿La edificación cuenta con Luces de Emergencia?	✓		
48	¿Los cables de la red eléctrica y de comunicaciones están separados para evitar interferencias?	✓		
SEGURIDAD LÓGICA				
49	¿El sistema cuenta con parámetros establecidos para catalogar una operación como sospechosa o ilícita?	✓		Parámetros específicos
50	¿El sistema fue aprobado por el comité de riesgos?	✓		
51	¿El sistema cuenta con respaldo de un proveedor externo en la solución de problemas o errores?	✓		

52	¿Están debidamente segregadas las funciones de cada empleado del departamento respecto a los módulos con los que necesita?	✓		
53	¿El sistema solicita para el acceso un usuario y contraseña?	✓		
54	¿Los usuarios pueden ingresar al sistema desde fuera de las instalaciones de la empresa?		✓	Depende de la necesidad que requiere cada usuario
55	¿El sistema posee accesos restringidos para cada usuario?	✓		
56	¿Las computadoras del cuentan con acceso a internet ilimitado?	✓		
57	¿Las computadoras del tienen acceso restringido para sustraer información a través de medios de almacenamiento externo?		✓	
58	¿Cuenta el sistema con protecciones confiables en caso de ataques por parte de “hackers”?	✓		
59	¿Todas las licencias informáticas del área son originales?	✓		
60	¿Cuenta la empresa con licencias originales de antivirus y “antimalwares”	✓		
61	¿El sistema está montado sobre una infraestructura adecuada?	✓		Aunque a veces muestra fallos menores
62	¿Se realizan “back ups” de toda la información almacenada en las bases de datos?	✓		
63	¿El resguardo de la información está debidamente protegido?	✓		
64	¿Los empleados que utilizan el sistema de información están conformes con respecto a la confiabilidad y oportunidad de los informes que emiten dichos sistemas?	✓		
65	¿Existen resguardos apropiados de la información contra alteraciones, pérdidas y falta de confidencialidad?	✓		
66	¿Se han definido los responsables de implantar, documentar, probar y aprobar cambios en los sistemas de información?	✓		
67	¿Existe apoyo de la Dirección hacia la implantación de nuevos y más aptos sistemas de información?	✓		
68	¿Se destinan recursos suficientes para mejorar o desarrollar sistemas de información operativos?		✓	
69	Hay conciencia de la necesidad de definir requerimientos y de identificar soluciones tecnológicas.	✓		
70	Los jefes de áreas tienden a reunirse para discutir necesidades de manera informal de	✓		

	aquellos detalles que por lo general no están documentados.			
71	Se consideran soluciones alternativas, incluyendo un análisis de costos y ganancias.	✓		
CONTRA EL LAVADO DE DINERO (NRP-O8)				
72	¿Se ha aprobado un manual para la prevención de prácticas de lavado de dinero y financiamiento al terrorismo?	✓		
73	¿Se revisa y actualiza el manual cada año?		✓	
74	¿Se cuenta con una oficialía de cumplimiento para presidida por un oficial de cumplimiento?	✓		
75	¿Cuál es el cargo que el Oficial de Cumplimiento desempeña dentro de la empresa?			Exclusivamente fue contratado para Oficial de Cumplimiento.
76	¿Se recibe el apoyo adecuado de parte de la administración para ejecutar los oficios adecuados en la prevención de lavado de activos y financiamiento al terrorismo?	✓		
77	¿La Oficialía de Cumplimiento incluye 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?		✓	
78	¿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?	✓		
79	¿Se elaboran políticas y procedimientos de prevención de LD/FT para su posterior aprobación por la Junta Directiva u Órgano de Administración?	✓		
80	¿Se elabora 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?	✓		
81	¿La Auditoría Interna evalúa la gestión de la Oficialía de Cumplimiento e informa a la Junta Directiva tanto de los hallazgos de auditoría en la materia como de los resultados de la evaluación de la gestión de la Oficialía?	✓		
82	¿Se cuenta con una base de datos de Personas Expuestas Políticamente (PEP´s?		✓	

Observaciones:

_____

Elaborado por: **Revisado por:**

PROGRAMA DE AUDITORÍA PARA EVALUAR EL CONTROL INTERNO DEL ÁREA DE OPERACIONES REALIZADO POR LA SPDE

Empresa: SPDE, S.A.	
Nombre del papel de trabajo: PROGRAMA DE CONTROL INTERNO OPERATIVO	Índice de papeles de trabajo
Ejercicio: Del 01 de enero al 31 de diciembre de 2017	Ref.: PT:

OBJETIVO:

- Verificar la aplicación de los controles implementados por la Compañía en el área de operaciones dirigidos a gestionar operaciones ilícitas relacionadas a Lavado de Dinero y Financiemiento al Terrorismo (LD/FT)..

ALCANCE:Revisión de reporte de transacciones realizadas en la plataforma y cumplimientos establecidos por la Superintendencia del Sistema Financiero.

No.	Descripción	Ref.	Fecha
1	Solicitar a la Administración el flujograma de los procedimientos de las áreas de operaciones de la compañía.		
2	Verificar que las políticas han sido autorizadas por la administración de la entidad.		
3	Elaborar una narrativa del procedimiento a seguir para el registro de usuarios en la plataforma		
4	Verificar si existen transacciones de un mismo usuario que superan el monto de US$300 semanales y US$1,200.00 acumulados en el mes, límites establecidos por la Superintendencia del Sistema Financiero.		
5	Solicitar listado de los lugares considerados por la sociedad como de alto riesgo.		
6	Solicitar a la administración listado de corresponsales situados en zonas de alto riesgo.		
7	Solicitar comprobantes de las capacitaciones y/o evaluaciones realizadas al personal.		
8	Solicitar comprobantes de las actualizaciones realizadas al sistema.		
9	Solicitar reportes de las evaluaciones realizar por el Comité de Riesgo.		

Observaciones	
Elaborado por	Fecha
Supervisado por	Fecha

CONCLUSIONES Y HALLASGOS OPERATIVOS ENCONTRADOS

Se observó que los riesgos relacionados con la identificación de clientes, su manejo e interacción con ellos es limitada y se hace énfasis en la importancia de fortalecer los controles en esta área debido a que se encontraron los siguientes factores de riesgos:

1 No existencia controles para verificar el registro de usuarios

2 Suplantación de identidad (Phishing)

3 Operaciones en zonas de alto nivel de criminalidad

4 Exceder los montos establecidos legalmente

5 Actividades fraudulentas de empleados

6 Permitir que trabajos informáticos se lleven a cabo fuera la empresa

7 No motivación de empleados

8 No contar con un programa de actualización constante del software

9 Riesgos Transfronterizos

10 Falta de políticas de confidencialidad

11 Dependencia de un proveedor informático externo.

La correcta aplicación y supervisión del sistema actual de control interno es prioritaria para evitar errores, facilitando la corrección de los ya cometidos y tomar experiencia para otros nuevos que pudieran surgir en el futuro.

PROGRAMA DE AUDITORÍA PARA EVAUAR ASPECTOS LEGALES

Empresa: SPDE MONE, S.A.				
Nombre del papel de trabajo: PROGRAMA DE AUDITORÍA PARA EVAUAR ASPECTOS LEGALES			Índice de papeles de trabajo	
Ejercicio:	Del 01 de enero al 31 de diciembre de 2017		Ref.:	PT:

OBJETIVO:

- Verificar la ejecución de los controles implementados por la Compañía en el área legal.

ALCANCE:

- Revisión de contratos vigentes de la Compañía.

No.	Descripción	Ref.	Fecha
1	Solicitar las políticas de control interno para la elaboración de contratos.		
2	Solicitar a la Administración flujograma de los procesos para la creación y autorización de contratos.		
3	Verificar que las políticas han sido autorizadas por la administración de la entidad.		
4	Realizar lectura de Actas de Junta General Accionistas y Junta Directiva para identificar las personas autorizadas a negociar y hacer contratos en nombre de la Compañía.		
5	Inspeccionar que los contratos estén resguardados en lugares con adecuadas medidas de seguridad.		
6	Realizar lectura de contratos para identificar obligaciones contraídas por la compañía y su cumplimiento.		
7	Solicitar a la Administración manifestación por escrita del listado de Asesores Legales externos que hayan prestado sus servicios a la Compañía.		
8	Verificar el cumplimiento de los contratos de confidencialidad firmado por los empleados de acuerdo al desempeño de sus funciones.		

Observaciones			
Elaborado por		Fecha	
Supervisado por		Fecha	

PROGRAMA DE AUDITORÍA PARA VERIFICAR EL CONTROL INTERNO DEL ÁREA DE INFORMÁTICA REALIZADOS POR LA SPDE

Empresa:			
Nombre del papel de trabajo:		Índice de papeles de trabajo	
Ejercicio:	Del 01 de enero al 31 de diciembre de 2017	Ref.:	PT:

OBJETIVO:

- Verificar la ejecución de controles aplicados por el área de informática a la plataforma de dinero electrónico.

ALCANCE:

- Revisión de procesos de TI.

No.	Descripción	Ref.	Fecha
1	Solicitar las políticas de control interno por escrito del área de informática		
2	Solicitar a la Administración flujograma de los procesos del Departamento de TI.		
3	Verificar que las políticas han sido autorizadas por la Administración de la entidad.		
4	Solicitar detalles de la parametrización del sistema		
5	Indagar si el sistema fue comprado a un proveedor externo o es un programa hecho a la medida de las necesidades de la Compañía (In house)		
6	Solicitar a la Administración manual de funcionamiento del sistema		
7	Verificar la existencia de sistemas de claves o contraseñas para acceder al sistema en base a la segregación de funciones		
8	Inspeccionar la periodicidad con la que son cambiadas las claves de accesos al sistema		
9	Verificar que las computadoras estén en lugares que cumplan con normas adecuadas de seguridad (Lugar seguro, ambiente adecuado, equipos de protección)		
10	Confirmar la existencia de respaldos periódicos de la información del sistema		
11	Confirmar que los equipos cuentan con licencias informáticas originales		
12	Verificar la existencia de cláusulas o cartas de fidelidad de los encargados del funcionamiento del sistema		

Observaciones			
Elaborado por		Fecha	
Supervisado por		Fecha	

CONCLUSIÓN Y RIESGOS LEGALES, REPUTACIONALES E INFORMÁTICOS IDENTIFICADOS.

Debido a que la entidad no poseía manuales de procesos específicos para el área legal, Reputacional ni informáticos, los factores se generalizan, lo que podría ocasionar nuevos riesgos con mayores impactos.

Los riesgos identificados en estas áreas se detallan a continuación:

RIESGOS DE POR INCUMPLIMIENTO LEGAL

12 Incumplimiento de leyes, normas y reglamentos.

13 Incumplimiento de derechos y obligaciones con terceros

RIESGOS REPUTACIONALES

14 Daños a la imagen

15 No cumplir con las expectativas de los clientes

16 No existencia de controles específicos para identificar cobro de Extorsión

RIESGOS INFORMÁTICOS

17 Accesos no autorizados a almacenes de información

18 Ataques al sistema

19 Inadecuada infraestructura del sistema

PROGRAMA DE AUDITORÍA PARA VERIFICAR CONTROLES RELACIONADOS CON EL LAVADO DE DINERO Y DE ACTIVOS.

Empresa:			
Nombre del papel de trabajo:		Índice de papeles de trabajo	
Ejercicio:	Del 01 de enero al 31 de diciembre de 2017	Ref.:	PT:

OBJETIVO:

- Verificar el cumplimiento de los lineamientos establecidos en la Ley Contra el Lavado de Dinero y de Activos y en las Normas Técnicas para la Gestión de los Riesgos de lavado de Dinero y de Activos, y de Financiamiento al Terrorismo (NPR-08).

ALCANCE:

- Revisión general de aspectos contenidos en la NRP-08.

No.	Descripción	Ref.	Fecha
1	Solicitar las políticas de control interno por escrito del área de la Oficialía de Cumplimiento		
2	Verificar que las políticas han sido autorizadas por la Administración de la entidad.		
3	Solicitar los documentos que comprueben la debida inscripción de Oficial de Cumplimiento en la Unidad de Información Financiera (UIF).		
4	Verificar si existe un plan anual que incluya programas de capacitación, en atención a lo dispuesto en el Art. 35 literal “j” de la Ley de Supervisión y Regulación del Sistema Financiero		
5	Verificar la existencia de matrices 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		
6	Solicitar a Auditoría Interna las conclusiones realizadas de la gestión de la Oficialía de Cumplimiento, tanto de los hallazgos de auditoría en la materia como de los resultados de la evaluación de la gestión de la Oficialía		
7	Revisar la existencia de una base de datos de Personas Expuestas Políticamente (PEP´s), cual es la relación con estas personas y si se toma la debida diligencia.		

Observaciones			
Elaborado por		Fecha	
Supervisado por		Fecha	

CONCLUSIÓN DE LA REVISIÓN A ASPECTOS RELACIONADOS CON EL LAVADO DE DINERO Y FINANCIEMIENTO AL TERRORISMO.

La Oficialía de Cumplimiento está funcionando razonablemente en base a las disposiciones contenidas en la Ley Contra el Lavado de Dinero y de Activos y en las Normas Técnicas para la Gestión de los Riesgos de lavado de Dinero y de Activos, y de Financiamiento al Terrorismo (NPR-08).

Por otra parte, importante melonar la importancia incluir en su plan anual, capacitaciones a todos los empleados de las demás en materia de Lavado de Dinero, lo que generaría ciertas deficiencias y el riesgo de estas prácticas se eleva.

MON-E, S.A. DE C.V
Matriz de riesgos identificados en las distintas áreas de la sociedad.

A continuación, se presentan la matriz de riesgos identificados por medio de Cuestionario de Control Interno, su descripción, las causas que los generan y sus posibles consecuencias.

Tabla 1. Criterios de identificación de riesgos basados en la Norma Prudencial de Bancos 4-47.

ID	Riesgo	Descripción	Causa	Efecto
AREA OPERATIVA				
1	No existencia controles para verificar el registro de usuarios	La posibilidad de abrir múltiples cuentas para esconder el valor real de los depósitos utilizando varias personas	Los nombres sospechosos no pueden ser capturados por sistema, permitiendo el ocultamiento de criminales y terroristas y extorsionistas	Movimiento de fondos ilícitos asociados con el terrorismo
2	Suplantación de identidad (Phishing)	Probabilidad que un usuario se registre con documentación falsa o de otra persona.	Falta de controles para verificar la autenticación de los documentos al momento de der de alta a un usuario.	Daños a la imagen de la Sociedad Proveedora e implicaciones legales que pueden traducirse a multas por no aplicar la Debida Diligencia sugerida por la Ley contra el Lavado de Dinero y de Activos.
3	Operaciones en zonas de alto nivel de criminalidad	Las ubicaciones de donde se realizan las transacciones su frecuencia podrían arrojar indicios claves de riesgo.	No controlar ni rastrear la ubicación geográfica de cada transacción y las frecuencias con las que estas se realizan.	Problemas legales por la involuntaria Contribución de manera con actos delincuenciales por desconocer la importancia de este factor
4	Exceder los montos establecidos legalmente	No parametrización eficiente del sistema que evite exceder los límites preestablecidos legalmente.	Deficiencia de controles, ausencia o no aplicación de los mismos, confiando a que el sistema esta parametrizado.	Sanciones por Incumplimiento a la Circular de fecha 9 de marzo de 2017 “Ajuste a los Limites Máximo Establecido en la Ley para Facilitar la Inclusión Financiera para Registros de Dinero Electrónico y Depósitos en cuenta de ahorro con

				Requisitos simplificados”
5	Actividades fraudulentas de empleados	Acciones de empleados en contra de la Sociedad Proveedora que pueden comprometerla o dañarla.	Descontentos o represalias que pueden llevar a un empleado a actuar por sí mismo o colusionar con otro u otros en perjuicio de la Sociedad Proveedora.	Daños a la infraestructura física o informática de la empresa, además de fugas de información que podrían colocarla en desventaja ante la competencia.
6	Permitir que trabajos informáticos se lleven a cabo fuera la empresa	Pérdidas de información confidencial propiedad de la Sociedad Proveedora	Olvido de documentos, portafolios, dispositivos USB o cualquier otro artículo que pueda contener datos importantes que podrían comprometer o debilitar su funcionamiento.	No competitividad ante la competencia, o vulnerabilidad ante personas capaces de descifrar su contenido
7	No motivación de empleados	No existe un compromiso mutuo en la relación empresa-empleado.	No motivación del personal que lo incentive a sentirse identificado con las Sociedad Proveedora.	Filtración de información, infracciones deliberadas con el fin de perjudicar a la Sociedad Proveedora.
8	No contar con un programa de actualización constante del software	La no actualización continua de los sistemas informáticos y los controles asumiendo que estos han demostrado ser efectivos en su última revisión	El creciente avance de la tecnología que vuelve obsoletos sistemas que hasta hace poco era tecnología de punta.	Un incremento de ilícitos por personas más capacitadas que las mismas fortalezas del sistema.
9	Riesgos Transfronterizos	La posible transgresión de regulaciones en servicios prestados más allá de las fronteras de un país.	Desconocer de ciertas regulaciones legales del otro país	Demandas o conflictos que pueden traducirse en gastos legales que puedan comprometer a la Sociedad Proveedora.
10	Falta de políticas de confidencialidad	Ausencia de políticas que contribuyan a proteger los derechos de autor o de uso de los sistemas informáticos para la firma de contratos.	Desconocimiento de leyes que protegen los derechos y obligaciones relacionados con activos informáticos	Violación de términos en contratos que pueden conllevar a poner en desventaja a la Sociedad Proveedora ante sus competidores o pérdidas económicas sustanciales.

11	Dependencia de un proveedor informático externo	Cuando el sistema lo provee una fuente externa a la Sociedad Proveedora y existe una excesiva dependencia operativa de esta.	La excesiva confianza que se deposita en el desarrollador de un sistema informático, por tanto, los ataques y fallos que ocurrieren, deben ser resueltos exclusivamente por el desarrollador.	Atrasos en las reparaciones si el desarrollador tiene contratos firmados con otras empresas.
	AREA LEGAL			
12	Incumplimiento de leyes, normas y reglamentos.	No estar en constante actualización en cuanto a leyes y normativa vigente.	Por desconocimiento o por accidente.	Imposición de multas y/o sanciones a la Sociedad Proveedora.
13	Incumplimiento de derechos y obligaciones con terceros	No brindar un servicio completo tanto a usuarios como a comercios afiliados.	Demandas por litigios por incumplimientos a terceros.	Daños a la imagen y pérdida de credibilidad. Imposici ón de indemnizaciones a los sujetos afectados.
AREA REPUTACIONAL				
14	Daños a la imagen	Personas malintencionadas pueden hacer ‘smurfing’ con las ganancias provenientes de la actividad criminal en múltiples cuentas	Los criminales pueden realizar múltiples transacciones para confundir el rastro del dinero y el verdadero origen de los fondos.	Los fondos que han sido objeto de ‘smurfing’ desde múltiples cuentas pueden ser retirados al mismo tiempo
15	No cumplir con las expectativas de los clientes	Opinión negativa del servicio prestado por la Sociedad Proveedora ate los clientes como el impedimento de acceso a sus fondos sobre todo si no existieran medios alternativos para hacerlo	Por una mala gestión y la prestación de un servicio con deficiencias	Alejamiento de clientes, disminución en ventas y utilidades en decrecimiento.
16	No existencia de controles específicos para identificar cobro de Extorsión	Cobro de la comúnmente denominada “Renta” en dinero electrónico	Falta de controles destinados a prevenir operaciones ilícitas específicas. Como causa externa, el índice de criminalidad que impera en el país.	Deterioro de la imagen de la Sociedad Proveedora restándole valor corporativo.

AREA INFORMÁTICA

17	Accesos no autorizados a almacenes de información	La ausencia de controles puede ocasionar que dineros electrónicos pueden ser rápidamente depositados y transferidos ilegalmente a otra cuenta	Las transacciones ocurren en tiempo real, dejando poco tiempo para pararlas si existe sospecha de financiamiento del terrorismo o lavado	El dinero criminal puede ser movido a través del sistema rápidamente y ser retirado de otra cuenta
18	Ataques al sistema	La probabilidad que Hackers ingresen al sistema.	Fallos en la seguridad del sistema. Y robo de información	Daños y/o modificaciones en la estructura del mismo que perjudiquen a la Sociedad.
19	Inadecuada infraestructura del sistema	No cumplir con las expectativas del usuario al momento de consultar su saldo disponible u operar con sus fondos.	Actualizaciones poco frecuentes o no fundamentadas en estudios de necesidades de los usuarios	No contar con una adecuada infraestructura se debilita la seguridad del sistema. Descontentos y/o retiro de usuarios.

Según el Artículo 5 de las Normas para la Gestión de Integral de Riesgos de las Entidades Financieras (NPB4-47) define la identificación como "(…) la etapa en la que se reconocen y se entienden los riesgos existentes en cada operación, producto, procesos y líneas de negocios que desarrolla la entidad (…)". (pg.2)

Medición de Riesgos

Los criterios adoptados para medir los riesgos son dos variables (probabilidad de ocurrencia y probabilidad de impacto) dada la naturaleza de los mismos, dichas variables se muestran representadas gráficamente en la Figura 3.

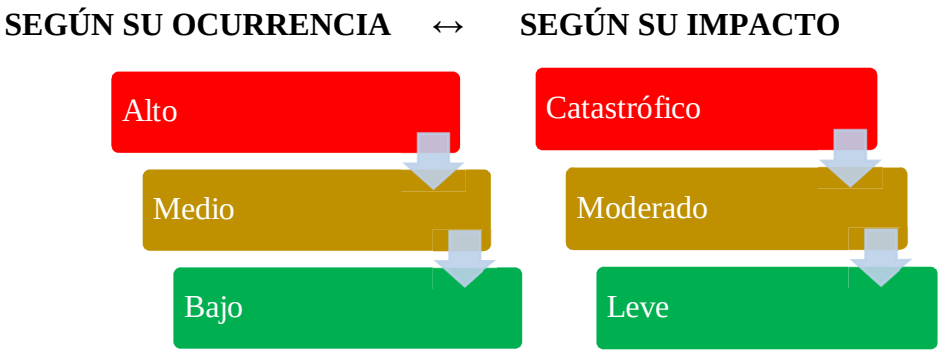
Según la probabilidad de ocurrencia:

- ***Alto:*** cuando el evento ocurre una vez en tres meses.

- ***Medio:*** *cuando el evento ocurre una vez en seis meses.*
- ***Bajo:*** cuando el evento ocurre una vez con una periodicidad mayor a seis meses.

Según la probabilidad de impacto:

- ***Catastrófico:*** cuando afectan los objetivos, proyectos y procesos, generando un retraso en el cumplimiento de los mismos; existe la posibilidad de demandas en contra por faltas en la prestación del servicio e indemnizaciones que llamen la atención de los medios de comunicación generen una imagen negativa de la entidad.
- ***Moderado:*** cuando afectan los objetivos, proceso y proyectos secundarios; amerita una investigación por parte de los encargados del control interno para mitigarlos.
- ***Leve:*** cuando el grado de afectación es mínimo en la consecución de los objetivos, proyectos y procesos, las quejas recibidas por faltas las prestaciones del servicio son de fácil solución; las autoridades de control hacen recomendaciones y pueden generarse algunos comentarios no favorables por algunos medios de comunicación.



Fuente: *Equipo de trabajo.*

Figura 8: Representación gráfica de la probabilidad de ocurrencia e impacto, según la magnitud del riesgo y el alcance de este.

Valoración de los riesgos

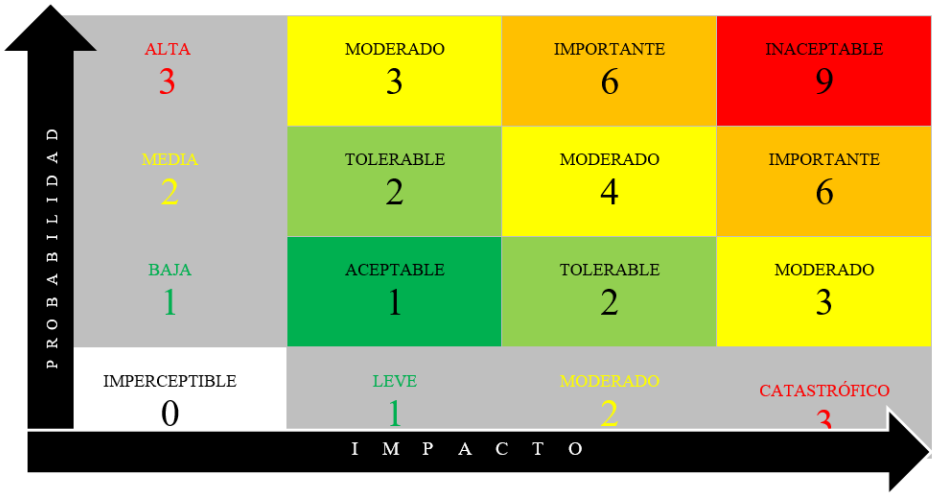
Los riesgos son valorados de acuerdo a la siguiente calificación:

Tabla 2. Valoración de riesgo

NIVEL DE RIESGO INHERENTE	CALIFICACIÓN
INACEPTABLE	**9**
IMPORTANTE	**6**
MODERADO	**3 - 4**
TOLERABLE	**2**
ACEPTABLE	**1**
IMPERCEPTIBLE	**0**

Matriz de riesgos

La entidad mide los riesgos basados en la matriz que se muestra en la Figura 10.



Fuente: *Elaboración por el grupo de trabajo.*

Figura 9: Matriz de riesgos de la SPDE. En función de la figura 8 y la TABLA 2 esta matriz permite medir y valorar el rango en que se encuentra cada uno de los riesgos identificados.

Controles aplicados

Para disminuir la probabilidad de ocurrencia o impacto, se aplicaron los siguientes tipos de controles, evaluándolos en la escala del 1 al 4:

- ***Preventivos:*** (4) Aplicados antes o al iniciar un proceso con el objeto de evitar que eventos adversos ocurran o si ocurren, disminuir su impacto.
- ***Correctivos:*** (3) Los aplicados durante los procesos y están destinados a mitigar eventos que se han generado ya a causa de las actividades realizadas.
- ***Detectivos:*** (2) Los aplicados una vez hayan finalizados los procesos y se hayan generado los eventos adversos.

- ***Inexistentes:*** (1) cuando no existen controles definidos para tratar eventos, sea por su naturaleza o porque no se había presentado antes.

Periodicidad de los controles

La periodicidad en la aplicación de controles fue fundamental en la valoración de riesgos para la entidad, es por ello que el producto resultante de multiplicar la valoración de la aplicación por la periodicidad, se mide si el control es eficaz y se clasifican como:

- **Permanentes*:*** (3) Son los controles que se aplican a todo el proceso o en cada actividad.
- ***Periódicos:*** (2) Son los que se aplican por un lapso de tiempo determinado o transcurrido un número determinado de actividades.
- ***Ocasionales:*** (1) Son los aplicados solo de manera eventual en uno o procesos aislados.

Criterio utilizado para medir la eficacia de los controles

Tabla 3. Medición de la eficacia de los controles aplicados en cada área de la organización.

APLICACIÓN DEL CONTROL	MEDIDA	PERIODICIDAD DE APLICACIÓN	MEDIDA	RESULTADO (PRODUCTO)	EFICACIA
PREVENTIVO	**4**	**PERMANENTE**	**3**	**12**	**ALTA**
PREVENTIVO	**4**	**PERIÓDICO**	**2**	**8**	**MEDIA**
PREVENTIVO	**4**	**OCACIONAL**	**1**	**4**	**BAJA**
CORRECTIVO	**3**	**PERMANENTE**	**3**	**9**	**ALTA**
CORRECTIVO	**3**	**PERIÓDICO**	**2**	**6**	**MEDIA**
CORRECTIVO	**3**	**OCACIONAL**	**1**	**3**	**BAJA**
DETECTIVO	**2**	**PERMANENTE**	**3**	**6**	**MEDIA**
DETECTIVO	**2**	**PERIÓDICO**	**2**	**4**	**BAJA**
DETECTIVO	**2**	**OCACIONAL**	**1**	**2**	**BAJA**
INEXISTENTE	**1**	**-**			**INEXISTENTE**

Las calificaciones comprenden del uno al cuatro, tomándose el producto de la aplicación por el control como el resultado, de esta forma se calcula la eficacia de los mismos.

Cálculo del riesgo residual

Para monitorear el nivel resultante a los que se ha reducido un riesgo después de haber aplicado controles se calcula mediante una formula con la cual se divide el nivel del riesgo entre el nivel de eficacia del control asociado a cada riesgo.

$$\textbf{Riesgo residual} = \frac{\textbf{Nivel de Riesgo Inherente}}{\textbf{Control (eficacia)}}$$

El resultado se mide de acuerdo a la escala representada en la Tabla 4.

Tabla 4. Escala para medir el riesgo residual.

NIVEL DE RIESGO RESIDUAL	CALIFICACIÓN
INACEPTABLE	5 <
IMPORTANTE	4 <= 5
MODERADO	3 <= 4
TOLERABLE	2 <= 3
ACEPTABLE	1 < =2
IMPERCEPTIBLE	>= 1

Las calificaciones en esta ocasión comprenden del uno al cinco, seccionándolos de acuerdo al nivel de riesgo al que está asociado.

MON-E, S.A. DE C.V

Calificación de los riesgos detectados en las distintas áreas de la sociedad.

Tabla 5. Criterios basados en "Normas Técnicas para la Gestión de los riesgos de Lavado de Dinero y de Activos, y de Financiamiento al Terrorismo" (NRP-08) para calificar riesgos.

Área	No	Riesgo	Probabilidad de ocurrencia	Probabilidad de Impacto	Calificación (Valoración)	Nivel asignado
Operativa	1	**No existencia controles para verificar el registro de usuarios**	2	3	6	Importante
	2	**Suplantación de identidad (Phishing)**	1	3	3	Moderado
	3	**Operaciones en zonas de alto nivel de criminalidad**	3	3	9	Inaceptable
	4	**Exceder los montos establecidos legalmente**	2	2	4	Moderado

	5	**Actividades fraudulentas de empleados**	1	3	3	Moderado
	6	**Permitir que trabajos informáticos se lleven a cabo fuera la empresa**	1	3	3	Moderado
	7	**No motivación de empleados**	2	2	4	Moderado
	8	**No contar con un programa de actualización constante del software**	2	3	6	Importante
	9	**Riesgos Transfronterizos**	2	1	2	Tolerable
	10	**Falta de políticas de confidencialidad**	1	3	3	Moderado
	11	**Dependencia de un proveedor informático externo**	2	3	6	Importante
Legal	12	**Incumplimiento de leyes, normas y reglamentos.**	1	3	3	Moderado
	13	**Incumplimiento de derechos y obligaciones con terceros**	2	3	6	Importante
Reputacional	14	Daños a la imagen	1	2	2	Tolerable
	15		2	2	4	Moderado

		No cumplir con las expectativas de los clientes				
	16	Cobro de Extorsión	2	3	6	Inaceptable
Seguridad	17	Accesos no autorizados a almacenes de información	1	3	3	Moderado
	18	Ataques al sistema	1	3	3	Moderado
	19	Inadecuada infraestructura del sistema	1	3	3	Moderado

Mapa de riesgos

La entidad mide los riesgos basados en la siguiente matriz:

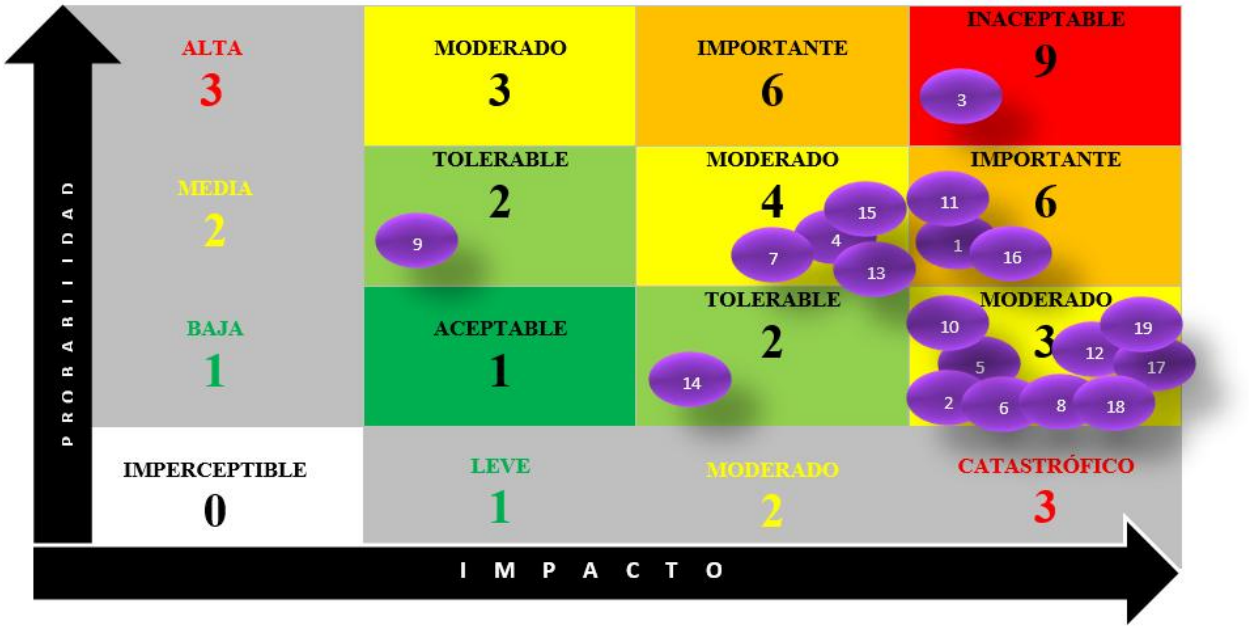


Figura 10. El mapa de riesgo es el que permite ver de manera global la valoración de riesgos, dividiéndolos cada uno pos su calificación dada.

4.7.4 Control y Mitigación de Riesgos.

Según el literal c) del artículo 5 de la NPB4-47 establece que esta fase "(…) busca asegurar que las políticas, límites y procedimientos establecidos para el tratamiento y mitigación de los riesgos son apropiadamente tomados y ejecutados".

Monitoreo y comunicación:

Es dar seguimiento a los controles sistemáticos aplicados para disminuir el impacto que podrían ocasionar los riesgos en caso de darse el evento. El sistema de monitoreo es importante que brinde la información suficiente para apoyar en la toma de decisiones.

4.7.5 Sistema de monitoreo de alerta.

Según el artículo 20 del Instructivo de la Unidad de Investigación Financiera para la Prevención de Lavado de Dinero establece que las alertas para la detección de transacciones sospechosas "(…) son mecanismos de control que las instituciones incluyen en sus sistemas de monitoreo, a fin de detectar comportamientos inusuales o que las mismas presentan patrones inconsistentes con la actividad propia del cliente".

Las alertas pueden ser de dos tipos:

Alertas Planas: Son las que por sí solas no constituyen un riesgo pero que en conjunto o repetición pueden contribuir a detectar riesgos potenciales de LD/FT; generalmente son parametrizaciones automatizadas de los sistemas de información como medidas de control.

Alertas con base en Riesgos parametrizados: Son indicios o síntomas de ciertas operaciones que podrían ayudar a detectar operaciones ilícitas de LD/FT.

Estos factores de riesgos están presentes generalmente en las operaciones que la SPDE realiza con clientes y/o productos, y en los distintos puntos geográficos en las que opera.

Respecto al oficial de cumplimiento

Según el Artículo 14 de la Ley Contra el Lavado de Dinero y de Activos establece que "(…) los sujetos obligados deben establecer una oficialía de cumplimiento a cargo de un oficial nombrado por la Junta Directivo u Órgano competente".

El oficial de cumplimiento debe ostentar un cargo gerencial y su objetivo es de planificar, implementar, coordinar y vigilar las políticas y procedimientos internos; capacitar y fomentar una cultura de prevención y mitigar el riesgo relacionados al lavado de dinero y de activos.

Las funciones del Oficial de Cumplimiento

a) Cumplir con el marco legal y normativo en materia de LD/FT e instrucciones generadas por la UIF y SSF.

b) Elaborar políticas, programas relacionados al Lavado de Dinero y financiamiento del terrorismo, las cuales deberán ser aprobadas por la Junta Directiva.

c) Elaborar una matriz de riesgos de lavado de dinero en la cual se evalúen e identifiquen los riesgos a que se está expuesta la entidad considerando los factores de riesgo en el negocio.

d) Analizar aquellos casos que puedan considerarse como operaciones sospechosas.

e) Realizar monitoreos permanentes a través de sistemas informáticos de las transacciones realizadas por los clientes o usuarios, para detectar existencia de casos considerados como inusuales o sospechosos que deban informarse a la UIF.

f) Elaborar el plan anual de capacitación en conjunto con la unidad administrativa, el que debe ser debidamente autorizado por Junta Directiva.

g) Capacitar al personal por lo menos una vez al año.

h) Establecer y modificar las disposiciones internas de la institución, para prevenir y detectar actos y operaciones sospechosas de lavado de dinero.

i) Vigilar el cabal y oportuno cumplimiento dentro de la Institución de las disposiciones emitidas en materia de cumplimiento, así como la normativa interna.

j) Reportar a las autoridades competentes operaciones sospechosas, así como las operaciones reguladas en efectivo que superen los USD$10,000.00 y transacciones por cualquier otro medio que superen los USD$25,000.00 en un mismo día o acumuladas en el mes.

k) Evaluar 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.

l) Recibir información y alertas de colaboradores, mediante reportes de operaciones que pudieran ser sospechosas, para evaluación y análisis.

m) Elaborar y mantener expedientes electrónicos o físicos de los clientes.

n) Requerir a las áreas pertinentes la actualización del expediente de clientes cuyas operaciones resultan inconsistentes con el perfil declarado.

o) Preparar informes para la Junta Directiva y la Unidad de Investigación Financiera UIF.

p) Elaborar el plan de trabajo y someterlo a aprobación de Junta Directiva.

q) Dar respuesta a las solicitudes de información requeridas por la UIF y cualquier otro ente legal.

r) Establecer un comité de prevención de lavado de dinero y activos, el cual deberá ser aprobado por Junta Directiva.

s) Elaborar controles para Personas Expuestas Políticamente

t) Preparar y presentar al Comité de Cumplimiento la gestión realizada en la Oficialía de Cumplimiento; y

u) Fungir como secretario del Comité de Prevención de Lavado de Dinero y elaborar las actas respectivas

De acuerdo al artículo 26 en las "Normas Técnicas para la Gestión de los riesgos de Lavado de Dinero y de Activos, y de Financiamiento al Terrorismo" (NRP-08) establece que "(…) 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".

Factor	No	Riesgo	Probabilidad de ocurrencia	Probabilidad de Impacto	Calificación (Valoración)	Nivel asignado
Riesgo cliente	1	**Clientes que la entidad determine que son Personas Expuestas Políticamente (PEP's)**	3	3	9	Inaceptable
	2	**Listas emitidas por organismos internacionales señalando personas sobre las cuales existen sospechas de actividad criminal**	3	3	9	Inaceptable

Riesgo de servicios	1	**Transferencias frecuentes a diferentes personas sin ningún tipo de relación familiar.**	1	3	3	Moderado
	2	**Transferencias superiores a USD$300.00**	2	3	6	Importante
	3	**Transferencias con un acumulativo mensual de USD$1,200.00**	2	3	6	Importante
Riesgo geográfico	1	**Movimientos frecuentes de fondos entre personas de varias ubicaciones geográficas**	1	3	3	Moderado
	2	**Operaciones en zonas de alto nivel de criminalidad**	3	3	9	Inaceptable

Plan de mitigación de riesgos de los procesos en Sociedades Proveedoras de Dinero Electrónico (SPDE)

Introducción

El Plan de Mitigación de Riesgos de la SPDE MON-E, S.A. es el resultado de un conjunto de esfuerzos estratégicos conforme al estudio de los riesgos identificados y medidos, encaminados a reducirlos a un coeficiente de probabilidad mínimo de ocurrencia.

Este plan es una evidencia clara de la mejora continua de la SPDE en sus procesos como gestión institucional.

Objetivo del Plan

Disminuir la probabilidad de ocurrencia de los riesgos que podrían ocasionar un impacto negativo dentro de la SPDE y pudiese dañar los procesos, ralentizarlos e incurrir en pérdidas económicas generalizadas.

Tabla 6. Plan de mitigación de riesgos

Riesgo	Causa	Estrategias y acciones de mitigación	Recursos que supone su aplicación	Responsables del cumplimiento del control	Responsable de monitorear el cumplimiento del control
· Incumplimiento de control de registro de usuarios	Los nombres sospechosos no pueden ser capturados por sistema, haciendo de esta una zona segura para criminales y terroristas conocidos	Aplicar la debida diligencia que propone la Ley Contra el Lavado de Dinero y de Activos	Tiempo y dinero para capacitar a los pontos de venta autorizados para registrar clientes	Los puntos de venta autorizados por la SPDE de afiliar usuarios.	Auditoría Interna en Colaboración con el comité de Riesgos y el Oficial de Cumplimiento de la Ley contra el Lavado de Activo de Dinero y de Activo
· Suplantación de identidad (Phishing)	Falta de controles para autenticar los documentos al momento de dar de alta a un usuario.	Implementar controles robustos que disminuyan la posibilidad de ser burlados por clientes malintencionados	Tiempo y dinero para capacitar a los pontos de venta autorizados para registrar clientes	Los puntos de venta autorizados por la SPDE de afiliar usuarios.	Auditoría Interna en Colaboración con el comité de Riesgos y el Oficial de Cumplimiento de la Ley contra el Lavado de Activo de Dinero y de Activo
· Frecuencia de operaciones en zonas de alto nivel de criminalidad	No contar con un sistema capaz de rastrear la ubicación geográfica de cada transacción	Controlar y tomar en consideración la ubicación de donde se está realizando Operaciones inusuales.	Económicos y humanos para implementar tecnología basada en triangulación de señal mediante antenas.	Departamento de Informática.	Auditoría Interna y el Comité de riesgos,
· Exceder los montos	Deficiencia de controles,	Diseñar controles que tomen en	Recursos humanos,	Departamento de informática	Auditoría Interna y el

	establecidos legalmente	ausencia o no aplicación de los mismos, confiando a que el sistema esta parametrizado.	cuenta errores que el sistema pueda cometer.	tecnológicos y financieros		Comité de riesgos,
·	Actividades fraudulentas de empleados	Descontentos que pueden llevar a un empleado a tomar represalias y actuar por sí mismo o colusionar con otro u otros en perjuicio de la Sociedad Proveedora.	Monitoreo constante de la actividad de los empleados en cada área y en tiempo real mediante la instalación de cámaras de seguridad en áreas clave.	Recursos económicos	Departamento de Recursos Humanos	Auditoría Interna
·	Fuga accidental de información	Olvido de documentos, portafolios, dispositivos USB o cualquier otro artículo que pueda contener datos importantes que podrían comprometer o debilitar su funcionamiento.	Evitar que programadores y demás empleados involucrados en manipular el sistema extraigan de la entidad cualquier material para trabajar fuera de esta.	Logística de revisión de salida del personal	Departamento de Recursos Humanos	Auditoría Interna
·	Descontentos de empleados	No motivación del personal que lo incentive a sentirse identificado con las Sociedad Proveedora.	Elaboración de un plan integral de convivencia y plan de motivación para incentivar a empleados	Recurso humano y para capacitaciones y talleres motivacionales	Departamento de Recursos Humanos	Auditoría Interna
·	Desfase del sistema	El creciente avance de la tecnología que vuelve obsoletos sistemas que hasta hace poco era tecnología de punta.	Elaborar un plan de mantenimiento y actualizaciones del sistema	Recursos económicos	Departamento de Informática, departamento de Investigación y desarrollo	Auditoría Interna
·	Riesgos Transfronterizos	Desconocer de ciertas regulaciones legales del otro país donde podría llegar la cobertura	Capacitaciones para conocer las leyes vigentes del país donde hay cobertura de la red o instalar bloqueadores de señal si se trata solamente de cobertura no deseada.	Recursos Económicos y tecnológicos.	Departamento de Informática	Auditoría Interna

· Falta de políticas de confidencialidad	Desconocimiento de leyes que protegen los derechos y obligaciones relacionados con activos informáticos	Capacitar al personal o contratar especialistas en Leyes	Recursos Humanos y Económicos	Departamento de Recursos Humano, Departamento Legal.	Auditoría Interna
· Dependencia de un proveedor informático externo	La excesiva confianza que se deposita en el desarrollador de un sistema informático, por tanto, los ataques y fallos que ocurrieren, deben ser resueltos exclusivamente por el desarrollador.	Un plan de contingencia que mitigue el riesgo de pérdidas económicas por un mal funcionamiento durante un tiempo prolongado del sistema,	Capacitación del personal interno de la empresa para afrontar contingencias	Dirección General	Auditoría
· Incumplimiento de leyes, normas y reglamentos.	Por desconocimiento o por accidente.	Capacitación de personal o contratación de personal capacitado en Leyes.	Recursos Humanos y Económicos	Área Legal	Auditoría Interna
· Incumplimiento de derechos y obligaciones con terceros	Demandas por litigios por incumplimientos a terceros.	Capacitación de personal o contratación de personal capacitado en Leyes.	Recursos Humanos y Económicos	Área Legal	Auditoría Interna
· Daños a la imagen	Los criminales pueden realizar Múltiples transacciones para confundir el rastro del dinero y el verdadero origen de los fondos.	Crear mecanismos de control que identifiquen las Operaciones Sospechosas	Recursos Humanos	Comité de Riesgos	Auditoría Interna
· No cumplir con las expectativas de los clientes	Por una mala gestión y la prestación de un servicio con deficiencias	Hacer evaluaciones y estudios sobre cómo perciben los clientes el servicio brindado	Recursos Económicos para los estudios	Departamento de Mercadeo	Auditoría Interna
· Cobro de Extorsión	Como causa externa, el índice de criminalidad que impera en el país. Internamente, la ausencia o debilidad de controles que	Estudias a detalle los comportamientos inusuales en transacciones realizadas por clientes y relacionarlas con el perfil del	Capacitaciones de personal y Recursos Económicos	Gerencia General	Auditoría Interna.

	mitiguen este riesgo.	formulario “Conozca a su cliente”			
· Accesos no autorizados a almacenes de información	Las transacciones ocurren en tiempo real, dejando poco tiempo para pararlas si existe sospecha de financiamiento del terrorismo o lavado	Documentar las operaciones sospechosas y clasificarlas según su importancia, para ser analizadas en bancos de datos con acceso restringido solo a personal autorizado.	Recursos económicos y tecnológicos	Departamento de Informática	Auditoría interna.
· Ataques al sistema	Fallos en la seguridad del sistema.	Planes de contingencia que mitiguen el impacto de posibles fallos de acuerdo a su naturaleza	Recursos económicos y tecnológicos	Departamento de Informática	Auditoría interna.
· Inadecuada infraestructura del sistema	Actualizaciones poco frecuentes o no fundamentadas en estudios de necesidades de los usuarios	Estudio de estabilidad y cumplimiento de las necesidades que demandan los usuarios.	Recursos económicos	Investigación y desarrollo	Gerencia de Investigación y desarrollo

Política de riesgos

Según la NPB-4-50 “Normas para la Gestión del Riesgo Operacional de las Entidades Financieras” los riesgos operacionales deben tratarse con especial cuidado, ya que son los que más comúnmente se encuentran presentes en una entidad, como en otras, en la SPDE. Esta norma define el Riesgo operacional como “La posibilidad de incurrir en pérdidas por fallas en los procesos, de las personas, de los sistemas de información y a causa de acontecimientos externos (…)”.

Sistema de organización

La entidad está estructurada de manera que permita la gestión integral de riesgos, con funciones debidamente segregadas, según lo que establece la Norma Prudencial de Bancos 4-47 en relación a la Gestión Integral de Riesgos.

Funciones de la Junta Directiva

La junta directiva de la responsable de velar por la adecuada gestión integral, según como establece el artículo siete, tener conocimiento y comprender todos los riesgos inherentes a los cargos que ejecuta, aprobar una estructura organizacional, crear el Comité de Riesgo y nombrar a sus miembros, aprobar las estrategias y políticas, límites de exposición para los riesgos, aprobar la propuesta del comité de Riesgos en cuanto la mitigación de los mismos, aprobar la incursión de la sociedad en nuevos productos, operaciones y actividades así como asegura que la Auditoría Interno verifique la existencia y cumplimiento de los esquemas de gestión y control aplicados en la sociedad.

Funciones del comité de riesgo

El comité de riesgo mencionado en NRP-08 está compuesto según lo explican también las Normas de Gobierno Corporativo para las Entidades Financieras (NPB 4-48) y ejecutar la función de establecidas en el artículo ocho de las Normas para la Gestión Integral de Riesgos de las Entidades Financieras (NPB4-47), entre otras las siguientes:

a) Informar a la junta directiva sobre los riesgos asumidos por la entidad, su evolución, sus efectos internos en los recursos patrimoniales y la metodología para su mitigación.
b) Velar por que la entidad cuente con una adecuada estructura organizacional, estrategias, políticas y recursos para la gestión integral de riesgos.
c) Asegurar a informar a la junta directiva la correcta ejecución de las estrategias y políticas aprobadas.
d) Proponer a la junta directiva los límites de tolerancia la exposición para cada tipo de riesgo
e) Aprobar la metodología de gestión de cada uno de los riesgos
f) Requerir y dar seguimiento los planes correctivos para normalizar incumplimientos a los límites de exposición o deficiencias reportadas.

Función desde la alta gerencia

Las funciones de la alta gerencia están especificadas como sigue:

a) Establecer las condiciones necesarias a nivel de toda la organización para proporcionar un ambiente adecuado que procure desarrollo del proceso de gestión integral de Riesgo.

b) Conformar la Unidad de riesgos, designar a sus responsables y asegurar su carácter de independencia, así como dotarle recurso humano, material y capacitación técnica adecuada.

c) Asegurar el incumplimiento de planes de contingencia para los riesgos que enfrenta la entidad como

d) Entre otras asignaciones que la Junta Directiva crea conveniente.

Función desde la unidad de riesgo

La junta directiva es la encargada de asignar a los miembros de la unidad de riesgo, encargados de evaluar supervisar y monitorear riesgos específicos dentro de la organización, te acuerdas experiencia, conocimiento o pericia respecto de riesgos que afecten tanto financiera como operativamente activo, pasivos no fuera del balance de la SPDE.

Entre otros, las siguientes son funciones y responsabilidades de la unidad de riesgo:

a) Identificar, retiro y controlar los riesgos en que incurre la entidad dentro de sus diversas unidades de negocio y sus efectos en su solvencia.

b) Señalar y proponer las propuestas de solución, políticas y procedimientos, así como sus manuales respectivos a cada uno nos Riesgos identificados.

c) Proponer para su aprobación los métodos, modelos y parámetros para medir los distintos tipos de riesgos que afecte a la entidad.

d) Informar al comité de riesgos sobre los principales riesgos asumidos por la entidad.

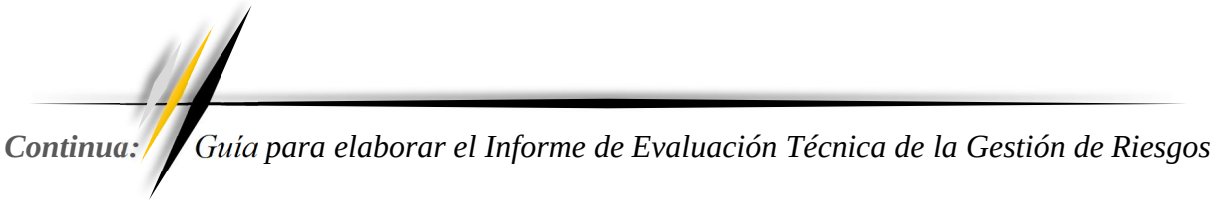
e) Opinar sobre los posibles riesgos que conlleve la introducción de nuevos productos, operaciones y actividades.

f) Dar seguimiento al cumplimiento de los límites de exposición a los riesgos, su nivel de tolerancia por el tipo de riesgo cuantificable

g) Elaboraron y propone comité de riesgos planes de contingencia y pruebas de atención para gestionar cada uno de los riesgos.

Informe de Evaluación Técnica de la Gestión de Riesgos de la Sociedad al 31 de diciembre de 2017.

La SPDE, como otras entidades financieras, está en la obligación de presentar a la superintendencia sistema financiero, los primeros ciento veinte días cada año un informe de evaluación de la gestión integral de riesgos, previa autorización de la junta directiva y que deberá contener como mínimo lo siguiente:



- La estructura organizativa para la gestión integral de riesgos
- Detalle de los principales riesgos asumidos por la sanidad de la entidad
- Las Políticas actualizadas por la gestión integral de riesgos
- Descripción de la metodología, sistemas y herramientas utilizadas para cada uno de los riesgos
- Los resultados de las evaluaciones realizadas (Hallazgos)
- Proyectos asociados a la gestión de riesgos a desarrollar en un ejercicio siguiente al reportado.

Divulgación sobre la gestión integral de riesgo

NPB4-47 también establece en su artículo dieciocho que "Las entidades deberán divulgar banderas resumida en un apartado de su sitio web, dentro de los primeros noventa días cada año, la información relativa a las políticas, metodología y demás medidas relevantes para la gestión cada tipo de riesgo.

Información adicional

La Superintendencia del Sistema Financiero podrá requerir en cualquier momento cualquier documento necesario para la adecuada gestión de riesgo, ya sea de manera física o electrónica a la que se refiera, así como la información de las auditorías o revisiones, por lo que es necesario mantener o de la documentación orden.

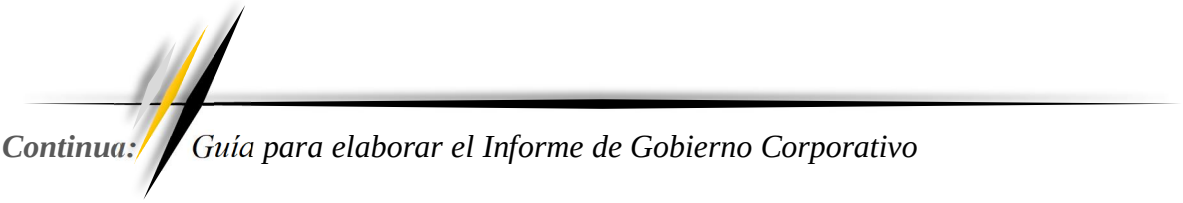
Gestión Integral de riesgos y el papel del Gobierno Cooperativo

En cumplimiento a la Norma Prudencial de Bancos (NPB4-48)

De acuerdo a esta norma, en su artículo primero establece las bases mínimas que deben adoptar las entidades para fortalecer sus prácticas de gobierno corporativo dentro del proceso de gestión de riesgos financieros, operacionales y otros, conforme a estándares internacionales en la materia y acordes con la naturaleza y escala de sus actividades.

"El gobierno corporativo es el sistema por el cual las sociedades son administradas y controladas; su estructura deberá establecer las atribuciones y obligaciones de los que participan en su administración, supervisión y control, tales como los accionistas, la Junta Directiva, miembros de la Alta Gerencia, Comités y Unidades de control; asimismo, debe proporcionar un marco adecuado de transparencia de la organización y la protección de los intereses de los depositantes, asegurados y demás usuarios de las entidades".

Y aunque explícitamente no menciona a las Sociedades Proveedoras de Dinero Electrónico, La Superintendencia del Sistema Financiero obliga a estas a aplicarla, basándose en la similitud del giro en el que desarrollan las actividades.



Informe de gobierno corporativo

De acuerdo a los estándares internacionales establecidos por el Comité de Basilea, las "Normas Técnicas para la Gestión de Riesgo de Lavado de Dinero y de Activos y Financiamiento al Terrorismo" (NRP-08), las "Normas para la gestión Integral de Riesgos de las entidades financieras" (NPB4-47) y "Normas de Gobierno Corporativo" (NPB4-48), emitidas por la Superintendencia del Sistema Financiero, MON-E, S.A. ha implementado la gestión integral de riesgos, siendo la Junta Directiva el ente responsable de velar por una adecuada gestión integral de riesgos.

Información general

1. Conglomerado Financiero local al que pertenece.	N/A
2. Entidades miembros del Conglomerado Financiero local y principal negocio.	N/A
3. Grupo Financiero Internacional al que pertenece.	N/A

Accionistas

1. Número de Juntas Ordinarias celebradas durante el período y quórum.	1 sola reunión 1000%= 500 acciones
2. Número de Juntas Extraordinarias celebradas durante el período y quórum.	1 sola reunión 1000%= 500 acciones

Junta directiva

1. Miembros de la Junta Directiva y cambios en el período informado.

- Presidente y Representante Legal: *Nombre del Presidente y Representante Legal*
- vice-presidente: *nombre del vice-presidente*
- secretario: *nombre del secretario*
- Director Propietario: *Nombre del Director Propietario*
- Director Propietario: *Nombre del Director Propietario*
- Director Propietario externo: *nombre del Director Propietario externo*
- Director Suplente: *Nombre del Director Suplente*
- Director Suplente: *Nombre del Director Suplente*
- Director Suplente: *Nombre del Director Suplente*

2. Cantidad de sesiones celebradas durante el período informado.

Durante el periodo informado se celebró únicamente una sesión.

3. Descripción de la política sobre la permanencia o rotación de miembros.

3.1. Elección y conformación de la Junta Directiva

La Junta Directiva será integrada con los cargos y por el número de directores que determine la Junta General de Accionistas, pero en todo caso habrá un presidente y un secretario y un mínimo de tres y un máximo de seis miembros Propietarios. Habrá tres Directores Suplentes.

3.1.1. Período de Funciones.

El período de funciones de los miembros de la Junta Directiva será de tres años, prorrogables hasta que la Junta General Ordinaria de Accionistas elija a sus sustitutos dentro de los tres meses siguientes una vez finalizada su gestión, y por ello no se incurrirá en falta alguna frente a terceros.

3.2. Modo de proveer las vacantes que ocurran en la Junta Directiva.

Cualquiera de los administradores Propietarios que faltaren temporal o permanentemente, se convocará a la Junta General para designar a quien nombrarán y a quien sustituirán. En todo caso, para ello debe respetarse el mínimo de quorum de un veinticinco por ciento del capital social.

Alta gerencia

1. **Miembros de la Alta Gerencia y los cambios durante el período informado.**

La Alta Gerencia para el periodo informado está constituida de la siguiente manera:

· Presidente y Representante Legal: *Nombre del presidente y Representante Legal*

· Gerente General: *Nombre del Gerente General*

· Gerente Administrativo Financiero: *Nombre del Gerente Administrativo Financiero*

· Gerente de Operaciones: *Nombre del Gerente de Operaciones*

Importante: *Cuando se mencione al Gerente general o Director Ejecutivo se estará refiriendo a la Alta Gerencia de MON-E, S.A.*

Durante el periodo que se informa, lo hubo cambios entre los miembros de la gerencia de uno.

Comité de Auditoría

· Miembros del comité de auditoría y cambios durante el periodo informado.

· Numero de sesiones realizadas durante el periodo.

· Detalle de las principales funciones desarrolladas.

· Temas corporativos conocidos durante el periodo.

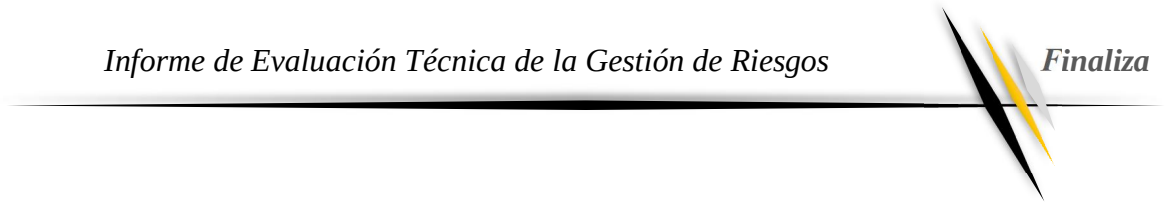
Comité de riesgos

- Miembros del comité de auditoría y cambios durante el periodo informado.
- Numero de sesiones realizadas durante el periodo.
- Detalle de las principales funciones desarrolladas.
- Temas corporativos conocidos durante el periodo.

Otros

Descripción de los cambios en el Código de Gobierno Corporativo durante el periodo.

- Descripción de los cambios en el Código de Ética durante el periodo.



CONCLUSIONES

1. Las Sociedades Proveedoras de Dinero Electrónico, por su giro, son sociedades con riesgos complejos o poco comunes, que pueden afectar los recursos físicos y/o virtuales de las mismas, siendo estos últimos los de mayor importancia, ya que, por tratarse de un servicio prestado, en gran parte, con tecnología informática reciente, es más difícil profundizar en soluciones concretas. La tecnología inicial con la que comenzó a funcionar el dinero electrónico ha tenido cambios importantes, la seguridad informática cada día se perfecciona, pero de igual manera lo hacen los delitos informáticos, cada parche de seguridad en un sistema puede ser naturalmente vulnerado por un hacker, un virus o aplicativos maliciosos.

2. La intervención de un ente regulador como la Superintendencia del Sistema Financiero en El Salvador ha sido de vital importancia en la gestión de riesgos de las Sociedades Proveedoras de Dinero Electrónico, haciéndolas más responsables en la aplicabilidad de sus controles internos encaminados a garantizar el buen servicio a los usuarios ya la prevención de delitos, pero existen otras áreas que no cubre la supervisión de estos entes reguladores y es tarea de cada SPDE velar por la aplicabilidad de controles en contra de aquellos factores que atenten con su patrimonio.

3. La aprobación de la Ley para facilitar la Inclusión Financiera en El Salvador sentó un precedente importante para la aceptación del Dinero Electrónico como medio legal de pago, aunque aún quedan aspectos de la misma que pudieran generar confusión en cuanto a su aplicabilidad debido a que tres años después de haber entrado en vigencia y a la fecha de esta investigación, no cuenta aún con su respectivo Reglamento.

RECOMENDACIONES

1. Priorizar en las áreas con mayor probabilidad de riesgos como los recursos informáticos que son la base fundamental para prestar su servicio, invirtiendo en ellos con el fin de mantenerlos actualizados y en óptimas condiciones; con procesos más simplificados para el usuario, pero sin perder la seguridad.

2. A las futuras SPDE que se constituyan, tomar en cuenta que la supervisión de la Superintendencia del Sistema Financiero no es nada más que un apoyo en su Gestión de Riesgos y no el gestor de Riesgos en sí, cuyo objetivo es preservar la estabilidad del Sistema Financiero y velar por la eficiencia y la transparencia del mismo.

3. Las SPDE deben tomar en cuenta que la no existencia de un Reglamento que complemente la Ley de Inclusión Financiera estaría provocando dificultades en la correcta aplicación de la Ley y menos probabilidad de amparo en casos judiciales, por lo que es necesario la exigencia del mismo.

BIBLIOGRAFIA

Federación Latinoamericana de Bancos (FELABAN). (2016). II Reporte de Inclusión Financiera. Recuperado de: http://www.felaban.net/publicaciones.php

CONAPES. Informativa. Boletín Informativo (2013). Recuperado de: https://conapes.wordpress.com/informativas/

Dudley, S. y Lohmuller, M. Triángulo del Norte, epicentro mundial de la extorsión" (Julio de 2015). InSight Crime. Recuperado de: https://es.insightcrime.org/noticias/noticias-del-dia/

La extorsión: negocio millonario (Boletín No. 258, agosto 2016). Instituto de Estudios Estratégicos y Políticas Públicas (IEEPP). Recuperado de: https://www.ieepp.org/boletines/mirador-de-seguridad/2016/

Asamblea Legislativa de la República de El Salvador. Ley para Facilitar la Inclusión Financiera. (2015). Decreto No. 72

Catota, Cortez y Escobar (2017). Modelo de Gestión del Riesgo como herramienta en la prevención de Lavado de Dinero y Activos para las Sociedades Proveedoras de Dinero Electrónico en El Salvador. Universidad de El Salvador.

OneLife IMA Oficial. (2016). Historia del Dinero. OneLife Webinars. Recuperado de: https://www.youtube.com/watch?v=UxHTbT4Xk4k

Barrios, V. (2004). Boletín Informativo. Información Comercial Española (ICE). ¿Por qué existen los Bancos? Págs. 34

Inclusión Financiera. (noviembre de 2016). Banco Mundial. Recuperado de: http://www.bancomundial.org/es/topic/financialinclusion/overview

Vega, M. (2013) Moneda/Innovaciones (BCR Perú). Dinero Electrónico: Innovación de pagos al por menor, para promover la inclusión. Pág. 16. Recuperado de: www.bcrp.gob.pe/docs/Publicaciones/Revista-Moneda/moneda.../moneda-153-04.pdf

Grupo de Acción financiera – GAFI. (2014). Informe Monedas Virtuales. Definiciones claves y Riesgos Potenciales de LA/FT. Recuperado de: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwiZ4YqXie_aAhXBxVkKHTDyASgQFggvMAE&url=http%3A%2F%2Fwww.uaf.cl%2Fasuntos%2Fdescargar.aspx%3Farid%3D961&usg=AOvVaw0Zi0V_d9qI-aKGogWxsHEk

European Banking Authority. (2013). Aviso a los consumidores sobre las monedas Virtuales. Recuperado de: http://www.eba.europa.eu/documents/10180/598420/EBA_2013_01030000_ES_TRA1_Vinay.pdf

García, H. (18 de mayo de 2007). Dinero real desapareciendo en Japón. Recuperado de: http://www.kirainet.com/

Velez, L. (2014). La desmaterialización del dinero. Recuperado de: http://luisguillermovelezalvarez.blogspot.com/2014/10/la-desmaterializacion-del-dinero.html

Asamblea Legislativa de la República de El Salvador. Ley para Facilitar la Inclusión Financiera. (2015). Decreto No. 72

Banco Central de Reserva de El Salvador (2017). Circular. Ajuste de los Límites Máximos establecidos en La Ley Para la Inclusión Financiera para Registros de Dinero electrónico y Depósitos en Cuenta de Ahorro con requisitos Simplificados. Recuoperado de: http://www.bcr.gob.sv/bcrsite/uploaded/content/category/786473149.pdf

Shigla, A. & Villavicencio, K. Ventajas y desventajas del uso de Dinero Electrónico en la ciudad de Guayaquil", (2017). Repositorio Institucional de la Universidad de Guayaquil, Perú. Recuperado de: http://repositorio.ug.edu.ec/handle/redug/20069

Real Academia Española. Diccionario de la Lengua Española. Edición de Tricentenario (Act. 2017). Recuperado de: http://dle.rae.es/

"Origen e historia de las maras (parte 2)" (diciembre 2015). El País. Recuperado de: http://elpais.com.sv/origen-e-historia-de-las-maras-parte-2/

Nueva modalidad de extorsión en las cárceles. (07 de marzo de 2012). La Página. Recuperado de: http://www.lapagina.com.sv/nacionales/63528/2012/03/08/

Brinda balance anual de la actividad policial (enero 2018). Policía Nacional Civil. Recuperado de:http://www.pnc.gob.sv/portal/page/portal/informativo/novedades/noticias

Saravia. Extorsión. Portal de Transparencia. Recuperado de: http://transparencia.pnc.gob.sv/?p=1060

Ponce. C. Informe SOLUCIONES (Junio de 2016). "Extorsiones a la Micro y Pequeña empresa de El Salvador". Fundación Salvadoreña para el Desarrollo Económico y Social (FUSADES). Recuperado de: http://fusades.org/sites/default/files/extorsiones%20a%20micro%20y%20peque%C3%B1a%20empresa%20de%20El%20Salvador.pdf

Grupo de Acción Financiera de Sudamérica– GAFISUD. (2012). “Guía sobre los nuevos métodos de pago: tarjetas prepagas, pagos por telefonía móvil y pagos por internet” (Junio de 2013).

Grupo de Acción Financiera– GAFI. (2013). “Guía del GAFI sobre Medidas Antilavado de Activos y contra el Financiamiento al Terrorismo e Inclusión Financiera”.

ANEXOS

Anexo 1

Mobile Cash fue autorizado como proveedor de dinero electrónico

La Superintendencia del Sistema Financiero (SSF) autorizó oficialmente las operaciones de la Sociedad Proveedora de Dinero Electrónico Mobile Cash, comercialmente conocida como Tigo Money El Salvador, convirtiéndose en la primera sociedad proveedora de dinero electrónico que en el país.

La autorización oficial de inicio de operaciones de dicha entidad será a partir del 1 de agosto de 2018 fecha a la cual además deberá efectuar el traslado de los fondos a la cuenta de depósito aperturada en Banco Central de Reserva para respaldar el cien por ciento del dinero electrónico en circulación, conforme lo establece el artículo 10 de la Ley para Facilitar la Inclusión Financiera.

El Superintendente del Sistema Financiero, Ing. José Ricardo Perdomo, aseguró felicito a Tigo Money por ser la primera sociedad proveedora de dinero electrónico en ser autorizada y fortalecer con ello la inclusión financiera en el país.

La autorización, que incorpora a la Sociedad Proveedora de Dinero Electrónico Mobile Cash dentro de las instituciones registradas, permitirá a la Superintendencia efectuar la supervisión de sus operaciones electrónicas.

San Salvador, 2 de julio de 2018

Banco Central de Reserva de El Salvador

OFICINA DEL VICEPRESIDENTE

CIRCULAR

9 de marzo de 2017

ASUNTO: Ajuste de los límites máximos establecidos en la Ley para la Inclusión Financiera para Registros de Dinero Electrónico y Depósitos en Cuentas de Ahorro con Requisitos Simplificados, de acuerdo al reciente aumento del salario mínimo.

Señores
Presidentes y/o Representantes Legales de los Integrantes del Sistema Financiero
Presidente de la Asociación Bancaria Salvadoreña
Presidente de la Asociación Salvadoreña de Empresas de Seguros
Presidente de la Asociación Salvadoreña de Administradoras de Fondos de Pensiones
Presidente de la Asociación Salvadoreña de Bancos Cooperativos y Sociedades de Ahorro y Crédito (ASIFBAN)
Presidente de la Asociación Salvadoreña de Intermediarios Bursátiles
Superintendente del Sistema Financiero
Presente

Estimados Señores:

Les comunico que el Comité de Normas del Banco Central de Reserva de El Salvador, en Sesión No. CN-02/2017, celebrada el 8 de marzo de 2017, acordó aprobar el ajuste de los límites máximos establecidos en la Ley para Facilitar la Inclusión Financiera para Registros de Dinero Electrónico y Depósitos en Cuentas de Ahorro con Requisitos Simplificados, con base al reciente aumento del salario mínimo de la manera siguiente:

Monto Máximo por transacción	Monto Máximo de transacciones acumuladas en el mes	Saldo Máximo acreditado
$300.00	$1,200.00	$1,200.00

Los límites establecidos por el Comité de Normas entrarán en vigencia a partir de la fecha de su comunicación.

En aplicación del inciso segundo del Artículo 100 de la Ley de Supervisión y Regulación del Sistema Financiero, la modificación arriba relacionada se hace de su conocimiento mediante su publicación en el sitio de internet del Banco Central de Reserva de El Salvador, www.bcr.gob.sv, en la Sección Normativa/Normativa Financiera.

Atentamente,

Marta Evelyn de Rivera
Secretario Comité de Normas

Banco Central de Reserva de El Salvador ★ COMITE DE NORMAS

Anexo 3

Secretaría del Consejo Directivo

Superintendencia del Sistema Financiero

Certificación No. 100/2018

La Infrascrita Directora Secretaria del Consejo Directivo de la Superintendencia del Sistema Financiero, **CERTIFICA:** Que en el punto **VI)** del acta de la sesión No. CD-23/2018 celebrada el 21 de junio de 2018, aparece asentado el acuerdo, que en los romanos I, II y III literalmente dice: "I) Autorizar el inicio de operaciones de la Sociedad Proveedora de Dinero Electrónico Mobile Cash, Sociedad Anónima, a partir del día 1 de agosto de 2018; II) Autorizar los asientos registrales de la Sociedad Proveedora de Dinero Electrónico Mobile Cash, Sociedad Anónima, en los registros relativos a: 1) De los miembros de Junta Directiva y Director Ejecutivo, siguientes: Director Presidente: Esteban Cristian Iriarte, Director Vicepresidente: Xavier Charles Rocoplan, Director Secretario: Harold Lynn Rogers, Director Vocal: José Enrique Sorto Campbell, Directores Suplentes: Marcelo Julio Alemán Zapata, Mauricio Alfonso Marenco Rodríguez y Álvaro José Mayora Re; y del Director Ejecutivo: Daniel Wilfredo Barrientos Sorto; y 2) De accionistas de la sociedad correspondientes a: Millicom International One, S.L. y Millicom Spain, S.L.; III) Instruir a la Sociedad Proveedora de Dinero Electrónico Mobile Cash, Sociedad Anónima, que de conformidad al artículo 10 de la Ley para Facilitar la Inclusión Financiera, efectúe el traslado de los fondos a la cuenta de depósito aperturada en Banco Central de Reserva, que respaldarán el cien por ciento del dinero electrónico en circulación previo al inicio de operaciones".

Es conforme con su original con el cual fue confrontado, y para los efectos legales consiguientes, extiendo, firmo y sello la presente Certificación en San Salvador, a los veinticinco días del mes de junio de dos mil dieciocho.

SUPERINTENDENCIA DEL SISTEMA FINANCIERO CONSEJO DIRECTIVO SECRETARIA

Ana Virginia de Guadalupe Samayoa Barón

Secretaria del Consejo Directivo

Anexo 4

CONTROL DE RECLAMOS DE OPERACIONES Y SERVICIOS DE LOS CLIENTES O DE LOS PARTICIPANTES

Nombre del Proveedor:
Fecha de referencia:

No. de Correlativo	Tipo de Reclamo	Fecha de Presentación	Nombre del Cliente	No. Referencia del Reclamo	Breve descripción del Reclamo	Monto Reclamado	Lugar donde sucedió el evento	Fecha de Resolución	Tipo de Resolución		Oficina que atendió el reclamo	Nombre del Empleado Responsable	Teléfono Directo y Dirección electrónica
									Positiva	Negativa			

Instrucciones

No. de Correlativo	Número de reclamos en este reporte.
Tipo de Reclamo	Clasificación propia del Proveedor según operación.
Fecha de presentación	Fecha en la que el cliente presentó el reclamo al Proveedor
Nombre del Cliente	Nombre del titular del registro sujeto al reclamo.
No. Referencia del Reclamo	Número de control y seguimiento asignado por el Proveedor.
Breve descripción del Reclamo	Descripción de la inconformidad del cliente que motiva el reclamo.
Monto Reclamado	El valor en USD$ que implicaría reconocer al Proveedor a favor del cliente.
Lugar donde sucedió el evento	Nombre del lugar de participante y ubicación.
Fecha de Resolución	Fecha en la que el Proveedor dio respuesta al cliente.
Tipo de Resolución	Positiva: Cuando se haya reconocido a favor del cliente; Negativa: Cuando se haya resuelto que el reclamo es infundado y por consiguiente en contra de los intereses del cliente.
Oficina que atendió el reclamo	Nombre de la unidad del Proveedor responsable de atender el reclamo.
Nombre del Empleado Responsable	Nombre del funcionario de más alto nivel dentro del Proveedor que se responsabiliza por la respuesta dada al cliente del reclamo presentado.
No. Telefónico y dirección electrónica	Número telefónico y correo electrónico directo en que se puede conectar a la persona que atendió el reclamo.

Anexo 5

MODELO DE DECLARACIÓN JURADA PARA DIRECTORES, GERENTES Y ACCIONISTAS DE LAS SOCIEDADES QUE REALICEN ACTIVIDADES SIMILARES A LA PROVEEDURIA DE DINERO ELECTRÓNICO INTERESADAS EN ADECUARSE

En la ciudad de San Salvador, a las _____horas del día _____de _____de dos mil ____. Ante mí, _____notario del domicilio de _____comparece el señor_____de _____años, (profesión u oficio) _____, del domicilio_____a quien conozco (o no conozco), portador de (o identifico por) Documento Único de Identidad número (o pasaporte número)_____, con Número de Identificación Tributaria _____quien actúa en nombre propio (o en representación de, en este caso consignar si es representante legal o apoderado y relacionar la personería según el caso, en este momento o al final) y ME DICE: Que en su calidad de futuro director o administrador de la sociedad _____, BAJO JURAMENTO HACE LAS SIGUIENTES DECLARACIONES: A) Que no soy menor de veinticinco años de edad (excepto si es accionista); B) Que no soy deudor del fisco y del sistema financiero salvadoreño clasificado en cualquiera de las categorías de mayor riesgo crediticio; C) Que no he sido condenado mediante sentencia ejecutoriada en el país o en el extranjero, por haber cometido o participado dolosamente en la comisión de cualquier delito; D) Que no me encuentro en estado de quiebra o suspensión de pagos, y que no he sido calificado judicialmente como responsable de una quiebra culposa o dolosa; E) Que no se me ha comprobado judicialmente mi participación en actividades relacionadas con el narcotráfico y delitos conexos, y con el lavado de dinero y activos y de financiamiento al terrorismo, en el país o en el extranjero; F) Que no he sido declarado inhábil en el país ni en el extranjero, para esta clase de cargo ni he sido sancionado administrativa o judicialmente por mi participación en infracciones a las leyes y normas de carácter financiero, en especial la captación de fondos del público sin autorización y en los delitos de carácter financiero. El suscrito notario hace constar: Que expliqué al compareciente sobre lo establecido en el Código Penal, en cuanto al delito de falsedad ideológica, regulado en el artículo doscientos ochenta y cuatro de dicho cuerpo legal. Así se expresó el compareciente a quien le expliqué los efectos legales de la presente acta notarial, que consta de _____ hoja (s) frente y vuelto; y leído que le fue por mí lo escrito, en un solo acto sin interrupción e íntegramente, ratifica su contenido y firmamos. DOY FE.

La declaración Jurada debe de cumplir con lo establecido en la Ley de Notariado.