# MANUAL DE PREVENCIÓN DE DELITOS

# LAVADO DE ACTIVOS Y FINANCIAMIENTO DEL TERRORISMO LEY 19.913

# VITA SOLUTIONS SPA


**NOVIEMBRE 2024**

# ÍNDICE

# I. INTRODUCCIÓN

El Manual de Prevención de Delitos de Lavado de Activos y Financiamiento del Terrorismo de la Ley N° 19.913[1] que se presenta a continuación, se compone de medidas de prevención y detección creadas en forma estructurada y orientadas a la prevención del Lavado de Activos y otros delitos base establecidos en la Ley N° 19.913, dándole vida a la norma dentro de la política interna del desarrollo de la actividad de Vita Solutions SpA[2], lo que permite mayor transparencia y probidad ante sus clientes y usuarios, así como también maiyor control de la gestión realizada por el equipo de trabajo, colaboradores y terceros; todo esto con el objeto de erigir este documento como un marco general de la norma sobre Lavado de Activos, de otras normas legales en la materia, y la abundante reglamentación administrativa existente, tanto para los sujetos obligados en general, como aquellas establecidas especialmente para el funcionamiento de empresas de transferencia de dinero, como lo es Vita.

Lo anterior, con intención de dar cumplimiento a lo establecido en la Ley N° 19.913 que crea la Unidad de Análisis Financiero[3] y modifica diversas disposiciones en materia de Lavado y Blanqueo de Activos, y las normas administrativas de la UAF establecidas en las Circulares N° 49 del 2012; N° 52, 53, 54 y 55 del año 2015; N° 59 y 60 de 2019; las Recomendaciones PEP de julio del 2013; los oficios ordinarios N° 428 del 2016 y N° 1745 de 2019; el oficio N° 603 de 2021 y la recopilación actualizada de normas UAF del año 2024; complementando con las normas pertinentes que al efecto se establecieron en la Ley N° 20.393 que establece la Responsabilidad Penal de las Personas Jurídicas -y su actualización del año 2023- y determina una serie de delitos de la más alta relevancia para la operación de Vita. Así, todas estas normas -y las demás aplicables- permiten incorporar controles efectivos de prevención y detección de delitos, y establecer parámetros de protección al equipo de trabajo, clientes, usuarios, colaboradores y terceros que se relacionen con la Empresa, estableciendo de forma clara y ordenada las políticas, límites, sanciones y procedimientos de acción en cada caso.

Finalmente, la existencia de este instrumento nos permite estar en línea con el arduo y fructífero trabajo que ha venido implementando Chile en la concreción de los objetivos de prevención del Lavado de Activos, con toda la institucionalidad asociada, que entre otras cosas le permite a Vita colaborar en su calidad de sujetos obligados de la norma, pudiendo aportar en conjunto al trabajo que realiza la UAF, siendo actores en la detección de operaciones sospechosas que se adviertan en la

[1] En adelante, indistintamente, ‘’el Manual’’, ‘’el Manual de Prevención de Delitos’’ o ‘’MDPDD’’
[2] En adelante, indistintamente, ‘’Vita’’ o ‘’la Empresa’’.
[3] En adelante, Indistintamente, ‘’la UAF’’.

prestación de los servicios de Vita. El fruto de este trabajo sin duda será el parte a la política nacional contra el lavado de activos, la elevación del valor reputacional de la empresa, y la mejor y mayor implementación de una cultura ética y legal del cumplimiento normativo.

# II. ANTECEDENTES GENERALES

## 1. OBJETIVO GENERAL

El objetivo de este instrumento es establecer políticas y procedimientos de prevención, detección y disuasión de comportamientos, indicios o actos vinculados a los delitos de Lavado de Activos y Financiamiento del Terrorismo (“LA/FT”), según lo establecido en la Ley N° 19.913, que permitan a los colaboradores de Vita informarse y canalizar estos comportamientos, implementando y adoptando medidas oportunas que ayuden a disminuir la comisión de estos delitos.

Además, en este documento se dará noticia de las bases jurídicas fundamentales asociadas al tratamiento de la materia de prevención de lavado de activos, el conocimiento de los delitos y sus sanciones, y cómo afectan consecuencialmente a la actividad del giro y la empresa, informando de las señales de alerta, canales de denuncia y procedimientos a realizar al efecto.

## 2. ALCANCE DEL MANUAL DE PREVENCIÓN DE DELITOS Y FINANCIAMIENTO DEL TERRORISMO EN EL DESARROLLO DE LA ACTIVIDAD DE VITA SOLUTIONS SPA

El presente Manual es aplicable a todo el equipo de trabajo y usuarios de la Empresa, propietarios, fundadores, directores, gerentes, ejecutivos, representantes, administradores, accionistas, colaboradores, clientes, así como cualquier tercero que pudiera estar en relación con Vita, dentro y fuera de Chile, independiente de su modalidad de contratación y calidad dentro de la organización.

Con este alcance, se procura dar cumplimiento a todos los aspectos normativos y políticas establecidas por la Unidad de Análisis Financiero, mediante la gestión de los procesos de negocios y los reportes que se realizan ante la UAF.

# 3. ORGANIZACIÓN INTEGRAL DEL MANUAL DE PREVENCIÓN DE DELITOS Y FINANCIAMIENTO DEL TERRORISMO EN EL DESARROLLO DE LA ACTIVIDAD DE VITA SOLUTIONS SPA

Este Manual forma parte de un flujo que se origina desde la ley hacia el establecimiento de acciones estratégicas relacionadas al resguardo, transparencia y probidad del servicio. Así, este Manual, el cual es una iniciativa estratégica para el funcionamiento del servicio, se enmarca dentro de un proceso de mejora continua, que descansa en los siguientes pilares:

- Procesos de identificación y evaluación de riesgos de LA/FT. Se identifican las áreas y procesos con mayor susceptibilidad a la ocurrencia de hechos o actos sospechosos de LA/FT, es decir, se analiza la documentación requerida tanto para los empleados de Vita, como de los usuarios del servicio y terceros relacionados; esto ayuda a despejar incongruencias en el origen de los fondos de los usuarios y conductas irregulares que pudieren provenir de actos ilícitos.
- Definición de los roles y responsabilidades dentro del Manual. La Ley establece que deberá designarse un funcionario responsable, el Oficial de Cumplimiento, quien se encargará de observar que efectivamente se cumplan las políticas y procedimientos establecidos.
- Definición de políticas y procedimiento relacionados con la detección de operaciones sospechosas de lavado de activos y financiamiento del terrorismo. Esto en el caso de que algún colaborador de Vita llegare a tener conocimiento de algún hecho ilícito o violación de las políticas y procedimientos por parte de cualquier persona (natural o jurídica), en cuyo caso se establecen los procedimientos para notificar de inmediato al funcionario responsable, ya que en caso contrario dicha omisión o silencio se reputará o entenderá como actividad ilícita.
- Resguardo de la confidencialidad dentro del sistema institucional de prevención de LA/FT. Vita mantiene un férreo compromiso con cumplir con las exigencias establecidas por el regulador, particularmente con la relacionada al deber de confidencialidad y resguardo de la información de los procesos y de los usuarios, así como también con la de aportar todos los antecedentes que la UAF requiera, con la debida celeridad y diligencia, para poder realizar los procesos de Inteligencia Financiera correspondientes.
- Capacitación permanente a los colaboradores de Vita en materias de prevención de los delitos de Lavado de Activos y Financiamiento del Terrorismo. La Empresa cuenta con un programa de capacitaciones

semestrales para sus colaboradores, en virtud del cual se generan presentaciones con información relacionada a la Prevención de los Delitos de LA/FT, la relevancia de dichas materias en la actividad de Vita -señales de alerta, controles y protocolos internos- y la importancia de que todos manejen de forma adecuada y suficiente dicha información; adicionalmente a las presentaciones, el programa de capacitaciones contempla talleres y evaluaciones breves.

- Monitoreo, auditoría y evaluación continua del Manual.

## 3.1. Gestión de Riesgos.

La gestión de riesgos consiste en el cabal conocimiento de los procesos operativos de Vita, con la finalidad de identificar los riesgos a los que potencialmente la Empresa puede verse expuesta en el desarrollo de su actividad económica, y los efectos que éstos podrían generar, así como las medidas preventivas y de mitigación que permitan su control.

### 3.1.1. Establecimiento del Marco.

Corresponde a la definición de los pasos internos y externos que van orientados a gestionar el riesgo dentro del desarrollo de la actividad de la Empresa. Esta fase fue creada considerando los contextos estratégicos, organizacionales y de gestión, y es considerada una etapa en constante desarrollo y evaluación, ya que se actualiza conforme a las nuevas normas y al contexto asociado al desarrollo de la actividad de Vita.

### 3.1.2. Evaluación del Riesgo.

Se trata del análisis, identificación y valoración de los riesgos que pueden afectar a la Empresa en cuanto a las posibilidades de LA/FT, para lo cual se contempla una metodología interna para la creación del proceso de evaluación de riesgos, la cual consiste en:

3.1.2.1. Identificación del Riesgo. Es el proceso de búsqueda, reconocimiento y descripción de los riesgos existentes en materia de LA/FT que se podría presentar en cada uno de los procesos.

3.1.2.2. Análisis del Riesgo. Se trata de creación de las señales de alerta contra la materialización de LA/FT, lo cual permitirá tener bases más claras para la valoración del riesgo y así adoptar las decisiones relativas al tratamiento del riesgo asociado a estos delitos

3.1.2.3. Valoración del Riesgo. Focalizado en la comparación de los resultados obtenidos del análisis del riesgo con los criterios

existentes, a objeto de determinar si cada uno de los riesgos identificados y sus magnitudes son aceptables o tolerables.

La evaluación del riesgo práctica, desde la perspectiva del análisis del comportamiento e información de los usuarios de Vita Wallet, comprende controles periódicos de las fichas tanto de ellos como de sus destinatarios, y así identificar los riesgos inherentes a las distintas actividades y categorías de los usuarios y destinatarios que utilizan la plataforma de la empresa. Para ello, se realizan controles de chequeo de la identificación del usuario, análisis de las operaciones que realiza el usuario, observación del manejo del flujo de dinero que opera el usuario, y seguimiento del beneficiario destinatario de la operación.

### 3.1.3. Organización Interna de Roles y Responsabilidades.

Toda organización requiere de un funcionario responsable para el reporte de operaciones sospechosas y la coordinación y supervigilancia de políticas y procedimientos para prevenir el lavado de activos y el financiamiento del terrorismo. Vita ha definido como funcionario responsable al Gerente de Cumplimiento y Legales, y como suplente en caso de su ausencia, al analista de Cumplimiento. Este funcionario responsable, a su vez, tiene responsabilidades y funciones específicas que serán detalladas más adelante.

# 4. GENERALIDADES DE LA LEY 19.913

El hito basal de Chile de un sistema Anti Lavado de Activos y Contra el Financiamiento del Terrorismo es el 18 de diciembre del año 2003, fecha en la que se publica la Ley N° 19.913, que creó la Unidad de Análisis Financiero y modificó diversas disposiciones en materia de lavado y blanqueo de activos.

Este sistema de prevención del LA/FT se materializa con la creación de la UAF y la determinación de una serie de obligaciones de carácter preventivo a diversas instituciones de los distintos sectores de la economía, establecidos en el art. 3° de la Ley N° 19.913.

La norma obliga a las personas naturales o jurídicas que indica, a proporcionar información relacionada con las operaciones sospechosas que se adviertan en el ejercicio de sus actividades, entendiendo por tales las que de acuerdo a los usos y costumbres de la actividad de que se trate, resulte inusual o carente de justificación económica o jurídica aparente, o que se relacionen con delitos terroristas, o con los listados de resoluciones del Consejo de Seguridad de las Naciones Unidas; mandata también la obligación de reportar operaciones en efectivo que superen el umbral de diez mil dólares o su equivalente en pesos chilenos; y la obligación de llevar y presentar determinados registros.

Dentro de los sujetos obligados del artículo tercero de la mentada ley, se hallan las empresas de transferencia de dinero; adicionalmente y con la entrada en vigencia de la Ley N° 21.251 (Fintec), encontramos a los prestadores de servicios de intermediación de instrumentos financieros, actual giro comercial de la Empresa.

## 4.1. Del Delito de Lavado de Activos y Financiamiento del Terrorismo.

El delito de Lavado de Activos se encuentra tipificado en los arts. 27 y 28 de la Ley N° 19.913, consagrando sus vertientes dolosa y culposa. En términos generales podemos entender el LA como aquel delito que busca legitimar la procedencia y naturaleza del dinero u otros bienes que fueron obtenidos ilegalmente, introduciendo estos activos en el circuito normal de la economía, dándoles apariencia de legalidad a través de actividades que son lícitas. Las penas establecidas para quien incurra en este tipo de delitos se enmarcan dentro del presidio mayor en sus grados mínimos a medio y multa de 200.000 UTM, así como también la pérdida temporal de derechos ciudadanos e inhabilitación, también temporal, para ejercer cargos públicos o en entidades privadas de relevancia nacional.

Por otro lado, el delito de Financiamiento del Terrorismo se encuentra tipificado en el artículo 8° de la Ley N° 18.314, que describe las conductas terroristas. Esta ley tiene un catálogo de delitos que incluye conductas que van desde el secuestro, encierro, detención o retención de rehenes y la sustracción de menores, hasta los atentados con bombas y otros artefactos que afecten la integridad física de las personas o les causen daño. Lo anterior, con el propósito de causar temor en la población, o para imponer exigencias a la autoridad. Ahora bien, el delito de FT consiste, básicamente, en prestar apoyo financiero a grupos o acciones de carácter terrorista. Finalmente,las sanciones establecidas en la ley sobre conductas terroristas contemplan la privación de libertad, multas y pérdida perpetua de derechos ciudadanos y de poder ejercer cargos públicos o en entidades privadas de relevancia nacional.

## 4.2. De los Delitos Base.

Se entiende por delitos base o precedentes del Lavado de Activos (LA) aquellos delitos que generan recursos en dinero o bienes, a través de un origen basado en actividades ilícitas y se procuran disimular u ocultar para ser insertados al circuito de la economía.

La ley determina un catálogo de estos delitos bases, entre los que se encuentran tráfico ilícito de estupefacientes y sustancias psicotrópicas; actos terroristas; control de armas; infracciones a la ley de mercado de malores; delitos establecidos en la ley general de bancos; delitos aduaneros; delitos contra la propiedad intelectual; delitos de la ley del banco central; algunos delitos tributarios; prevaricación; malversación de caudales públicos; fraude al Fisco; negociación incompatible; tráfico de influencias; exacciones ilegales; cohecho; secuestro y sustracción de menores; delitos de prostitución y pornografía infantil; trata de personas; algunas estafas y fraudes; asociación ilícita; responsabilidad de tarjetas de pago y transacciones electrónicas; delitos informáticos; delitos de revelación de información; delitos de robo; delitos asociados a procedimientos concursals y de reorganización; delitos contra la seguridad social, entre otros.

Según la Evaluación Nacional de Riesgos elaborada por la UAF en el año 2023, los delitos bases más frecuentes en Chile son la corrupción, estafas, narcotráfico, contrabando y la

asociación ilícita, seguidos del tráfico ilícito de migrantes, delitos tributarios, trata de personas, financiamiento del terrorismo, promoción de la prostitución y tráfico de armas. En relación con esta información, y la demás propia de la empresa, la Matriz de Riesgos de Vita identificó como delitos más probables -aunque con baja probabilidad- en el giro y actividad económica de la empresa los siguientes:

- Cohecho a funcionario público nacional o extranjero: Comete este delito quien ofrece o consiente en ofrecer o entregar a un empleado público un beneficio económico, en provecho de éste o de un tercero, para que realice acciones u omisiones con Infracción a los deberes de su cargo.

**Hipótesis en Vita:** caso en el cual algunos de los colaboradores, inversionistas o accionistas de Vita ofrece a un empleado público algún beneficio económico en provecho personal o de terceras personas para que realice acciones u omisiones con infracción a los deberes de su cargo.

**Medida de Control:** capacitaciones semestrales en materias relevantes asociadas a la prevención del lavado de activos y financiamiento del terrorismo; auditoría interna a los equipos de Vita, para revisar los procesos, protocolos y acciones tomadas dentro de cada equipo en el ejercicio de las actividades correspondientes.

**Áreas involucradas:** Gerencia, Cumplimiento, Operaciones, Desarrollo, Producto, Soporte, Marketing, Ventas, Recursos Humanos y Contabilidad y Finanzas; accionistas, inversionistas, y proveedores.

- Lavado de Activos: se identificó la posibilidad de que tanto colaboradores, accionistas e inversionistas, y usuarios de la plataforma de Vita incurran en estos actos y usen dicha plataforma como medio de movilización del dinero.

Las consecuencias potenciales de este delito en la empresa son múltiples, pudiendo afectar la moral, ética y buen funcionamiento de la misma, además de causar, eventualmente, el cierre de la empresa y sanciones a ésta y sus directivos por la responsabilidad penal de las personas jurídicas; también sanciones de prisión y multa para el sujeto directamente involucrado, según su responsabilidad penal. Adicionalmente, se verá afectado el valor reputacional de Vita y el giro de las transferencias de dinero, en tanto instrumento para distraer la ilicitud del origen de dineros o bienes.

Como mitigación se ha determinado la realización de procesos de verificación de clientes de forma automatizada utilizando softwares de screening y biométricos, además de una revisión estándar de las transacciones de usuarios respecto de señales de alertas automatizadas en la plataforma, las que nos permiten detectar si alguna operación realizada por los usuarios tiene el carácter de inusual y sospechosa, lo que eleva la correspondiente aplicación de protocolo de Debida DIligencia Reforzada, según sea el caso. Como controles adicionales, Vita Wallet mantiene operativo el Canal de Denuncias y un programa de capacitaciones para los colaboradores en materias de prevención de LA/FT.

**Hipótesis en Vita:** caso eventual en el que, en el ejercicio de las labores de los colaboradores con acceso a la información requerida para la realización de las transacciones de los usuarios, alguno de esos colaboradores incurra en actividades asociadas al LA/FT; caso en el cual alguno de los accionistas o inversionistas de Vita realice recargas en la plataforma con fondos que provengan de actividades ilícitas asociadas al LA/FT, utilizando la plataforma de Vita para entregarle a dichos fondos una apariencia de licitud y poder utilizarlos de forma normal.

**Medida de Control:** realización de procesos de verificación de clientes de forma automatizada utilizando softwares de screening y biométricos, además de una revisión estándar de las transacciones de usuarios respecto de señales de alertas automatizadas en la plataforma, las que nos permiten detectar si alguna operación realizada por los usuarios tiene el carácter de inusual o sospechosa, lo que eleva la correspondiente aplicación de protocolo de Debida DIligencia Reforzada, según sea el caso. Como controles adicionales, Vita Wallet mantiene operativo el Canal de Denuncias y un programa de capacitaciones para los colaboradores en materias de prevención de LA/FT; adicionalmente, auditoría interna a los equipos de Vita, para revisar los procesos, protocolos y acciones tomadas dentro de cada equipo en el ejercicio de las actividades correspondientes. También, se cuenta con un robusto sistema de KYC de forma tal de tener el mayor conocimiento posible de los usuarios de Vita y su comportamiento operacional, así como también con un sistema de levantamiento de información que permite realizar de forma eficiente y en tiempo los Reportes de Operaciones Sospechosas, toda vez que aquello sea necesario.

**Áreas involucradas**: Gerencia, Cumplimiento, Operaciones, Desarrollo, Producto, Soporte, Marketing, Ventas, Recursos Humanos y Contabilidad y Finanzas; accionistas e inversionistas; proveedores.

- Receptación: Comete este delito quien conociendo su origen o no pudiendo menos que conocerlo, tenga en su poder, transporte, compre, venda, transforme o comercialice especies que provengan de hurto, robo, receptación, apropiación indebida y/o hurto de animales. Asimismo, el delito de receptación sanciona las conductas negligentes de quienes adquieren o poseen dichos bienes.

**Hipótesis en Vita:** caso en que alguno de los colaboradores, accionistas o inversionistas de Vita ingrese a la plataforma fondos que provienen de actividades ilícitas asociadas a la receptación. Colaboradores utilizando dispositivos de trabajo que provengan de dicho delito.

**Medida de Control:** capacitaciones semestrales en materia de LA/FT y demás delitos relevantes en Vita, a fin de, por un lado, cumplir con lo establecido por el legislador y, por otro lado, crear conciencia en los colaboradores de Vita de las consecuencias asociadas a la comisión de estos delitos y su utilización dentro de la plataforma. Adicionalmente, se cuenta con un robusto sistema de revisión operacional, en virtud del cual se tienen controles y protocolos para evitar que los fondos que son utilizados en la plataforma, provengan de un origen ilícito. También, existe un protocolo respecto de la utilización de dispositivos de colaboradores en la empresa, y contratos asociados a su uso.

**Área involucrada:** Gerencia, Cumplimiento, Operaciones, Desarrollo, Producto, Soporte, Marketing, Ventas, Recursos Humanos y Contabilidad y Finanzas; accionistas e inversionistas.

- Financiamiento del Terrorismo: se identificó como una fuente probable de este delito que los usuarios de la plataforma la utilicen como medio de financiar al terrorismo por medio de transferencias internacionales en moneda FIAT y criptomonedas.

Las consecuencias de este delito son múltiples, puesto que afecta a la empresa a una escala ética y delictual, tanto para la Empresa como para sus integrantes. Medidas de mitigación y prevención para este tipo de delito son, principalmente, la revisión transaccional automatizada desde la plataforma con sus correspondientes señales de alerta, que son revisadas por los operadores de Cumplimiento y por el analista de Cumplimiento; adicionalmente, la Empresa cuenta con un programa de capacitaciones para los colaboradores en materias de prevención de LA/FT, de modo tal que todos los colaboradores estén enterados de la naturaleza de este delito, sus consecuencias y estén preparados para reconocer si hay indicio del mismo.

**Hipótesis en Vita:** Usuario o colaborador que solicita la realización de una o más transferencias internacionales hacia países catalogados como ‘’zonas de conflicto’’ (zonas controladas por grupos terroristas). Usuario o colaborador que solicita la realización de una o más transferencias en criptomonedas a un mismo destinatario sin razón aparente. Usuario o colaborador que solicita la realización de una o más transferencias internacionales hacia jurisdicciones con poca supervisión financiera.

**Medida de Control:** robusto sistema de KYC para conocer la mayor información posible de los clientes, cumpliendo con lo establecido por el legislador, en donde se genera una verificación documental, se utiliza tecnología que permite autenticar/verificar la identidad de los usuarios y protocolos para verificar la situación patrimonial de los mismos de manera efectiva; sistema de monitoreo transaccional en tiempo real con secciones automatizadas y otras manuales, cuando se requiere un análisis más exhaustivo.

**Áreas involucradas:** Gerencia, Cumplimiento, Operaciones, Desarrollo, Producto, Soporte, Marketing, Ventas, Recursos Humanos y Contabilidad y Finanzas; accionistas e inversionistas.

- Negociación incompatible: Comete este delito quien, a través de un poder de disposición o administración, interviene interesadamente en cualquier negociación, contrato, actuación, operación o gestión que involucre a un patrimonio (Artículo 240 del Código Penal).

**Hipótesis en Vita:** caso en que alguno de los gerentes de Vita, que tiene la facultad de intervenir en decisiones económicas o contractuales, realiza negocios o transacciones en su propio beneficio o en beneficio de terceros, aprovechándose de su posición**.**

**Medida de Control:** existencia de un ‘’Comité de Ética y Cumplimiento’’, a fin de supervisar algunas decisiones comerciales y que no existan intereses personales o alguna

incompatibilidad a la hora de que Vita suscriba contratos con otras entidades. Autonomía e independencia respecto de las áreas de Ventas, Contabilidad y Finanzas y Cumplimiento a la hora de tomar decisiones. Monitoreo transaccional que alcanza a los colaboradores más susceptibles de incurrir en actividades ilícitas asociadas a este delito. Utilización del Canal de Denuncias por parte de los colaboradores, toda vez que reconozcan actividades sospechosas. Auditoría interna a los equipos de Vita, para revisar los procesos, protocolos y acciones tomadas dentro de cada equipo en el ejercicio de las actividades correspondientes.

**Áreas involucradas:** Gerencia, Cumplimiento, Ventas; accionistas e inversionistas.

- Corrupción entre particulares: delito que se verifica en la hipótesis en que un empleado o mandatario solicite o acepte recibir un beneficio económico, o de otra naturaleza, para él o para un tercero, con la finalidad de favorecer o por haber favorecido en el ejercicio de sus labores la contratación de un oferente por sobre otro. También considera a aquel que da, ofrece o consiente en dar a un empleado o mandatario este beneficio económico.

En Vita Wallet podría eventualmente llevarse a cabo por parte de colaboradores que se vean involucrados en actos irregulares o inusuales con el fin de beneficiarse de forma indebida por medio de actos relacionados con terceros.

Las consecuencias negativas de la comisión de este delito para la Empresa son variadas: importa un riesgo reputacional, tanto los colaboradores como terceros relacionados perderán o verán mermada su confianza en la Empresa y sus trabajadores; adicionalmente, la comisión de este delito trae consecuencias punitivas para quien lo cometa y así sea determinado por el correspondiente tribunal; como consecuencia dentro de la Empresa, puede verificarse la terminación de la relación laboral con el colaborador que incurrió en dicha actividad delictual.

Mitiga esta eventual hipótesis la revisión psicológica de parte de la empresa con respecto a sus colaboradores, revisión de los sistemas de seguridad que tengan un nivel altamente auditable, implementación de medidas de seguridad dentro de la plataforma y fuera de ella, el código de ética, sanciones y capacitación constante del personal, así como también el *‘’name screening”* de los colaboradores previo a su contratación y durante la prestación de sus servicios.

**Área involucrada:** Gerencia, Cumplimiento, Operaciones, Desarrollo, Producto, Soporte, Marketing, Ventas, Recursos Humanos y Contabilidad y Finanzas; accionistas e inversionistas; proveedores.

- Apropiación indebida: se verifica este delito toda vez que un sujeto, en perjuicio de otra persona, se apropie o distraiga dinero, efectos o cualquiera otra cosa que hubiere recibido en depósito, comisión o administración, o por otro título que produzca la obligación de entregarla o devolverla

En este caso, podría darse la eventual situación de que la Empresa se puede ver inmersa en un conflicto legal por no verificar el origen de los fondos de los clientes, y estos

provengan de personas, clientes, usuarios o colaboradores que hayan cometido apropiación indebida, con las consecuencias legales respectivas para Vita Wallet. La mitigación fundamentalmente se basará en la revisión de los antecedentes de los clientes mediante los mecanismos que ya hemos expuesto anteriormente, y que se detallarán también más adelante.

**Área involucrada:** Gerencia, Cumplimiento, Operaciones, Desarrollo, Producto, Soporte, Marketing, Ventas, Recursos Humanos y Contabilidad y Finanzas; accionistas e inversionistas.

- Administración desleal: este delito se produce toda vez que un sujeto que tenga a su cargo la salvaguardia o la gestión del patrimonio de otra persona, o de alguna parte de éste, en virtud de la ley, de una orden de la autoridad o de un acto o contrato, le genera perjuicio, ya sea ejerciendo abusivamente algunas facultades, o ejecutando u omitiendo cualquier otra acción contraria al interés del titular de este patrimonio.

Al igual que el punto anterior, la fuente de este delito en relación a la empresa, puede producirse toda vez que nos encontremos en la eventual situación de que un sujeto que haya cometido tal hipótesis, use la plataforma de Vita para disimular los efectos del delito.

**Áreas involucradas:** Gerencia, Cumplimiento, Operaciones, Desarrollo, Producto, Soporte, Marketing, Ventas, Recursos Humanos y Contabilidad y Finanzas; accionistas e inversionistas.

- Obtención fraudulenta de complementos en relación del seguro de cesantía por la pandemia: Se sanciona a las personas que, por medios fraudulentos, simulación o engaño obtuvieren, en relación al acceso al seguro de cesantía, complementos y/o prestaciones o un beneficio mayor al que correspondiere.

**Hipótesis en Vita:** caso en que alguno de los colaboradores o accionistas/inversionistas de Vita por medios fraudulentos, simulación o engaño obtuvieren, en relación al acceso al seguro de cesantía, complementos y/o prestaciones o un beneficio mayor al que correspondiere. Caso en que alguno de los colaboradores manipule los registros de empleados reportando falsamente que han sido despedidos o que su jornada ha sido reducida debido a la crisis pandémica, cuando en realidad siguen trabajando de manera remota o presencial con normalidad. Esto les permite acceder a pagos del seguro de cesantía a través de la Administradora de Fondos de Cesantía (AFC), sin que la empresa ni los empleados lo necesiten legítimamente.

**Medida de Control:** programa de capacitaciones semestrales en materias de prevención de lavado de activos, financiamiento del terrorismo y demás delitos relevantes para Vita; programa de auditoría interna.

**Áreas involucradas:** Gerencia, Cumplimiento, Operaciones, Desarrollo, Producto, Soporte, Marketing, Ventas, Recursos Humanos y Contabilidad y Finanzas; accionistas e inversionistas.

- Obligar al trabajador a concurrir al lugar de trabajo y que este se encuentre en cuarentena o aislamiento sanitario: Se sanciona al empleador que, a sabiendas y teniendo autoridad para disponer del trabajo de un subordinado, le ordenen concurrir a su lugar de trabajo cuando éste sea distinto a su domicilio o residencia, y el trabajador se encuentre en cuarentena o aislamiento sanitario obligatorio decretado por la autoridad sanitaria.

**Hipótesis en Vita:** caso en que la Empresa a sabiendas y teniendo autoridad para disponer del trabajo de un subordinado, le ordenen concurrir a su lugar de trabajo cuando éste sea distinto a su domicilio o residencia, y el trabajador se encuentre en cuarentena o aislamiento sanitario obligatorio decretado por la autoridad sanitaria.

**Medida de Control:** programa de capacitaciones semestrales en materias de prevención de lavado de activos, financiamiento del terrorismo y demás delitos relevantes para Vita; programa de auditoría interna.

**Áreas involucradas:** Gerencia, Cumplimiento, Recurso Humanos.

- Trata de personas: Sanciona al que mediante violencia, intimidación, coacción, engaño, abuso de poder, aprovechamiento de una situación de vulnerabilidad o de dependencia de la víctima, o la concesión o recepción de pagos u otros beneficios para obtener el consentimiento de una persona que tenga autoridad sobre otra capte, traslade, acoja o reciba personas para que sean objeto de alguna forma de explotación sexual, incluyendo la pornografía, trabajos o servicios forzados, servidumbre o esclavitud o prácticas análogas a ésta, o extracción de órganos.

**Hipótesis en Vita:** Caso en que alguno de los colaboradores que tienen acceso a la plataforma de la Empresa podrían utilizar su posición para facilitar o permitir transacciones financieras vinculadas a la trata de personas. Caso en que un inversionista invierte en la Empresa utilizando dinero obtenido de la explotación sexual o laboral de víctimas de trata de personas. Caso en que algún colaborador utilice su acceso a la infraestructura de la empresa para procesar pagos a otros actores involucrados en la trata de personas, como traficantes, reclutadores o facilitadores.

**Medida de Control:** políticas y protocolos robustos de KYC. Monitoreo transaccional de los usuarios, incluyendo a los integrantes de las gerencias. Aplicación de protocolos de Debida Diligencia Reforzada. Evaluación de riesgo basada en países o regiones. Programa de capacitaciones semestrales a los colaboradores en materia de prevención de LA/FT y demás delitos relevantes para la operación de Vita, con indicación de cuáles son las señales para detectar ese tipo de delitos. Canal de Denuncias Anónimas.

**Áreas involucradas:**, Gerencia, Cumplimiento, Operaciones, Desarrollo, Producto, Soporte, Marketing, Ventas, Recursos Humanos y Contabilidad y Finanzas; inversionistas y/o accionistas.

- Delitos informáticos: Ley N° 21.459. El art. 1° define el "Ataque a la integridad de un sistema informático. El que obstaculice o impida el normal funcionamiento, total o

parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos". El art. 2° determina el "Acceso ilícito. El que, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático". El art. 3° reza "Interceptación ilícita. El que indebidamente intercepte, interrumpa o interfiera, por medios técnicos, la transmisión no pública de información en un sistema informático". El art. 4 detalla "Ataque a la integridad de los datos informáticos. El que indebidamente altere, dañe o suprima datos informáticos". En el art. 5° define "Falsificación informática. El que indebidamente introduzca, altere, dañe o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos". En el art. 6° se construye una hipótesis de receptación especial "Receptación de datos informáticos. El que conociendo su origen o no pudiendo menos que conocerlo comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, a cualquier título, datos informáticos, provenientes de la realización de las conductas descritas en los artículos 2°, 3° y 5°". También existe una hipótesis específica en el art. 7° de "Fraude informático. El que, causando perjuicio a otro, con la finalidad de obtener un beneficio económico para sí o para un tercero, manipule un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático". Finalmente, el art. 8° sanciona el abuso de dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, para la realización de los anteriores delitos.

**Hipótesis en Vita:** caso en el cual algún colaborador, inversionista o accionista genere uno o más accesos ilícitos a sistemas informáticos -como a la plataforma- para robar información de los usuarios y luego venderla o tratarla sin la debida autorización. Caso en que algún colaborador, inversionista o accionista realice manipulación de datos de los usuarios -que también pueden ser personas que forman parte de la empresa-, como la información de sus cuentas, de forma tal que se desvíen los fondos hacia cuentas que maneje el colaborador, inversionista o accionista en cuestión. Caso en que caso en el cual algún colaborador, inversionista o accionista realice sabotaje informático a la Empresa. También podrían darse casos de *phishing,* espionaje informático, *account takeovers,* que fueren realizados tanto por colaboradores, inversionistas o accionistas, actuando de forma personal o instruidos por alguien dentro de la organización de la Empresa.

**Medida de Control:** para evitar y/o mitigar la verificación de este tipo de delitos en el ecosistema de la Empresa, contamos con las capacitaciones periódicas para el personal en las que no solamente se enseñan y demuestran temáticas relacionadas con los delitos de

LA/FT sino que también de todos los delitos relevantes para la Empresa en el desarrollo de sus funciones. Adicionalmente, se cuenta con un sistema de doble factor de autenticación para los ingresos a la plataforma de los usuarios, así como también con un sistema de controles de acceso a la plataforma por parte de los colaboradores, que debe ser debidamente autorizado en razón de las labores realizadas por los colaboradores. Utilización de un gestor de contraseñas, *''NordPass",* para los colaboradores, que aporta seguridad en la realización de sus labores e impide compartir información sensible. Evaluaciones de vulnerabilidades dentro de la plataforma, protección contra malware y ransomware, programa de capacitación en ciberseguridad para los colaboradores. Existe un Comité de Seguridad de la Información y Ciberseguridad que semanalmente se reúne a revisar incidentes y riesgos en la materia, con un proceso de Certificación ISO 27.001 vigente.

**Áreas involucradas**: Desarrollo, Gerencia, Cumplimiento, Operaciones, Producto, Soporte, Marketing, Ventas, Recursos Humanos y Contabilidad y Finanzas; inversionistas y/o accionistas; proveedor.

- Delitos de Mercado de Valores: se sancionará a quien maliciosamente proporcione antecedentes falsos o certifique hechos falsos ante la Comisión para el Mercado Financiero; a los directores, administradores, gerentes y ejecutivos principales de un intermediario de valores que entregaren antecedentes o efectuaren declaraciones maliciosamente falsas al Directorio o a los órganos de la administración de las entidades por ellos administradas; a quien realice oferta pública de valores sin cumplir con los requisitos legales para ello; quienes actuaren como corredores de bolsa, agentes de valores, empresas de auditoría externa o clasificadoras de riesgo sin estar legalmente autorizado para ello; quien se valga de información privilegiada para realizar operaciones en el mercado de valores o negociaciones privadas con la finalidad de obtener un beneficio pecuniario, para sí o para un tercero; quien revele información privilegiada con el objeto de obtención de un beneficio para sí o para un tercero; quien deliberadamente elimine o modifique antecedentes de cualquier naturaleza, impidiendo la fiscalización de la Comisión; quien con el objeto de inducir a error en el mercado de valores difunda información falsa; a quien habiendo sido citado por el Fiscal a declarar en un proceso de investigación, no concurra sin causa justificada; al interesado apersonado en un procedimiento sancionatorio que no guarde reserva respecto de la información relativa a un proceso de investigación del cual fue parte; a quien constantemente eluda la fiscalización de la Comisión; a los directores y gerentes que hubieren realizado una declaración falsa sobre el patrimonio de la empresa; quien realice alteraciones a los balances de situación patrimonial de la empresa.

**Hipótesis en Vita:** Caso en el cual Vita, al no tener la correspondiente autorización ni registro, usare las denominaciones de corredor de bolsa, agentes de valores o clasificadora de riesgos para referirse a sí misma y al servicio prestado; caso en el cual la CMF fiscalizara a Vita y algún funcionario eliminara, alterara, modificara, ocultara o destruyera registros e información que formen parte de la investigación de la CMF; caso en que en un proceso de investigación iniciado por la CMF o el Fiscal correspondiente, Vita obstaculizare o impidiere ya a la CMF o al Fiscal el pleno ejercicio de sus funciones, esto es, no entregar la información requerida, entregar información falsa, entregar información tardía respecto de

la situación financiera de Vita; caso en que, de haber sido requerida a ello por la CMF o el Fiscal, Vita no proporcionare información, no proporcionare información veraz, no proporcionare información concreta respecto de su situación jurídica, económica o financiera al público; caso en que la CMF o el Fiscal cite a declarar a alguno de los socios, directores, representantes empleados y/o ex empleados de Vita a citar a declarar en un proceso de investigación, y las personas llamadas a ello no asistan sin entregar causa justificada de dicha inasistencia; caso en que la CMF o el Fiscal cite a declarar a alguna persona que la CMF o el Fiscal consideren que tenga conocimiento de algún hecho que se requiera aclarar en alguna operación realizada en Vita.

**Medida de Control:** programa de capacitaciones semestrales en materias de prevención de lavado de activos, financiamiento del terrorismo y demás delitos relevantes para Vita. Nombramiento de colaborador especialmente encargado de las comunicaciones con los reguladores.

**Áreas involucradas:** Gerencia, Producto, Operaciones, Soporte, Marketing, Ventas, Cumplimiento, Contabilidad y Finanzas, RRHH y Desarrollo; inversionistas y accionistas.

- Delitos Aduaneros: se sancionará a quien indebidamente perciba la devolución de costos de exportación; a quien realice contrabando.

**Hipótesis en Vita**: Caso en que los colaboradores, inversionistas o accionistas facilite pagos para transacciones ilegales relacionadas con la importación o exportación de productos prohibidos o regulados (como productos farmacéuticos, armas, o bienes culturales). Que contabilidad no realice en forma y dentro de la legalidad todas aquellas declaraciones y facturación relacionadas a la exportación de servicios de la empresa.

**Medida de Control:** Robusto sistema de Conocimiento del Cliente y Conocimiento de las Transacciones, recabando información personal y del origen de los fondos de los usuarios. Implementación de sistemas de monitoreo de transacciones en tiempo real que identifiquen pagos inusuales hacia y desde países o regiones con alto riesgo de contrabando, con una arista manual y otra automatizada. Dentro de dichos sistemas, se prevee la restricción de cuentas de usuarios que participen en sectores vulnerables al contrabando, como el comercio de productos de lujo, tabaco, alcohol o bienes culturales. Adicionalmente, se cuenta con una herramienta interna automatizada de geolocalización, que permite el rastreo de las ubicaciones de los usuarios, lo que permite, a su vez, tener especial cuidado con las transacciones que vayan dirigidas a zonas de tránsito internacional propensas al contrabando. Programa de capacitaciones semestrales en materias de prevención de lavado de activos, financiamiento del terrorismo y demás delitos relevantes para Vita. Auditorías en contabilidad para el cumplimiento de la resolución de exportación de servicios.

**Áreas involucradas:** Desarrollo, Gerencia, Cumplimiento, Operaciones, Producto, Soporte, Marketing, Ventas, Recursos Humanos y Contabilidad y Finanzas.

- Delitos Bancarios: se sancionará a quien incurriere en falsedad maliciosa en los documentos que acompañe en sus actuaciones con el Banco; a la persona jurídica, que no habiendo sido autorizada para ello, se dedique a un giro que corresponda a las empresas bancarias y promocione ese tipo de servicios, de la forma que sea; a

quien proporcione antecedentes relativos a operaciones de depósito y captaciones que reciba, a menos que la Comisión requiera dicha información para un proceso de investigación de su competencia; a la persona jurídica que omita contabilizar cualquier clase de operación que afecte al patrimonio de la misma.

**Hipótesis en Vita:** caso en que la empresa acompañe documentación que contenga falsedad maliciosa al banco; caso en que Vita ofrezca y realice servicios correspondientes a empresas bancarias. Caso en que se publique información en redes sociales relativa a la calidad de empresa bancaria de Vita, sin que Vita tenga dicha calidad. Caso en que se ofrezca un servicio bancario a potenciales clientes, que Vita no está autorizada para prestar. caso en que alguno de los directores o gerentes de Vitan realicen declaraciones falsas sobre la situación económica de la empresa.

**Medida de Control:** programa de capacitaciones semestrales en materias de prevención de lavado de activos, financiamiento del terrorismo y demás delitos relevantes para Vita. Adicionalmente, la empresa cuenta con un robusto sistema de análisis transaccional y de operaciones realizadas por los usuarios, el que se encuentra estrictamente asociado al giro de la Empresa, y no tiene relación directa ni coincidencia con el giro asociado específicamente a los bancos.

**Áreas involucradas:** Finanzas y Contabilidad, Gerencia; Cumplimiento; inversionistas, accionistas.

- Delitos contra Libre Competencia: se sancionará a la persona natural o jurídica que, habiendo sido requerida de información o actuación por parte del Fiscal Nacional Económico, no cumpla con el requerimiento de forma injustificada o cumpla con él de manera parcial; a quien alegue la existencia de conductas atentatorias a la libre competencia respecto de competidores con antecedentes falsos y con la finalidad de perjudicar a otros agentes económicos; será sancionado quien concierte con más agentes económicos la fijación/modificación de precios de los bienes y servicios ofrecidos, la limitación de su provisión, la repartición de zonas de mercados,

**Hipótesis en Vita:** eventual caso en el que la Empresa o alguno de sus colaboradores haya sido requerido de información por parte del Fiscal Nacional Económico, o haya sido requerido de realizar cualquier gestión en dicho sentido y no cumpla con ella; adicionalmente, también se contempla el caso en el cual el Fiscal Nacional Económico requiera de información a la empresa y que el responsable de hacerla llegar oculte información o entregue información falsa; caso en que algún funcionario de Vita o inversionista o accionista alegue que alguno de nuestros competidores haya realizado acuerdos con otros competidores o tengan prácticas asociadas a la fijación de precios de los servicios prestados por las empresas de la plaza, a la exclusión de competidores o a la afectación de las posibilidades de una licitación pública y aquello no sea cierto/ realice la alegación con antecedentes falsos o fraudulentos con la finalidad de obtener ventaja en el mercado respecto de dicho competidor; caso en que alguno de los funcionarios de Vita

celebre u ordene celebrar, ejecute u organice un acuerdo que involucre a dos o más competidores entre sí, para fijar precios de venta o de compra de bienes o servicios en uno o más mercados, o para limitar su producción o provisión, o dividir, asignar o repartir zonas o cuotas de mercado, o o afectar el resultado de licitaciones realizadas por empresas públicas, privadas prestadoras de servicios públicos, u órganos públicos. Adicionalmente, caso en que algún funcionario de Vita realice modificaciones en el admin de forma tal que los precios presenten diferencias con los precios normales de los envíos, comisiones o precios preferenciales; caso en que, desde el equipo de Operaciones se tenga noticia de que el cambio de una determinada divisa es un monto determinado, pero informe que dicho monto sea inferior o superior, generando una ganancia para la empresa o el trabajador en particular, con la contraprestación de un cobro excesivo que deberán costear los clientes.

**Medidas de Control:** programa de capacitaciones semestrales en materias de prevención de lavado de activos, financiamiento del terrorismo y demás delitos relevantes para Vita, como los delitos asociados a la libre competencia; constante evaluación de los protocolos del equipo de Ventas por parte el área de Cumplimiento y Legales para evitar que se generen actividades ilícitas asociadas a estos delitos; programa de auditoría interna, particularmente del área de Operaciones.

**Área involucrada:** Gerencia, Cumplimiento, Ventas, Operaciones; accionistas e inversionistas.

- Delitos contra la Propiedad Industrial: se sancionará a quienes utilicen con fines comerciales marcas ya inscritas, con inscripción caduca, sin derecho a usarla; a quienes falsifiquen y distribuyan productos de cualquier tipo; a quien realice las conductas antes descritas respecto de productos ya patentados.

**Hipótesis en Vita:** La Empresa podría utilizar un software especializado para la gestión de transacciones o seguridad de pagos que ha sido patentado por otra empresa, sin contar con las licencias necesarias para su uso. La Empresa podría utilizar imágenes, colores o símbolos que son idénticos o muy similares a los de una marca registrada en el ámbito de los servicios financieros. Algún colaborador podría copiar una base de datos de clientes que está protegida como un activo intangible de la empresa y luego vender o usar esa información para beneficio personal o para otras empresas competidoras.

**Medidas de Control:** capacitaciones semestrales en materias relevantes asociadas a la prevención del lavado de activos y financiamiento del terrorismo; auditoría interna a los equipos de Vita, para revisar los procesos, protocolos y acciones tomadas dentro de cada equipo en el ejercicio de las actividades correspondientes.

**Áreas involucradas:** Producto, Desarrollo, Marketing, Ventas; accionistas e inversionistas.

- Delitos contra la Propiedad Intelectual: se sancionará a quienes reproduzcan obras de dominio ajeno sin tener autorización para ello; a quienes falsifiquen obras protegidas por la Ley de Propiedad Intelectual; a quienes comercialicen las obras ya mencionadas.

**Hipótesis en Vita:** Casos en que algún colaborador de Vita o inversionistas/accionistas, en el ejercicio de sus labores, reproduzcan y utilicen softwares de dominio ajeno sin autorización, o los falsifiquen, haciéndolo pasar por propio de la Empresa.

**Medidas de Control:** capacitaciones semestrales en materias relevantes asociadas a la prevención del lavado de activos y financiamiento del terrorismo; auditoría interna a los equipos de Vita, para revisar los procesos, protocolos y acciones tomadas dentro de cada equipo en el ejercicio de las actividades correspondientes.
**Áreas involucradas:** Producto, Desarrollo, Marketing, Ventas; accionistas e inversionistas

- Delitos culposos: se sancionará a quien por imprudencia temeraria ejecutare un hecho que, si mediara malicia, constituiría un crimen o un simple delito contra las personas; a quien con infracción de los reglamentos y por mera imprudencia o negligencia, ejecutare un hecho o incurriere en una omisión que, a mediar malicia, constituiría un crimen o un simple delito contra las personas.

**Hipótesis en Vita:** Este tipo de delitos se refieren a aquellos en los que los colaboradores o inversionistas no tienen intención de causar un daño o cometer un delito, pero lo hacen por negligencia, descuido o falta de diligencia en el cumplimiento de sus responsabilidades. Caso en que hay negligencia en la detección de transacciones sospechosas vinculadas al lavado de activos. Caso en que haya falta de diligencia en la implementación de controles KYC. Caso en que haya negligencia en la protección de datos personales que facilita delitos informáticos. Caso en que haya negligencia en la actualización de sistemas de seguridad informática. Caso en que se omita la capacitación de empleados sobre prevención de delitos financieros y de otra índole relevante para la Empresa.

**Medidas de Control: c**apacitaciones semestrales en materias relevantes asociadas a la prevención del lavado de activos y financiamiento del terrorismo, así como también en cumplimiento normativo y ética; auditoría interna a los equipos de Vita, para revisar los procesos, protocolos y acciones tomadas dentro de cada equipo en el ejercicio de las actividades correspondientes; implementación de procedimientos detallados para la revisión y aprobación de transacciones. Utilización del Canal de Denuncias de la Empresa.

**Áreas involucradas:** Desarrollo, Gerencia, Cumplimiento, Operaciones, Producto, Soporte, Marketing, Ventas, Recursos Humanos y Contabilidad y Finanzas; accionistas e inversionistas.

- Delitos de Amenazas: se sancionará a quien amenazare seriamente a otro con causar a él mismo o a su familia, en su persona, honra o propiedad, un mal que constituya delito, siempre que por los antecedentes aparezca verosímil la consumación del hecho.

**Hipótesis en Vita:** Colaboradores involucrados en actividades fraudulentas o ilícitas podrían amenazar a otros empleados para silenciar cualquier posible denuncia o informe que los implique. Caso en que inversionistas amenacen a los integrantes de la gerencia para influir en decisiones relevantes para la Empresa. Caso en que colaboradores responsables de la gestión de proveedores o asociaciones comerciales empleen amenazas para forzar a los proveedores a otorgar mejores términos o para asegurar la cooperación en

prácticas cuestionables. Caso en que se generen amenazas internas para forzar la aprobación de clientes de alto riesgo.

**Medidas de Control:** capacitaciones semestrales en materias relevantes asociadas a la prevención del lavado de activos y financiamiento del terrorismo, así como también en materias de conducta ética; auditoría interna a los equipos de Vita, para revisar los procesos, protocolos y acciones tomadas dentro de cada equipo en el ejercicio de las actividades correspondientes.Utilización del Canal de Denuncias de la Empresa para que los colaboradores y terceros puedan dar cuenta de actividades irregulares dentro de la plataforma.

**Áreas involucradas:** Desarrollo, Gerencia, Cumplimiento, Operaciones, Producto, Soporte, Marketing, Ventas, Recursos Humanos y Contabilidad y Finanzas; accionistas e inversionistas.

- Delitos contra la Seguridad Social: se sancionará al empleador que no pague en tiempo y forma las cotizaciones previsionales, de salud ni seguro de cesantía a sus trabajadores o realice pagos incompletos de los mismos; se sancionará al empleador que retenga montos que le corresponda percibir a los trabajadores, relativo a sus cotizaciones; a las personas que incurran en falsedad en la certificación de enfermedades, lesiones, estados de salud, en las fechas de los diagnósticos o en prestaciones otorgadas; a la persona jurídica, que no estando debidamente registrada, se dedique al giro propio de las administradoras de fondos de pensión; a quien falsifique u oculte información que haya sido requerida por la Superintendencia de Pensiones.

**Hipótesis en Vita:** caso en que Vita no pague o pague de forma incompleta o extemporánea las cotizaciones previsionales de sus trabajadores. Caso en que Vita como empleador pagara subsidios a sus trabajadores y no lo hiciera en tiempo y forma, y no lo declarara ante la Administradora correspondiente. Caso en que Vita no realice la declaración de cotizaciones previsionales pagadas respecto de un trabajador que ha sido desvinculado, ya por Vita, ya en la figura de despido indirecto. Caso en que Vita como empresa o alguno de sus funcionarios, en perjuicio del trabajador o de sus derechohabientes se apropiare o distrajere el dinero proveniente de las cotizaciones que se hubiere descontado de la remuneración del trabajador. Caso en que Vita sin el consentimiento del trabajador, omita retener o enterar las cotizaciones previsionales de un trabajador o declare ante las instituciones de seguridad social, pagarle una renta imponible o bruta menor a la real, disminuyendo el monto de las cotizaciones que debe descontar y enterar. Caso en que Vita omita retener o enterar las cotizaciones previsionales de un trabajador o declare ante las instituciones de seguridad social, pagarle una renta imponible o bruta menor a la real, disminuyendo el monto de las cotizaciones que debe descontar y enterar, con el consentimiento del trabajador obtenido en razón de su grave de su situación de necesidad, inexperiencia o incapacidad de discernimiento. Caso en que Vita no haya pagado las cotizaciones previsionales a sus trabajadores y reciba recursos provenientes de

otras instituciones financieras con cargo a recursos fiscales de fomento productivo. Caso en que Vita haya pagado las cotizaciones previsionales a sus trabajadores, pero no lo haya acreditado y reciba recursos provenientes de otras instituciones financieras con cargo a recursos fiscales de fomento productivo. Caso en que Vita ofreciera servicios propios de una Institución de Salud Previsional y comenzara a captar cotizaciones de salud. Caso en que Vita exprese al público ser una Institución de Salud Previsional, con propaganda de ello, sin serlo. Caso en que Vita falsifique u oculte información a la Superintendencia de Salud en un proceso de requerimiento de información por parte de dicha institución.

**Medida de Control:** capacitaciones semestrales en materias relevantes asociadas a la prevención del lavado de activos y financiamiento del terrorismo; auditoría interna a los equipos de Vita, para revisar los procesos, protocolos y acciones tomadas dentro de cada equipo en el ejercicio de las actividades correspondientes.

**Áreas involucradas:** Cumplimiento, Contabilidad y Finanzas, Recursos Humanos; accionistas e inversionistas.

- Delitos asociados a Estafas y Otras Defraudaciones: se sancionará al que defraudare a otro en la sustancia, cantidad o calidad de las cosas que le entregare en virtud de un título obligatorio; a quienes en perjuicio de otro se apropiaren o distrajeren dinero, efectos o cualquiera otra cosa mueble que hubieren recibido en depósito, comisión o administración, o por otro título que produzca obligación de entregarla o devolverla; a quienes cometieren alguna defraudación abusando de firma de otro en blanco y extendiendo con ella algún documento en perjuicio del mismo o de un tercero; a quienes cometieren defraudaciones sustrayendo, ocultando, destruyendo o inutilizando en todo o en parte algún proceso, expediente, documento u otro papel de cualquiera clase; a quienes con datos falsos u ocultando antecedentes que les son conocidos, celebraren dolosamente contratos aleatorios basados en dichos datos o antecedentes; a quienes defraudaren haciendo suscribir a otro con engaño algún documento; a quien teniendo a su cargo la salvaguardia o la gestión del patrimonio de otra persona, o de alguna parte de éste, en virtud de la ley, de una orden de la autoridad o de un acto o contrato, le irrogare perjuicio, sea ejerciendo abusivamente facultades para disponer por cuenta de ella u obligarla, sea ejecutando u omitiendo cualquier otra acción de modo manifiestamente contrario al interés del titular del patrimonio afectado; a quien otorgare en perjuicio de otro un contrato simulado.

**Hipótesis en Vita:** Caso en que alguno de los colaboradores con acceso a las cuentas y transacciones de los usuarios aprovechen su posición para desviar fondos de manera fraudulenta. Caso en que integrantes del área de Gerencia o inversionistas/accionistas cometan fraude contable manipulando los datos de la Empresa para inflar cifras de crecimiento, de volumen transaccional o cantidad de usuarios activos. Caso en que alguno

de los colaboradores manipulen los sistemas de cobros o de comisiones para sobrecargar a los usuarios o aplicar cobros indebidos, generando una ganancia mal habida. Caso en que integrantes del área de Gerencia o inversionistas/accionistas cometan fraude al falsificar documentación financiera de la Empresa para acceder a beneficios. Caso en que alguno de los colaboradores cometa fraude de devoluciones de pagos asociados a la Vita Card.

**Medidas de Control:** capacitaciones semestrales en materias relevantes asociadas a la prevención del lavado de activos y financiamiento del terrorismo; auditoría interna a los equipos de Vita, para revisar los procesos, protocolos y acciones tomadas dentro de cada equipo en el ejercicio de las actividades correspondientes.

**Áreas involucradas:** Desarrollo, Gerencia, Cumplimiento, Operaciones, Producto, Soporte, Marketing, Ventas, Recursos Humanos y Contabilidad y Finanzas; accionistas e inversionistas.

- Delitos asociados a la Falsedad de Documentos Públicos y Privados: se sancionará al particular que cometiere en documento público falsedades; al que maliciosamente hiciere uso del documento falso.

**Hipótesis en Vita:** Caso en que inversionistas falsifiquen documentos financieros para obtener líneas de crédito, financiamiento o inversiones basadas en información engañosa. Caso en que algún colaborador o inversionista/accionista presenta informes falsos o alterados a las autoridades reguladoras para encubrir fraudes, deficiencias financieras o actividades ilegales. Caso en que algún colaborador o inversionista falsifican firmas en documentos relevantes para la autorización de transacciones o relativas a decisiones de alto impacto para la Empresa. Caso en que algún colaborador o inversionista/accionista altere documentación de la empresa en procesos de Debida Diligencia.

**Medidas de Control:** capacitaciones semestrales en materias relevantes asociadas a la prevención del lavado de activos y financiamiento del terrorismo; auditoría interna a los equipos de Vita, para revisar los procesos, protocolos y acciones tomadas dentro de cada equipo en el ejercicio de las actividades correspondientes. Adicionalmente, se cuenta con una robusta política de gestión documental y controles de acceso para la documentación relevante. Finalmente, se cuenta con un Canal de Denuncias en el cual los colaboradores y terceros podrán dar cuenta de eventuales operaciones irregulares que evidencien,

**Áreas involucradas:** Gerencia, Cumplimiento, Desarrollo, Operaciones, Producto, Soporte, Marketing, Ventas, Recursos Humanos y Contabilidad y Finanzas; accionistas e inversionistas.

- Delitos de Financiamiento Irregular de la Política: se sancionará a quien estando obligado a ello, proporcione antecedentes falsos o certifique hechos falsos en sus rendiciones de cuentas al Servicio Electoral.

**Hipótesis en Vita:** Caso en el que se desvíen fondos de la Empresa para financiar campañas políticas, disfrazándolos de pagos legítimos. Caso en que algún colaborador o inversionista utilice la plataforma de Vita Wallet para canalizar donaciones ilícitas. Caso en que se financien de eventos políticos bajo la fachada de actividades corporativas. Caso en

que se utilicen los servicios de Vita Wallet para fragmentar grandes donaciones.Caso en que alguno de los colaboradores o inversionistas presten servicios de asesoría a partidos políticos disfrazados de operaciones comerciales.

**Medidas de Control:** capacitaciones semestrales en materias relevantes asociadas a la prevención del lavado de activos y financiamiento del terrorismo; auditoría interna a los equipos de Vita, para revisar los procesos, protocolos y acciones tomadas dentro de cada equipo en el ejercicio de las actividades correspondientes. Adicionalmente, se cuenta con robustas políticas de Conocimiento del Cliente, así como también monitoreo de transacciones y se cuenta, también, con el Canal de Denuncias de la Empresa.

**Áreas involucradas:** Gerencia, Cumplimiento, Recursos Humanos y Contabilidad y Finanzas; accionistas e inversionistas.

- Delitos asociados a Fraude de Cheques o Tarjetas de Pago y Transacciones Electrónicas: se sancionará a quien en la gestión de notificación de un protesto de cheque tache de falsa su firma y resultare en definitiva que dicha firma es auténtica; a quien utilice maliciosamente una tarjeta de pago o clave y demás credenciales de seguridad o autenticación, que se encuentren bloqueadas; a quien obtenga maliciosamente, para sí o para un tercero, el pago total o parcial indebido, sea simulando la existencia de operaciones no autorizadas, provocándolo intencionalmente, o presentándolo ante el emisor como ocurrido por causas o en circunstancias distintas a las verdaderas

**Hipótesis en Vita:** Casos en que colaboradores o inversionistas manipulen sistemas de pagos, creen mecanismos fraudulentos o abusen de su posición dentro de la empresa para cometer actos delictivos que involucren el uso indebido de tarjetas de pago (crédito o débito) y transacciones electrónicas. Caso en que alguno de los colaboradores de la Empresa manipule el sistema de devoluciones (*''chargeback"*) de pagos para beneficio propio o de terceros.

**Medidas de Control:** capacitaciones semestrales en materias relevantes asociadas a la prevención del lavado de activos y financiamiento del terrorismo; auditoría interna a los equipos de Vita, para revisar los procesos, protocolos y acciones tomadas dentro de cada equipo en el ejercicio de las actividades correspondientes.Adicionalmente, se cuenta con un sistema de monitoreo y autorización transaccional, con una arista automatizada y ot5ra manual, que es revisada por operadores de la Empresa para poder procesar o no una determinada transacción. Monitoreo transaccional en tiempo real y aplicación de protocolos de prevención de fraude en las operaciones de los usuarios, compuestos, entre otras cosas, por alertas automatizadas asociadas a la señales de alerta propias de la Empresa.

**Áreas involucradas:** Gerencia, Cumplimiento, Desarrollo, Operaciones, Producto, Soporte, Marketing, Ventas, Recursos Humanos y Contabilidad y Finanzas; accionistas e inversionistas.

- Delitos de Revelación de Información: se sancionará a quien fraudulentamente hubiere comunicado secretos de la empresa en que ha estado o está empleado.

**Hipótesis en Vita:** Caso en el cual alguno de los colaboradores o inversionistas/accionistas de la empresa realice una divulgación no autorizada de información confidencial y/o sensible de la Empresa. Caso en el cual los accionistas o inversionistas hagan uso indebido de información privilegiada relativa a la Empresa y/o su funcionamiento, en atención a su especial posición dentro de la Empresa.

**Medidas de Control:** capacitaciones semestrales en materias relevantes asociadas a la prevención del lavado de activos y financiamiento del terrorismo; auditoría interna a los equipos de Vita, para revisar los procesos, protocolos y acciones tomadas dentro de cada equipo en el ejercicio de las actividades correspondientes. Entrega del Código de Ética de la Empresa, así como también del Modelo y Manual de Prevención de Delitos a cada nuevo integrante de la Empresa, con la finalidad de que se permee de las expectativas de comportamiento dentro de Vita Wallet y sus consecuencias negativas. Robustas políticas de Confidencialidad y Acuerdos de No Divulgación para con los clientes y/o proveedores. Canal de Denuncias de Vita Wallet.

**Áreas involucradas:** Gerencia, Cumplimiento, Desarrollo, Operaciones, Producto, Soporte, Marketing, Ventas, Recursos Humanos y Contabilidad y Finanzas; accionistas e inversionistas.

- Delitos de Robo: se sancionará a quien, para obtener un provecho patrimonial para sí o para un tercero, constriña a otro con violencia o intimidación a suscribir, otorgar o entregar un instrumento público o privado que importe una obligación estimable en dinero, o a ejecutar, omitir o tolerar cualquier otra acción que importe una disposición patrimonial en perjuicio suyo o de un tercero.

**Hipótesis en Vita:** Colaborador, accionista o inversionista que, con la finalidad de generar un beneficio a la empresa, obligue a un tercero a firmar un contrato. Obligar a un ministro de fe, certificador o auditores a generar documentación falsa para procesos de debida diligencia.

**Medidas de Control:** capacitaciones semestrales en materias relevantes asociadas a la prevención del lavado de activos y financiamiento del terrorismo; auditoría interna a los equipos de Vita, para revisar los procesos, protocolos y acciones tomadas dentro de cada equipo en el ejercicio de las actividades correspondientes.

**Áreas involucradas:** Gerencia, Cumplimiento, Desarrollo, Operaciones, Producto, Soporte, Marketing, Ventas, Recursos Humanos y Contabilidad y Finanzas; accionistas e inversionistas.

- Delitos asociados a Procedimientos Concursales y de Reorganización: se sancionará a los asesores que se concierten con algún deudor o acreedor para proporcionar ventajas indebidas para sí o para terceros; al veedor o liquidador designado en un procedimiento concursal de reorganización o liquidación que se apropiare de bienes del deudor que deban ser objeto de un procedimiento concursal

de reorganización o liquidación, que defraudare a los acreedores, alterando en sus cuentas de administración los valores obtenidos en el procedimiento concursal de reorganización o liquidación, suponiendo gastos o exagerando los que hubiere hecho, o que proporcionare ventajas indebidas a un acreedor, al deudor o a un tercero; la persona jurídica sujeto de un procedimiento concursal disminuyere, ocultare su patrimonio de cualquier forma durante los dos años anteriores a la resolución de liquidación.

**Hipótesis en Vita:** Caso en que, en medio de un eventual proceso de concursal y/o de reorganización por el cual esté pasando la Empresa, algún colaborador, accionista o inversionista utilice la plataforma para ocultar o desviar bienes propios de la Empresa, por ejemplo, realizando envíos de criptomonedas con fondos de la Empresa ‘’guardados’’ para dicho fin. Caso en que inversionistas o accionistas den preferencia a determinados acreedores con los que tienen vínculos de forma tal que sus deudas se paguen primero que las de los acreedores legítimos. Caso en que alguno de los colaboradores destruya o manipule documentación contable relevante de la Empresa para el proceso en el que se encuentra. Caso en que se genere una reorganización fraudulenta para eludir responsabilidades propias de la Empresa.

**Medidas de Control:** capacitaciones semestrales en materias relevantes asociadas a la prevención del lavado de activos y financiamiento del terrorismo; auditoría interna a los equipos de Vita, para revisar los procesos, protocolos y acciones tomadas dentro de cada equipo en el ejercicio de las actividades correspondientes. Adicionalmente, se cuenta con controles internos de Gestión Financiera, con protocolos de constante monitoreo transaccional y operacional y con el Canal de Denuncias de la Empresa.

**Áreas involucradas:** Gerencia, Cumplimiento, Desarrollo, Operaciones, Producto, Soporte, Marketing, Ventas, Recursos Humanos y Contabilidad y Finanzas; accionistas e inversionistas.

- Delitos en relación al Contrato de Prenda: se sancionará a quien defraudare a otro disponiendo de las cosas constituidas en prenda en conformidad a esta ley, sin señalar el gravamen que las afecta o constituyendo prenda sobre bienes ajenos como propios, o alzando la prenda que haya cedido, al deudor prendario y el que tenga en su poder la cosa constituida en prenda en conformidad a esta ley que, defraudando al acreedor prendario, la altere, oculte, sustituya, traslade o disponga de ella, y al deudor prendario que, tratándose de prendas de créditos o de cualquier otra clase de derechos constituidos en prenda en conformidad a esta ley, defraude al acreedor prendario, ocasionando la pérdida o el menoscabo de los derechos otorgados en garantía.

**Hipótesis en Vita:** Accionistas o inversionistas que con la finalidad de mejorar la capacidad económica o financiera de la empresa graven bienes de forma ilegal.

**Medidas de Control:** auditoría interna a los equipos de Vita, para revisar los procesos, protocolos y acciones tomadas dentro de cada equipo en el ejercicio de las actividades correspondientes.

**Áreas involucradas:** Gerencia, Cumplimiento, Desarrollo, Operaciones, Producto, Soporte, Marketing, Ventas, Recursos Humanos y Contabilidad y Finanzas; accionistas e inversionistas.

- Delitos en relación con la Gestión de Residuos: se sancionará a quien exporte, importe o maneje residuos peligrosos, prohibidos o sin contar con las autorizaciones para ello.

**Hipótesis en Vita:** casos de eventuales residuos tecnológicos que pudiesen quedar del desarrollo de la actividad comercial.

**Medidas de Control:** capacitaciones semestrales en materias relevantes asociadas a la prevención del lavado de activos y financiamiento del terrorismo; auditoría interna a los equipos de Vita, para revisar los procesos, protocolos y acciones tomadas dentro de cada equipo en el ejercicio de las actividades correspondientes.

**Áreas involucradas:** Gerencia, Cumplimiento, Desarrollo.

- Delitos asociados a relaciones con Proveedores: se sancionará a quienes hayan sido culpables del fraude en la naturaleza, calidad o cantidad de los objetos o mano de obra, o de las cosas suministradas, con daño grave e inevitable de la causa pública.

**Hipótesis en Vita:** prestación de servicios viciosa.

**Medidas de Control:** auditoría interna a los equipos de Vita, para revisar los procesos, protocolos y acciones tomadas dentro de cada equipo en el ejercicio de las actividades correspondientes; QA.

**Áreas involucradas:** Gerencia, Cumplimiento, Desarrollo, Operaciones, Producto, Soporte, Marketing, Ventas, Recursos Humanos y Contabilidad y Finanzas; accionistas e inversionistas; proveedores.

- Delitos Tributarios: se sancionará a quien maliciosamente aporte información fraudulenta a la autoridad con la finalidad de obtener la autorización de los documentos necesarios para el desarrollo de su giro; a su vez, será sancionado quien presente declaraciones maliciosamente falsas o incompletas a fin de recibir un beneficio o burlar un impuesto; la omisión maliciosa de declaraciones exigidas por las leyes tributarias para la determinación o liquidación de un impuesto; quien realice determinado comercio ejercido a sabiendas sobre mercaderías, valores o especies de cualquiera naturaleza sin que se hayan cumplido las exigencias legales relativas a la declaración y pago de los impuestos que graven su producción o comercio; a quien realice el ejercicio efectivamente clandestino del comercio o de la industria; la reapertura de un establecimiento comercial o industrial o de la sección que corresponda, con violación de una clausura impuesta por el Servicio de Impuestos Internos; el que maliciosamente utilizare los cuños verdaderos u otros medios tecnológicos de autorización del Servicio para defraudar al Fisco.

**Hipótesis en Vita:** ejercicios tributarios maliciosos realizados por la contabilidad de la empresa.

**Medidas de Control:** auditoría interna a los equipos de Vita, para revisar los procesos, protocolos y acciones tomadas dentro de cada equipo en el ejercicio de las actividades correspondientes.

**Áreas involucradas:** Gerencia, Cumplimiento, Contabilidad y Finanzas; accionistas e inversionistas.

# III. POLÍTICAS DE PREVENCIÓN Y DETECCIÓN DE DELITOS DE LAVADO DE ACTIVOS Y FINANCIAMIENTO DEL TERRORISMO

En base a la identificación del riesgo de LA/FT que ha realizado Vita Wallet dentro de su funcionamiento general e integral, se especificarán las políticas, controles y protocolos que permitan prevenir y detectar operaciones sospechosas asociadas a dichos delitos, entre ellos la creación y mantención del Canal de Denuncias. Este es de vital importancia para la Empresa, pues le permitirá recibir denuncias directas y anónimas sobre posibles infracciones internas, incumplimiento de las normas, conflicto de intereses, conductas ilegales, eventuales delitos cibernéticos, eventuales delitos de LA/FT, cohecho a funcionarios públicos nacionales o extranjeros, faltas a la ética y buenas costumbres, así como de cualquier otra clase de delitos que se pudiesen presentar tanto por empleados, dueños, fundadores, terceros con quien se pueda tener alguna alianza, como por los usuarios de la Empresa.

Es importante señalar respecto del Canal de Denuncias, que Vita Wallet se compromete a realizar un análisis oportuno, independiente, confidencial y sin represalias a sus denunciantes, a través de un proceso estructurado y monitoreado por el funcionario responsable designado y a su vez, este se encargará de hacer llegar los reportes respectivos a los entes encargados de llevar los procesos de investigación respectiva. Todas estas denuncias podrán realizarse a través del formulario de Canal de Denuncias disponible en el sitio web (https://vitawallet.io/politica-de-cumplimiento/). Con fin de dar cumplimiento a lo anteriormente descrito, VITA SOLUTIONS SPA hace la siguiente descripción:

# 1. DE LA DEBIDA DILIGENCIA Y CONOCIMIENTO DEL CLIENTE (DDC)

## 1.1. DDC ESTÁNDAR Y CONTINUA

Vita Wallet funciona a través de la utilización que sus usuarios hacen de los servicios de transferencias de dinero, servicio al cual acceden registrándose en la plataforma de vitawallet.io y leyendo y aceptando los Términos y Condiciones de la plataforma.

Por esto, y dando cumplimiento al Título III número 2, de la Circular N° 49 del año 2012, modificada por la Circular N° 59 del año 2019, Vita Wallet recopila los siguientes datos sobre cada uno de los usuarios registrados:

### 1.1.1. Información relativa a la verificación de personas naturales.

1.1.1.1. Nombre.
1.1.1.2. Número de documento de identidad.
1.1.1.3. Estado civil.
1.1.1.4. Sexo.
1.1.1.5. Lugar de nacimiento.
1.1.1.6. Profesión, ocupación u oficio.
1.1.1.7. País de residencia.
1.1.1.8. País de emisión del documento de identidad.
1.1.1.9. Correo electrónico.
1.1.1.10. Número de teléfono de contacto.
1.1.1.11. Imagen del documento de identidad.
1.1.1.12. Imagen del rostro de la persona que se registra (verificación biométrica)
1.1.1.13. Propósito de la relación legal o contractual, o de la transacción ocasional.

### 1.1.2. Información relativa a la verificación de personas jurídicas.

1.1.2.1. Nombre legal de la empresa.
1.1.2.2. Número de documento de identificación de la empresa.
1.1.2.3. Domicilio de la empresa.
1.1.2.4. Naturaleza del negocio realizado por la empresa.
1.1.2.5. Uso que desea darle a la plataforma de Vita.
1.1.2.6. Nombre de fantasía *(''doing business as"),* si aplica.
1.1.2.7. País y fecha de constitución.
1.1.2.8. Información relativa al modelo de negocios:
  1.1.2.8.1. Número de empleados de la empresa.
  1.1.2.8.2. Link de la página web.
  1.1.2.8.3. Descripción detallada del modelo de negocio, producto o servicio y tipo de clientes.
1.1.2.9. Información relativa al representante legal:
  1.1.2.9.1. Nombre completo.
  1.1.2.9.2. Cargo dentro de la empresa.

1.1.2.9.3. Correo electrónico de contacto.
1.1.2.9.4. Número de teléfono de contacto.
1.1.2.10. Información relativa a los beneficiarios finales efectivos, directos o indirectos, con una participación superior al 20%:
1.1.2.10.1. Nombre completo.
1.1.2.10.2. Fecha de nacimiento.
1.1.2.10.3. Domicilio.
1.1.2.10.4. Porcentaje de propiedad.
1.1.2.10.5. Número de documento de identidad.
1.1.2.11. Información relativa a todos los directorios y, al menos, de un miembro de la Alta Dirección (Gerente General, Gerente de Operaciones, etc. )
1.1.2.11.1. Nombre completo.
1.1.2.11.2. Fecha de nacimiento.
1.1.2.11.3. Profesión.
1.1.2.11.4. Domicilio.
1.1.2.11.5. Número de documento de identidad.

Adicionalmente a lo anterior, para verificar **cuentas asociadas a personas jurídicas** se solicita la siguiente información adicional:

- Copia del documento nacional de identidad del representante autorizado.
- Copia del documento nacional de identidad de los beneficiarios finales.
- Copia del documento nacional de identidad de cada Director y miembros de la Alta Dirección.
- Comprobante de domicilio de la persona jurídica con una antigüedad no mayora 90 días.
- Copia de documentación que permita acreditar la existencia de la persona jurídica como el acta constitutiva, escritura social, contrato de sociedad, registro en los organismos públicos de comercio.
- Copia del documento tributario de la empresa.
- Cualquier otra información adicional necesaria para verificar que la naturaleza de la entidad se condiga con la información aportada por ella.

Junto con lo anterior, también contamos con un listado de documentación que se le solicita a las empresas cuando su giro es alguno de los siguientes:

**a) Instituciones financieras:** además de la información antes indicada, se solicitará:
i) Lista de todos los países en los que la institución tenga licencia o se encuentre registrada.
ii) Descripción de los tipos de clientes y ubicación de los mismos.
iii) La siguiente información del Oficial de Cumplimiento:
1) Nombre completo.
2) Cargo.
3) Domicilio.
4) Estructura Compliance o Políticas AML de la empresa en donde ejerce sus funciones.

5) Identificación de los destinatarios de las transacciones, motivo de ellas y su correspondiente comprobante.

**b) Negocios de servicios de dinero:** además de la información antes indicada, se solicitará:

i) Misma información requerida para instituciones financieras.
ii) Si el cliente está ubicado o tiene clientes en Estados Unidos, se requerirá el número de registro en la ‘’Crime Enforcement Network’’ (FinCen).
iii) Si el cliente es una empresa transmisora de dinero ubicada en Estados Unidos o que tiene clientes en dicho país, se requerirá adicionalmente la ‘’Money Transmitter’s License’’ (MLT) o una opinión legal del cliente indicando porqué no se requiere dicha licencia.
iv) Si el cliente está ubicado o tiene clientes en el Reino Unido, se requerirá el número de registro del cliente en la ‘’Financial Conduct Authority (‘’FCA’’), o evidencia de que la FCA ha generado un registro temporal al cliente.
v) Si el cliente está ubicado o tiene clientes en Canadá, se requerirá el número de registro del cliente en el ‘’Financial Transactions and Reports Analysis Center’’
vi) Si el cliente está ubicado o tiene clientes en Australia, se requerirá el número de registro en el ‘’Australian Transaction Reports and Analysis Center’’
vii) Si el cliente está ubicado o tiene clientes en Singapur, se requerirá el número de registro en el ‘’Monetary Authority of Singapore’’

**c) Fondos de inversión:** además de la información antes indicada, se solicitará:

i) Misma información requerida para las instituciones financieras.
ii) Copia del folleto, memorando de oferta o memorando de colocación privada de los fondos.
iii) Confirmación de que el administrador del fondo está registrado cumpliendo con todas las exigencias legales.

**d) Empresas de gestión de activos:** además de la información antes indicada, se solicitará:

i) Misma información requerida para las instituciones financieras.
ii) Copia de la declaración de política de inversión o documento regulador.

**e) Fideicomisos:** además de la información antes indicada, se solicitará:

i) Nombre y fecha de nacimiento del individuo que establece el fideicomiso.
ii) Nombre y fecha de nacimiento del individuo establecido para dirigir a los fideicomisarios en relación con su administración del fideicomiso.
iii) Respecto de la persona o institución que tiene la administración del fideicomiso, si se trata de una persona natural, se requerirá su nombre y fecha de nacimiento; si se trata de una persona jurídica se requerirá la información relativa al ‘’KYC’’ solicitada para todas las personas jurídicas con cuentas en Vita Wallet.
iv) Contrato o escritura en donde conste el fideicomiso.

La política descrita anteriormente en el caso de personas jurídicas, se aplicará también para los casos de tutores en los casos en se requiera. Esta información del usuario deberá actualizarse en el plazo máximo de un año, sin excepción, ya que las relaciones comerciales pueden verse afectadas por cambios en la actividad financiera del usuario. Este comportamiento se mantendrá siempre que exista una relación de Vita Wallet y el usuario.

Esta recopilación de información de cada uno de los usuarios es realizada a través de las siguientes etapas:

**Verificación del usuario:**

Consiste en solicitarle al usuario información y documentación, a través del registro en la plataforma de Vita Wallet y con el apoyo de un software biométrico automatizado -Onfido- a partir del cual se puede verificar su identidad y documento de identidad, y generar información conexa; este proceso es complementado con los softwares de *''name screening"* Neitcom y Truora, que permiten una revisión más completa del estatus de los usuarios, relativo a si se encuentran en listas restrictivas que impidan su verificación en la plataforma. Es de vital importancia dentro del mercado financiero contar con esta información, ya que hace posible poder cumplir con el deber de conocer el origen legal de los fondos manejados por los usuarios, así como de su capacidad para manejar dichos fondos.

Por ello, la verificación de los usuarios es de carácter obligatorio, ya que le permite a la Empresa evitar que, por acción u omisión, sus servicios sean utilizados para encubrir fondos que pudieren provenir de fuentes ilícitas.

Tomando en cuenta que actualmente las personas jurídicas son el medio más usado para la comisión de delitos de LA/FT, ya sea por medio de transacciones financieras o por la adquisición de activos de valores muy altos o sobrevaluados, se solicitará el perfil financiero no solo de la persona jurídica, sino también de sus fundadores, directivos, representantes legales, propietarios, así como toda la información detallada de actividad de la persona jurídica y de las personas naturales que están detrás de ella, sus beneficiarios finales.

**Protocolo de aceptación del usuario:**

La persona natural, como usuario persona o como representante legal de una empresa, al crear una cuenta en Vita, debe entregar información mínima imprescindible para poder acceder a los servicios que la Empresa ofrece. Como se estableció anteriormente, se solicita al momento del registro en la plataforma: nombre, apellido, estado civil, profesión u ocupación, sexo, fecha de nacimiento, país de nacimiento, dirección de residencia, país de residencia, ciudad de residencia, código postal, teléfono, número de documento de identidad y fotografías del mismo, así como también fotografía del rostro del usuario en verificación.

Esta labor se realiza a través de un software especializado en biometría llamado Onfido, el cual además de extraer los datos personales requeridos, permite el reconocimiento facial del usuario que está en proceso de registro. A mayor abundamiento, mediante la verificación biométrica de los perfiles se revisa la prueba de vida del usuario y también su

documento de identidad, país al cual corresponde dicho documento, y que la información aportada por el usuario a la hora de verificarse se condiga con la aportada en la verificación biométrica de su perfil, y, además, que dicha información no se encuentre repetida en un registro anterior, ya que, por política de la Empresa -y para la prevención de la eventual comisión de delitos- cada usuario de Vita podrá mantener activa **una sola cuenta su nombre,** salvo situaciones excepcionalísimas.

Este proceso de verificación biométrica es complementado por la revisión, también automatizada, de *''name screening",* llevada a cabo por las herramientas Neitcom y Truora, como ya se indicó, en donde se genera una revisión asociada al nombre, número de documento de identidad y país de residencia del usuario en verificación y que permite verificar, entre otras cosas, la calidad de Persona Expuesta Políticamente de un eventual usuario (o destinatario de la transacción de un usuario ya verificado) o de encontrarse dentro de alguna de las listas restrictivas internacionales o de tener antecedentes penales de relevancia para la operación de la Empresa.

En el párrafo anterior puede apreciarse la información y documentación necesaria para una verificación exitosa. Siempre será obligatorio acompañar los siguientes documentos: i) el documento de identidad; ii) una imagen del rostro (que se extrae durante el proceso biométrico del registro de usuario); iii) documentación de comprobante de domicilio; iv) documentación de origen de fondos. Estas dos últimas serán requeridas con posterioridad a la verificación del usuario, con el objeto de tomar conocimiento y mantener antecedentes del comportamiento del usuario en la plataforma.

Asimismo, la plataforma cuenta con sistema de evaluación de riesgos para la verificación de los usuarios en el proceso de registro, y su respectivo uso de la plataforma, basado en los siguientes elementos: i) segmento B2B y B2C; ii) el país de residencia; iii) montos deseados a transaccionar; iv) servicios o productos que el usuario desea obtener, tales como acceso a criptomonedas (intercambio), Vita Card[4], cuenta en USD y links de pago. Actualmente la plataforma de Vita cuenta con un sistema de limitación de transacciones y de generación automatizada de alertas respecto de determinados umbrales de montos, países, y transacciones relacionadas. Adicionalmente a ello, se cuenta con la posibilidad de revisar permanentemente las IP de los usuarios, de su registro, sesiones y transacciones, y cuando cambia de lugar geográfico emite una alerta, que será analizada por el equipo de Cumplimiento para verificar el comportamiento del usuario en cada caso, y toma una decisión respecto tanto de la transacción como de la cuenta del usuario que la realiza. Sobre las señales de alerta y los protocolos que estas gatillan se hará una revisión más detallada en un acápite posterior.

A este respecto es imprescindible hacer presente que toda vez que el análisis que realice el analista de Cumplimiento y el Oficial de Cumplimiento determine irregularidades en el comportamiento operacional de los usuarios, dicho equipo podrá solicitar información adicional que permita aclarar la situación irregular o inusual asociada a determinada transacción y/o comportamiento operacional, pudiendo, adicionalmente, bloquear determinada transacción o determinadas transacciones hasta que pueda esclarecerse su

[4] Tarjeta de prepago virtual asociada a la plataforma de Vita.

naturaleza, impidiendo, así, que esta sea procesada hasta contar con la información necesaria para que pueda ser normalmente procesada o bien, rechazada.

Adicionalmente, es menester hacer presente que determinadas jurisdicciones cuyo registro de usuarios está prohibido, estas son: Estados Unidos de América, en todos sus estados; Rusia; Cuba; Irán; Corea del Norte; Siria; Birmania; Albania; Barbados; Burkina Faso; Camboya; Islas Caimán; República del Congo; Gibraltar; Haití; Jamaica; Jordan; Mali; Morocco; Mozambique; Nigeria; Panamá; Filipinas; Senegal; Sudáfrica, Sudán del Sur; Syria; Tanzania; Turquía; Uganda; Emiratos Árabes; Yemen; Afganistán; Bielorrusia; República Centroafricana; Guinea-Bisáu; Irak; Libia; Myanmar; Somalia; Sudán; Ucrania.

**Revisión de los antecedentes aportados.**

Una vez que el eventual usuario realiza la solicitud de verificación acompañando la información antes mencionada, dicha información y documentación pasará por un proceso de revisión, que tiene una arista automática y una arista manual, a saber: la verificación del usuario se generará de forma **automática** cuando en el acompañamiento de información y documentación no hayan reparos por parte del sistema, y eso sucederá cuando acompañe fotografías nítidas y completas tanto de su documento de identidad como de su fotografía selfie, y haya completado sus datos de forma íntegra y no posea coincidencias reportadas por los softwares de *name screening* y de verificación biométrica.

En el evento de que alguno de estos factores falle es que se procederá a la **revisión manual** de la información del usuario, llevada a cabo por el analista de Cumplimiento, quien estará encargado de verificar el motivo por el cual no pudo completarse automáticamente la verificación del usuario. En el evento de que el reparo a la verificación automática sea subsanable, el analista de Cumplimiento enviará una **solicitud de actualización de información** al usuario, explicando el motivo de su reparo en la verificación y cómo solucionarlo; si, por el contrario, el reparo en la verificación automática no es subsanable, el analista de Cumplimiento procederá a rechazar la solicitud de verificación del usuario, no completándose su registro en la plataforma.

Así las cosas, se puede apreciar que existen tres distintos estados en el proceso de revisión de la solicitud de verificación: i) **verificado,** en todos aquellos casos en que el usuario cumplió exitosamente con el proceso de reconocimiento biométrico, se pudieron extraer y comprobar sus datos personales, y no hubo coincidencias en listas AML o PEP; ii) **pendiente**, en todos aquellos casos en que no se pudo comprobar en su totalidad alguno de los elementos accesorios del proceso de identificación, en cuyo caso habrá de resolverse manualmente; o, iii) **rechazado,** en todos los casos en que el usuario no cumplió con éxito el reconocimiento facial, o la extracción de sus datos personales, o hubo coincidencias en las listas AML o PEP.

**No aprobación en la verificación del usuario.**

La Empresa está facultada para rechazar o no aceptarla solicitud de verificación de usuarios que no cumplan con los requisitos mínimos de identificación establecidos en el presente Manual, tales como: que no entreguen la información completa solicitada, que tengan

vinculaciones en listas terroristas del Consejo Seguridad ONU, que estén registrados como bloqueados en listas internas, entre otras; esta política no admite excepción y constituyen señales de alerta para dar cuenta de un reporte de operación sospechosa, y para limitar transacciones, bloquear y eliminar cuentas.

Además, se rechazará o dará de baja todo registro, usuario, cliente, persona natural o jurídica, y sus destinatarios, que de alguna forma estén vinculados con industrias restringidas por la empresa. La restricción que existe para el uso de la plataforma propiamente tal, se conocerá de ella en el proceso de registro, de actualización de información y de monitoreo de transacciones y destinatarios, y dice relación con las siguientes industrias:

- Servicios y entretenimiento para adultos, tales como fotos, videos, imágenes, actividades, comercio y servicio en general relacionados con la industria de la pornografía y/o el erotismo.
- Servicios de bares y clubes nocturnos.
- Servicios de subastas.
- Operadores de cajeros automáticos.
- Servicios de gestión de insolvencia y quiebras.
- Servicios de venta controlada de drogas y fármacos.
- Servicios de pagos ordenados judicialmente.
- Servicios de bloqueo cibernético.
- Servicios de cobro de deudas.
- Servicios de apuestas.
- Servicios asociados a cualquier tipo de actividad ilegal.
- Servicios asociados a la infracción de propiedad intelectual.
- Servicios asociados a la compraventa de joyería, artículos de lujo, minerales, piedras preciosas, metales y gemas.
- Servicios asociados a la compraventa de marihuana, en cualquiera de sus formatos, derivados e industrias relacionadas.
- Servicios asociados al marketing multinivel (piramidales).
- Servicios de prestamistas.
- Servicios de ransomware en todas sus formas.
- Bancos o instituciones financieras que no mantienen presencia física en su lugar de asiento informado (shell banks).
- Negocios de servicios monetarios sin licencia.
- Servicios asociados a la compraventa de armas.
- Servicios de sistemas de pagos a plazo.
- Servicios de compraventa de medicamentos.
- Servicios de compraventa de información personal.
- Servicios asociados a la facilitación de herramientas para hacking de todo tipo de instrumentos electrónicos.
- Servicios que promuevan el odio, violencia o intolerancia racial.
- Servicios psíquicos.

**Eliminación de las cuentas de los usuarios.**

Actualmente pueden generarse dos hipótesis para la eliminación de las cuentas de usuarios en Vita: ya por expresa solicitud del usuario, ya por decisión del área de Cumplimiento y Legales en atención al comportamiento del usuario.

En el primer caso, es el usuario quien toma contacto mediante el canal de Soporte solicitando la eliminación de su cuenta. Su caso será tomado por alguno de los operadores de Soporte, quien le solicitará información precisa relativa al motivo de la solicitud, ofreciendo soluciones a los posibles problemas que el usuario presente como motivo de su solicitud de eliminación de cuenta. De ser definitiva la solicitud de eliminación de cuenta por parte del usuario, el operador de Soporte notificará al área de Cumplimiento, desde donde se realizarán las gestiones conducentes al análisis del caso y eventual eliminación de la cuenta del usuario.

En el segundo caso, será el equipo de Cumplimiento quien tomará contacto con el usuario para indicarle que se encuentra en alguna hipótesis de vulneración de términos y condiciones u otra política de la plataforma, por ejemplo, que el usuario mantenga dos o más cuentas a su nombre; en este caso en particular, se le recordará al usuario que las cuentas en Vita Wallet son únicas de cada usuario, y se le solicitará indicar la cuenta que mantendrá, para pasar a la eliminación de la cuenta que quedará en desuso.

La eliminación de las cuentas de los usuarios se verán reflejadas con el bloqueo o restricción de la cuenta requerida de eliminación, a la cual ni el usuario ni VITA SOLUTIONS SpA tendrán acceso hacia el futuro, manteniéndose a la vista únicamente la información del usuario requerida para la creación de su cuenta. La circular UAF N° 49/2012 establece respecto ‘’De la Obligación de Crear y Mantener Registros’’ que la ‘’Toda información contenida en los registros señalados precedentemente deberá ser conservada y mantenida por los Sujetos Obligados por un plazo mínimo de 5 años (...)’’, obligación con la cual VITA SOLUTIONS SpA cumple a cabalidad, manteniendo dichos registros por un plazo máximo de 7 años.

## 1.2. DDC REFORZADA

En virtud del Título III número 5, de la Circular N° 49 del año 2012, modificada por la Circular N° 59 del año 2019, Vita ha determinado requisitos objetivos y subjetivos asociados, por un lado a las transacciones realizadas por los usuarios y, por otro, al comportamiento y estatus de los usuarios, los cuales al verificarse generarán el protocolo de DDC Reforzada, y que permite a la Empresa lo siguiente:

a) Obtención de información sobre el carácter que se pretende dar a la relación legal o contractual.
b) Obtención de información sobre el origen de los fondos del cliente.
c) Obtención de información sobre el origen del patrimonio del cliente.

d) Obtención de información sobre el propósito del acto, operación y/o transacción que se pretende efectuar o efectuada.
e) Obtención de la aprobación de la alta gerencia para comenzar o continuar la relación legal o contractual.
f) Intensificar la DDC Continua del cliente.
g) Obtención de información adicional del cliente y actualización con mayor frecuencia de la información y documentos de identificación del cliente y beneficiario final.

Vita mantiene procesos de Debida Diligencia Reforzada tanto respecto de los usuarios registrados en la plataforma como respecto de los destinatarios de las transacciones realizadas en la plataforma por sus usuarios. Así, toda vez que se requiera información adicional referente a la operación y motivos de las transacciones de los usuarios de Vita, se les solicitará determinada información y, asimismo, cuando se requiera información respecto de los destinatarios de las transacciones de los usuarios, también se requerirá información adicional.

El procedimiento que se realiza para llevar a cabo al DDC Reforzada respecto de los usuarios de la plataforma de Vita es el siguiente: se envía una comunicación formal vía correo electrónico al usuario, enviada desde la casilla de correo cumplimiento@vitawallet.io -de titularidad del área de Cumplimiento y Legales-, mediante la cual se le solicita al usuario, previamente verificado en la plataforma (y, por tanto, respecto del cual se tiene una ficha con la información de su DDC estándar) que proporcione la siguiente información:

a) Formulario de origen de fondos: https://form.typeform.com/to/CZ1ZBCNY; en este formulario el usuario deberá completar parte de su información personal y deberá aportar información específica sobre el origen de sus fondos y la actividad que realiza, adicionalmente, también se le consultará por el monto que deseará transaccionar mensualmente.
b) Comprobante de dirección (por ejemplo, boleta de pago de servicios básicos, contrato de arrendamiento, etc).
c) Comprobante de ingresos o actividad que realizas (por ejemplo, contrato de trabajo, boleta de honorarios, etc).

De esta manera, el equipo de Cumplimiento y Legales podrá realizar un análisis completo de la operación de los usuarios teniendo a la vista la información remitida respecto del origen de los fondos, principalmente. Esto es de vital importancia porque el tener claridad sobre el origen de los fondos de los usuarios y tener comprobantes que avalen que la información aportada por los usuarios es fidedigna le permitirá al área encargada una comprensión integral del uso que los usuarios realizan de la plataforma y así, poder evitar que dicho uso esté asociado a hipótesis de LA/FT.

Esta solicitud de información de Debida Diligencia Reforzada para los usuarios vía correo electrónico se aplicará en los casos en que el comportamiento de los mismos sea indiciario de operaciones sospechosas y/o inusuales, asociadas a las señales de alerta propias de la Empresa; adicionalmente, se solicitará información de Debida DIligencia Reforzada, pero desde la misma plataforma, toda vez que los usuarios quieran superar el umbral de 5.000 USD mensuales en un mismo mes. En esta última hipótesis, el usuario realizará la solicitud de aumento de cupo desde la plataforma, indicando la actividad a la cual se dedica y por la

cual percibe ingresos mensuales y acompañando comprobantes de la misma y de su domicilio vigente. Esta información será revisada por el analista de Cumplimiento, quien procederá a aprobar o no el aumento de cupo solicitado.

Por otro lado, el procedimiento que se realiza para llevar a cabo la DDC Reforzada respecto de los destinatarios de los transacciones de los usuarios de la plataforma de Vita se compone de lo siguiente: se envía una comunicación formal vía correo electrónico al usuario, enviada desde la casilla de correo cumplimiento@vitawallet.io -de titularidad del área de Cumplimiento y Legales-, mediante la cual se le solicita al usuario, previamente verificado en la plataforma (y, por tanto, respecto del cual se tiene una ficha con la información de su DDC estándar) que proporcione la siguiente información:

a) Motivo de la transacción y su correspondiente comprobante.
b) Fotografías del documento de identidad del destinatario de la transacción (a fin de verificar que el destinatario de las transacciones no se encuentre en alguna lista restrictiva, sea PEP o mantenga antecedentes penales de relevancia para la operación).
c) Comprobante de domicilio del destinatario de la transacción.
d) Indicación del origen de los fondos utilizados para realizar la transacción, con su correspondiente comprobante (si es que con anterioridad no se tiene registro de dicha información).

El contar con esta información le permitirá al área encargada realizar un análisis exhaustivo no solo del comportamiento del usuario, sino que también del motivo de las transacciones y las personas con las que los usuarios se relacionan.

## 1.3. DDC SIMPLIFICADA

Toda vez que las operaciones de los usuarios no superen el umbral objetivo de los USD 5.000, ni se traten de PEP ni de clientes realizando operaciones inusuales o sospechosas, la Empresa tomará como medidas de debida diligencia simplificada las siguientes: la posibilidad de completar datos DDC mediante terceras fuentes; reducción de la frecuencia de actualización de los datos; actualización de los datos DDC por terceras fuentes; reducción de la intensidad DDC Continua; exención de solicitud de antecedentes sobre el propósito de la relación.

## 1.4. INFORMACIÓN PRECISA Y SIGNIFICATIVA EN LAS TRANSFERENCIAS ELECTRÓNICAS DE FONDOS (TEF)

Vita Wallet, en tanto empresa de transferencias internacionales de fondos, se encuentra en cabal cumplimiento de lo establecido en el Título V de la Circular N° 49 del año 2012, modificada por la Circular N° 59 del año 2019, en cuanto se exige registrar la siguiente información:

- Monto, moneda y fecha de la transferencia.

- País o comuna de destino de los fondos.
- Nombre o razón social del ordenante.
- Número de cédula de identidad del ordenante, para chilenos y residentes, o de pasaporte o similar documento de identificación para extranjeros no residentes. En caso de personas jurídicas se deberá solicitar el RUT o similar si es extranjera.
- Número de cuenta del ordenante e institución, o en su defecto, de aquella usada de referencia para la operación.
- Domicilio del ordenante.
- Forma de pago por parte del ordenante (transferencia electrónica, efectivo, documentos u otro).
- Nombre o razón social del beneficiario.
- Documento de identidad del beneficiario o pasaporte cuando se trate de personas naturales. En el caso de personas jurídicas se deberá solicitar el RUT o similar si es extranjera, y prueba de su constitución, forma y estatus jurídico.
- País de origen de los fondos, o comuna si son transferencias nacionales.
- Estado de la transferencia (liquidada, anulada, rechazada o pendiente de liquidación).

A este respecto, Vita en razón de su alto compromiso con el mejor conocimiento de sus clientes, antes de siquiera realizar el servicio de transferencia electrónica, ya posee entre sus registros la mayoría de la información aquí requerida por la norma, a saber, toda la relativa al ordenante.

Con todo, la información requerida se genera automáticamente a través del formulario de transferencia que todo usuario debe registrar antes de utilizar este servicio, en el cual se le solicita: i) el país de dónde se realiza la transferencia; ii) la ciudad de la cual se realiza la transferencia; iii) la dirección exacta del ordenante; iv) la moneda en la cual realizará la transferencia electrónica; v) correo electrónico; vi) el tipo de documento de identidad y su número; vii) el nombre del banco del ordenante; viii) el tipo de cuenta del ordenante; ix) el número de cuenta de la misma; x) el estado civil, xi) ocupación, xii) teléfono del ordenante; xiii) declaración de origen de fondos; y, xiv) declaración PEP. Mientras que del beneficiario se solicita la siguiente información: i) nombre; ii) país; iii) correo electrónico; iv) número de cédula de identidad o pasaporte; v) nombre del banco; vi) tipo de cuenta bancaria; vii) número de la cuenta bancaria; viii) domicilio del destinatario; ix) monto total de la operación; x) fecha de la transferencia; xi) estado de la misma.

## 2. LISTADO DE CLIENTES EN RELACIÓN A LAS RESOLUCIONES DEL CONSEJO DE SEGURIDAD DE LAS NACIONES UNIDAS

Con el objeto de dar cumplimiento a los preceptuado por el Título VIII de la Circular N° 49 del año 2012, modificado por las Circulares N° 54 del 2015 y N° 60 del año 2019, que refieren a las Resoluciones dictadas por el Consejo de Seguridad de Naciones Unidas, en materia de prevención del financiamiento del terrorismo y del financiamiento de la

proliferación de armas de destrucción masivas, la Empresa ha dispuesto la utilización de dos softwares para evitar la relación de la empresa con estas actividades.

El primero es ‘’Neitcom’’, que es una herramienta que actúa como soporte y apoyo a la actividad del área de Cumplimiento y Legales el que, por medio de un sistema automatizado, permite verificar que los usuarios no sean parte ni se relacionen de alguna manera con los nombres y grupos establecidos en las resoluciones ONU respectivas.

El listado contempla las resoluciones relacionadas a Al-Qaida, EIIL (Daesh), República Islámica de Irán y la República Popular Democrática de Corea, según resoluciones consolidadas publicadas por la UAF. Además, el software identifica a través de fuentes de instituciones, organismos, policías y fiscalías, tanto nacionales como internacionales, a distintos usuarios provenientes de una investigación relacionada a fondos ilícitos, personas notificadas por un organismo de investigación, personas notificadas por un organismo supervisor de actividades ilícitas, personas de dudosa reputación que hayan sido reportadas por otros usuarios, o que se encuentren en bases públicas, usuarios de países y territorios no cooperantes FATF, personas que estén registradas en listas de OFAC (por sus siglas en inglés de Oficina de Control de Activos Extranjeros) y la ONU (Organización de las Naciones Unidas), PEP, Resoluciones actualizadas del Consejo de Seguridad de la ONU, paraísos fiscales OCDE, Interpol, PLC, FSE, SSI, PMLC, CFSP, DEA, Poder Judicial de diversos países, Banco Mundial, BID, entre otros.

Lo propio realiza el software de ‘’Truora’’, que es la segunda herramienta utilizada para verificar el estatus de los usuarios de Vita, la cual permite obtener información detallada respecto de los antecedentes penales de los usuarios, que es de mucha utilidad a la hora de realizar análisis.

La plataforma de Vita, en el proceso de registro y verificación, y en el proceso de actualización anual de información se encarga de revisar a cada nuevo usuario registrado en Vita contra la base de datos automatizada de Neitcom y Truora vía API, y se registra el resultado en la ficha respectiva del cliente, quedando una constancia de la fecha de revisión y de los resultados obtenidos en la plataforma del software y en el sistema de administración de Vita. De generarse una eventual coincidencia entre un cliente y los listados, el proceso de verificación de la cuenta, o de actualización de información en su caso, quedará suspendido hasta que se realice una verificación manual del usuario, y éste no podrá operar en la plataforma siendo restringido hasta obtener el visto bueno del área de Cumplimiento y Legales. En caso de ser rechazado, se levantará un Reporte a la Unidad de Análisis Financiero con todos los antecedentes respectivos.

Algo similar sucede respecto de los destinatarios de las transacciones puesto que ellos también son revisados por los softwares antes comentados, con la finalidad de determinar que el dinero que los usuarios de la plataforma no sea dirigido a personas que pudiesen estar relacionadas con hipótesis delictuales asociadas al lavado de activos y financiamiento del terrorismo.

La Empresa mantiene el férreo compromiso con sus usuarios de encontrarse en constante mejora del servicio, y en atención a lo anterior es que se procede la revisión periódica de antecedentes tanto de usuarios ya verificados así como también de los destinatarios de las

transacciones; esta revisión se lleva a cabo con las herramientas Neitcom y Truora, para corroborar que ninguno de ellos tenga coincidencias de antecedentes con posterioridad a su incorporación a la plataforma. Esta revisión, que es adicional a la del proceso de verificación y al de actualización anual de información, se realiza trimestralmente también de forma automatizada al igual que las hipótesis anteriores.

## 3. LISTADO DE CLIENTES EN RELACIÓN A LAS PERSONAS EXPUESTAS POLÍTICAMENTE (PEP)

En línea con lo determinado en el Título IV de la Circular N° 49 del año 2012, y las Recomendaciones para la Identificación y Procedimientos relacionados con Personas Expuestas Políticamente del año 2013, es que Vita ha implementado un sistema automatizado vía software que le permite identificar si un usuario del servicio, o beneficiario del mismo, es o no un PEP.

Tanto el software “Neitcom” como el software de ‘’Truora’’ -ambos de apoyo a la labor de Compliance- permiten contrastar el nombre de cada uno de los usuarios y de los destinatarios de las transacciones con diversas bases de datos, revisando tanto a fuente nacional en la información del Gobierno de Chile y del Registro Civil y de Identificación, y además con fuente internacional de PEP en 196 países a través de información de la Central de Inteligencia de Estados Unidos.

Se ha dispuesto una comunicación desde el correo electrónico de cumplimiento@vitawallet.io hacia la Gerencia de la Empresa, con el objeto de obtener el visto bueno para las operaciones donde figure un PEP y así tener la aprobación para el establecimiento o continuación de la relación del servicio con ese cliente. Por otro lado, se ha dispuesto como requisito que verifica la ejecución de la Debida Diligencia Reforzada todas aquellas transacciones en las que participe una Persona Expuesta Políticamente, de modo que podremos recabar de éstas la mayor información que se permite respecto de la fuente de sus fondos, el origen y destino de sus transferencias, personas y bancos asociados.

# IV. DETECCIÓN Y REPORTE DE OPERACIONES SOSPECHOSAS (ROS)

## 1. DETECCIÓN DE OPERACIONES SOSPECHOSAS EN LOS USUARIOS

Este proceso de detección consta de dos momentos: el primero, automatizado a través de alertas configuradas en el sistema interno de administración de la plataforma; y, el segundo, que es realizado por analistas expertos en materia de cumplimiento de normativa del sector.

1.1. Proceso automatizado. Se compone de las alertas automatizadas que se encuentran configuradas en la plataforma de Vita y son las siguientes:

1.1.1. Revisión de IP de los usuarios, mediante una herramienta de georeferenciación conectada vía API, la cual permite conocer el lugar desde el cual el usuario ha estado haciendo uso de la plataforma. Este lugar debe provenir de jurisdicciones permitidas en la plataforma de Vita Wallet, y no debe variar considerablemente durante los inicios de sesión.

1.1.2. Revisión de los montos asociados a las transacciones que los usuarios han realizado dentro de un mes. Tienen asociados límites transaccionales.

1.1.3. Revisión de los montos asociados a las transacciones recibidas por los destinatarios de los usuarios dentro de un mes. Tienen asociados límites transaccionales.

1.1.4. Revisión de comportamientos transaccionales basados en conductas parametrizadas, tales como: i) un mismo usuario, dentro de un mismo mes, realiza más de dos transacciones a un mismo beneficiario final; ii) dos o más usuarios hacen envíos internacionales hacia un mismo beneficiario final; iii) un usuario recibe envíos internos de dos o más Vita usuarios distintos; iv) un usuario recibe envíos internos de uno o más Vita usuarios distintos y luego intercambia cripto; v) cliente usa el mismo correo electrónico de destinatario para beneficiarios finales diferentes.

1.2. Proceso manual/ de analistas. Una vez realizada la revisión automatizada de los puntos antes descritos, y habiéndo generado alguna de las alertas en las operaciones, la transacción quedará en estado de bloqueo y se procederá a la revisión especializada del analista de cumplimiento.

El operador que haya detectado la irregularidad en alguna operación, teniendo como base las señales de alerta internas, procederá a bloquear dicha transacción en la plataforma y dar noticia de ello al analista de Cumplimiento, indicando ID interno de la transacción y motivo del bloqueo.

Luego, el analista de Cumplimiento tomará dicho reporte y procederá a analizarlo con suma detención, evaluando características asociadas al comportamiento de los usuarios, siendo algunas de las más relevantes: i) los fondos que maneja el usuario; ii) la frecuencia en que usa los servicios; iii) el perfil financiero declarado por éste; iv) que la operación realizada se corresponda con su profesión o actividad declarada; v) señales de alerta; vi) revisión de ficha de perfil de destinatarios. Durante este proceso de evaluación, la transacción se mantiene en estado de bloqueo, esto es, no puede ser procesada por la plataforma.

En el proceso de evaluación realizado por el analista de Cumplimiento, este podrá i) requerir de información adicional al usuario que está realizando la transacción, si la operación reportada así lo amerita o ii) evidenciar que no hay un riesgo asociado a la operación y solicitará el **desbloqueo y procesamiento de la transacción,** permitiendo que esta siga su curso normal.

En la primera hipótesis, el analista de Cumplimiento requerirá de información adicional al usuario, pudiendo darse los siguientes casos: i) el usuario responderá el correo enviando la información completa y suficiente, lo que le permitirá al analista de Cumplimiento tomar la decisión de ordenar el desbloqueo y procesamiento de la transacción; ii) el usuario no responderá la comunicación del área de Cumplimiento y Legales; pasados 3 días hábiles sin respuesta, **la transacción será rechazada** y el saldo devuelto a la billetera del usuario; iii) el usuario responderá enviando información incompleta y/o insuficiente, caso en el cual la transacción será rechazada y, eventualmente, la cuenta del usuario restringida hasta que pueda enviar la información que fue requerida. El rechazo de la operación podría dar lugar al procedimiento de Reporte de Operaciones Sospechosas ante la UAF.

# 2. SEÑALES DE ALERTA

La Unidad de Análisis Financiero define a las señales de alerta como ‘’aquellos indicadores, indicaciones, condiciones, comportamientos o características de ciertas operaciones o personas que podrían permitir potencialmente conducir a detectar una operación sospechosa de lavado de activos o de financiamiento del terrorismo.’’

Para efectos de este Manual, no solamente se tendrá a la vista la detección de operaciones sospechosas relacionadas a los delitos de lavado de activos y/o financiamiento del terrorismo, sino que a todos los delitos precedentes asociados a ellos, así como también a los demás delitos relevantes para la operación de la Empresa que se encuentren enunciados en los demás cuerpos legales ya mencionados.

El contar con señales de alerta le permite a la Empresa y a sus empleados estar preparados y, valga la redundancia, alertas a la eventual comisión de delitos que pueda generarse dentro de la operación, contando con una guía robusta para poder tomar decisiones al encontrarse frente a operaciones que puedan ser sospechosas. Las señales de alertas pueden dividirse en los siguientes grupos:

2.1. Señales de alerta generales:
- 2.1.1. Relacionadas con el comportamiento del cliente.
- 2.1.2. Relacionadas con el comportamiento de los empleados.
- 2.1.3. Relacionadas con situaciones en las que participan funcionarios de la Administración Pública.
- 2.1.4. Relacionadas con licitaciones y compras públicas.
- 2.1.5. Relacionadas con Personas Expuestas Políticamente, nacionales o extranjeras.
- 2.1.6. Relacionadas con cohecho a funcionario público extranjero
- 2.1.7. Relacionadas con clientes personas y estructuras jurídicas.

2.2. Señales de alerta relacionadas con las transferencias electrónicas y giros de fondos:

2.2.1. Cliente que realiza transferencias electrónicas nacionales o internacionales y paga con distintos instrumentos procedentes de diversas instituciones financieras.

2.2.2. Cliente que gira fondos en efectivo desde cuenta de ahorro extranjera para envío de fondos a Chile, sin justificación para las operaciones realizadas.

2.2.3. Cliente que, sin justificación aparente, comienza a recibir transferencias desde el exterior por montos elevados o con alta periodicidad.

2.2.4. Cliente que con frecuencia envía o recibe transferencias de dinero o desde países considerados no cooperantes por el GAFI, o territorios catalogados por la OCDE como regímenes fiscales o preferencialmente nocivos (paraísos fiscales), sin contar con una justificación económica aparente.

2.2.5. Recepción o remisión reiterada de fondos desde o hacia países con altos niveles de producción y/o tráfico ilícito de estupefacientes, no logrando justificar el origen de los fondos.

2.2.6. Montos enviados al extranjero no se condicen con la capacidad económica del cliente y/o en cortos períodos.

2.2.7. Cliente envía giros a múltiples beneficiarios dentro del mes, sin tener relación aparente con ellos.

2.2.8. Se solicitan antecedentes de operaciones del cliente por parte de instituciones policiales en el marco investigativo por causas judiciales.

2.2.9. Transferencias solicitadas por un cliente y remitidas a sí mismo en otra sucursal o agencia.

2.2.10. Cliente que se presenta en la sucursal a remitir o recibir una transferencia de dinero, siendo acompañado de una tercera persona, quien le entrega indicaciones respecto de lo que debe hacer.

2.2.11. Transferencias remitidas a diferentes países, con un mismo beneficiario y en un corto período

2.2.12. Envío (transferencia)/ recepción de fondos de distintos remitentes, respecto de los cuales se detectan datos en común (dirección, teléfono, entre otros),

2.2.13. Transferencias realizadas por montos exactamente bajo el umbral de registro, o utilizando varios cheques bancarios viajeros.

2.2.14. Recepción de transferencias por altos montos, remitidas por empresas procesadoras de pagos en línea (PayPal, Money Bookers, etc.), las cuales no aportan información acerca del remitente.

2.3. Señales de alerta específicas para Vita.

2.3.1. Usuario que realiza transacciones por montos que no se condicen con su capacidad económica.

2.3.2. Cambio repentino del comportamiento habitual financiero del usuario.

2.3.3. Usuario que se rehúsa a entregar información que le haya sido requerida en el marco de la aplicación de políticas de Debida Diligencia y Conocimiento del Cliente.

2.3.4. Usuario que entrega información falsa y/o adulterada al ser requerido de documentación.

2.3.5. Usuario que oculta información relativa al origen de sus fondos, motivo y destino de sus transacciones.

2.3.6. Usuario que procura realizar transacciones con extrema urgencia en intento de evadir los controles que le hayan sido aplicados.

2.3.7. Usuario que comienza a recibir transacciones desde el extranjero por altos montos y en forma periódica.

2.3.8. Usuario que entrega información inconsistente y/o falsa respecto de su actividad económica.

2.3.9. Usuario cuyas sociedades presenten ingresos que no se ajusten al promedio de la industria correspondiente, ni con la actividad económica declarada.

2.3.10. Usuario que envía/recibe transferencias de países catalogados como no cooperantes, que se encuentran en listas restrictivas y/o que son catalogados como con altos niveles de corrupción.

2.3.11. Usuario PEP que realiza operaciones por montos que no se condicen con sus ingresos.

2.3.12. Que se tome conocimiento por medios de difusión pública u otras fuentes que un determinado usuario está siendo investigado o procesado por delitos relevantes para la operación de la Empresa.

2.3.13. Usuario que habitualmente realiza transacciones a sí mismo en distintas cuentas o países.

2.3.14. Usuario que realiza transferencias con intermediarios con la finalidad de ocultar una identidad de PEP.

2.3.15. Usuario PEP que aporta información inconsistente con la información pública y actualizada que se mantiene a su respecto.

2.3.16. Usuario de la plataforma que solicite información sobre una operación y/o proceso de registro respecto de una tercera persona.

2.3.17. Destinatario de transacciones que recibe más de 8.000 USD en un mes, sin que se tenga información adicional a su respecto.

2.3.18. Dos o más usuarios realizando envíos a un mismo destinatario.

2.3.19. Dos o más usuarios realizando envíos a un mismo destinatario.Usuario que exige el procesamiento de transacciones bloqueadas por falta de envío de información, sin enviar la información/documentación requerida.

2.3.20. Usuario nacido en 1970 o años anteriores que realiza transacciones de criptomonedas, sin que se tenga información adicional a su respecto.

2.3.21. Cambio repentino y sin justificación aparente en la geolocalización asociada al inicio de sesión de un usuario.

2.3.22. Usuario registrado en residencia en Colombia que reporta recibir recargas de terceros en su cuenta Vita

2.3.23. Usuario registrado con residencia en Colombia que recarga su cuenta Vita y la operación inmediatamente posterior es el retiro del saldo recargado.

2.3.24. Usuario realizando envío de criptomonedas hacia una billetera catalogada con riesgo alto o severo.
2.3.25. Usuario realizando envío de criptomonedas hacia una billetera respecto de la cual no se tenga conocimiento de su titularidad.
2.3.26. Colaboradores y/o terceros relacionados que incurran en conductas asociadas a los delitos establecidos en la Ley 19.913.

# 3. DE LAS OPERACIONES CON ACTIVOS DIGITALES

Toda vez que un Vita Usuario desea realizar un retiro de criptoactivos, la plataforma realiza una llamada vía API a la herramienta “TRM” que permite realizar un análisis de riesgo de las transacciones en la blockchain, siendo un apoyo a la actividad de Cumplimiento y Legales, permitiendo realizar una investigación respecto del riesgo de las wallets de destino de los usuarios, dentro del proceso de debida diligencia reforzada.

La revisión en ‘’TRM’’ de las wallets de destino a las que los usuarios realizan envíos de criptomonedas -y también respecto de la wallets desde las que estos reciben criptomonedas- forma parte del análisis transaccional realizado por el área de Cumplimiento y Legales, el cual será realizado teniendo a la vista el tipo de riesgo asociado a la wallet de destino, el nivel de dicho riesgo y la posibilidad de acceder a variada información sobre las billeteras de destino de los usuarios, y todo lo anterior permitirá al área encargada realizar un análisis completo de la situación asociada a determinada transacción.

Ahora bien, lo mencionado recientemente dice relación con un proceso de revisión *automatizado* de parte de las transacciones, el que es complementado con un proceso de *revisión manual,* realizado por los operadores de Cumplimiento, quienes derivarán el caso al analista de Cumplimiento si es que dicho caso tiene una complejidad mayor.

Frente a estos casos de mayor complejidad, se tomará un curso de acción idéntico al tomado en los casos de transacciones en moneda FIAT, esto es, el operador notificará al analista de Cumplimiento, quien realizará la correspondiente evaluación del caso, la transacción y el comportamiento del usuario, pudiendo solicitar información adicional para analizar correctamente la transacción antes de que esta sea procesada o, en su defecto, rechazada; todo esto mientras la transacción se mantiene en estado de bloqueada en la plataforma.

# 4. REPORTE DE OPERACIONES SOSPECHOSAS (ROS)

El funcionario responsable, una vez concluido el procedimiento de detección anteriormente descrito, y habiendo dado cuenta de la inexistencia de una justificación económica o jurídica aparente para tal acto, comunicará la operación sospechosa dentro del mismo día en que se determinó el rechazo de la operación a la UAF, de manera confidencial, y a través de un reporte de operación sospechosa (ROS).

Esta declaración será enviada en línea a través de la página web institucional de la UAF (https://www.uaf.cl/), en el portal que al efecto se ha determinado, en la cual se registrarán todas aquellas operaciones que hayan sido reportadas como sospechosas, junto a los antecedentes totales y completos del usuario y de todas sus transacciones realizadas a través de la plataforma de Vita Wallet.

# 5. DEBER DE CONFIDENCIALIDAD DEL PERSONAL

Bajo ningún concepto el personal que haya comunicado una operación sospechosa o tenga conocimiento sobre un usuario vinculado a actividades ilícitas LA/FT, podrá revelar ni a los usuarios ni a terceros ningún tipo de información relacionada con el hecho denunciado o del que tenga conocimiento. Así lo establece el artículo 6° de la Ley 19.913, que *prohíbe expresamente a las personas e instituciones señaladas en el artículo 3° del mismo cuerpo legal en sus incisos primero y sexto, y a sus empleados, informar al afectado o a terceras personas la circunstancia de haberse requerido o remitido información a la UAF, como asimismo, proporcionarles cualquier otro antecedente al respecto.*

Para los efectos de resguardar la confidencialidad, el flujo de información en la detección de operaciones sospechosas se basa en la comunicación exclusiva entre el funcionario que la detectó y el Oficial de Cumplimiento que llevará adelante la investigación y el eventual reporte. La infracción a esta prohibición es constitutiva de delito de acción penal pública, pudiendo ser sancionada con pena de presidio menor en sus grados medio o máximo, y multa en UTM.

# 6. CHEQUEO PERMANENTE Y CONTINUO DE LAS OPERACIONES DE LOS USUARIOS

Como parte de la actividad propia del giro de la Empresa, esta cuenta con un sistema de análisis transaccional periódico y constante, al cual se ha hecho mención a lo largo de este Manual.

A su respecto existen reglas y protocolos que se aplican frente a las operaciones realizadas por los clientes, tanto del segmento B2B como del segmento B2C, como también respecto del comportamiento operacional de los usuarios.

Así las cosas, contamos con protocolos de análisis transaccional para operaciones FIAT como operaciones CRIPTO, que se detallan a continuación:

**Protocolo de Análisis Transaccional FIAT:**

Dentro de la plataforma se accede a una pestaña llamada ‘’retiros’’, en donde pueden encontrarse todas las transacciones internacionales pendientes de realización. Algunas de estas transacciones podrán procesarse y llegar a destino de forma **automática** -gracias a un sistema de pagos automáticos con el cual cuenta la Empresa- y otras serán objeto de una **revisión manual** por parte de los operadores que revisan las transacciones con reparos.

Los operadores de Cumplimiento pasarán a la revisión de estas transacciones toda vez que respecto de ellas se disparen algunas de las señales de alerta específicas para Vita, las que serán notificadas en el canal de comunicación interno de la Empresa al analista de Cumplimiento, y se mantendrán en un estado de **bloqueadas,** esto es, no podrán procesarse ni rechazarse inmediatamente.

Dentro del análisis que realizará el analista de Cumplimiento puede darse el caso en que no se cuenten con antecedentes suficientes para tomar una decisión respecto al reporte, en cuyo caso el analista de Cumplimiento podrá requerir de información adicional vía correo electrónico al usuario remitente de la transacción en comento. En dicho caso, el analista de Cumplimiento notificará que la transacción objeto de análisis debe permanecer en estado de **bloqueada,** y procederá a solicitar la información adicional que corresponda respecto del caso.

En un acápite anterior se detalló que las solicitudes de información adicionales pueden realizarse respecto del comportamiento e información del usuario que realiza la transacción como respecto del destinatario de las transacciones. En ambos casos, el usuario deberá enviar información completa y suficiente para que el analista de Cumplimiento pueda realizar la correcta evaluación del caso; de no hacerlo, el usuario sujeto a requerimiento podrá ver, como consecuencia de incumplir con las políticas de Debida DIligencia y Conocimiento del Cliente de la Empresa, restringido el uso de su cuenta -mediante la inhabilitación de la misma- hasta que envíe la información requerida, así como también podrá presentar restricciones a la hora de querer realizar envíos a algún destinatario en particular, respecto del cual no envíe la información solicitada.

Una vez que el analista de Cumplimiento contacte al usuario y este responda, tomará todas las medidas posibles para hacer de este proceso lo más expedito y con menos fricción posible, pero siempre manteniendo los estándares de Debida Diligencia enunciados en este Manual.

De la solicitud de información realizada desde el área de Cumplimiento y Legales pueden los siguientes resultados:

- El usuario envía la información solicitada y se descarta el riesgo asociado a la operación. En este caso, el analista de Cumplimiento solicitará el desbloqueo y procesamiento de la transacción, y esta podrá seguir su curso normal.
- El usuario envía la información solicitada, pero de ella se desprende un riesgo ajeno al apetito de riesgo de la Empresa, caso en el cual se le indicará aquello al usuario, se procederá al rechazo de la transacción y su devolución a la billetera del cliente para que este realice el retiro del saldo a la cuenta de origen, y se procederá a la inhabilitación de la cuenta y al correspondiente Reporte de Operación Sospechosa ante la UAF.
- El usuario envía información incompleta/insuficiente, que impide al analista realizar el correcto análisis transaccional, caso en el cual se procederá a indicarle aquello al usuario, y a rechazar la transacción, devolviendo el saldo a la billetera del usuario. **Como se indicó en un acápite anterior esto constituye una señal de alerta.**

- Si luego de 3 días hábiles contados desde el día en que se requirió la información el usuario no se ha contactado, se procederá al rechazo de la transacción y a la devolución del saldo a la billetera del usuario.

Para realizar este proceso, el analista de Cumplimiento no solo tendrá a la vista el comportamiento operacional del usuario y la documentación adicional que de este se disponga, sino que también se apoyará en las herramientas de Neitcom, Truora y Onfido para poder descartar eventuales coincidencias de antecedentes penales relevantes asociados tanto a los usuarios como a los destinatarios de las transacciones, así como también descartar que se trate de Personas Expuestas Políticamente o que se encuentren en alguna de las listas restrictivas internacionales.

**Protocolo de Análisis Transaccional CRIPTO:**

Dentro de la plataforma se accede a una pestaña llamada ‘’retiros crypto’’, en donde pueden encontrarse todas las transacciones de retiros de criptomonedas realizadas por los usuarios, las que pasan por un proceso de revisión antes de ser procesadas.

Dicho proceso se compone de una revisión tanto automatizada como manual, en su caso, en base a criterios preestablecidos asociados a señales de alerta internas, que le permiten a los operadores realizar una rápida revisión para procesar de forma eficiente y segura las transacciones de criptomonedas ordenadas por los usuarios.

Dentro de dicha revisión, no solamente se tendrán a la vista las alertas y protocolos internos creados para estos efectos, sino que también se cuenta con el apoyo de la herramienta ‘’TRM’’, que entrega información robusta y completa sobre las transacciones en criptomonedas. Esta herramienta entrega información relativa a:

- Si determinada wallet es riesgosa.
- Si la wallet es riesgosa, el nivel de riesgo asociado a ella. Desconocido, bajo, medio, alto y severo.
- Si la wallet es riesgosa, el tipo de riesgo asociado a ella. Si la wallet está relacionada con transacciones relacionadas con lavado de activos, financiamiento del terrorismo, exchanges de riesgo, fraudes, etc.
- Si la wallet es riesgosa, el indicador de riesgo asociado a ella. *‘’Indirect”, ‘’Counterparty” y ‘’Ownership”.*

Toda vez que, en revisión transaccional, alguno de los operadores encuentra una señal de alerta respecto de determinada transacción, se procederá al bloqueo de la misma, seguido de la notificación de aquello al analista de Cumplimiento, quien realizará una revisión en profundidad de la alerta y tomará la decisión de, mantener el bloqueo de la transacción y solicitar información adicional para un análisis más detallado o, por el contrario, si el analista de Cumplimiento detecta que la señal de alerta no comporta un riesgo para la operación, solicitará su desbloqueo y procesamiento.

En el caso de darse la primera hipótesis, el analista de Cumplimiento tomará contacto con el usuario vía correo electrónico consultando por el motivo de la operación y, dependiendo del caso, requiriendo de una autorización formal e inequívoca de parte del usuario para el procesamiento de la transacción.

Dependo de la información que el usuario aporte, podrán darse los siguientes cursos de acción:

- El usuario envía la información solicitada -y la correspondiente autorización para el procesamiento de la transacción- y se descarta el riesgo asociado a la operación. En este caso, el analista de Cumplimiento solicitará el desbloqueo y procesamiento de la transacción, y esta podrá seguir su curso normal.
- El usuario envía la información solicitada, pero de ella se desprende un riesgo ajeno al apetito de riesgo de la Empresa, caso en el cual se le indicará aquello al usuario, se procederá al rechazo de la transacción y su devolución a la billetera del cliente para que este realice el retiro del saldo, y se procederá a la inhabilitación de la cuenta y al correspondiente Reporte de Operación Sospechosa ante la UAF.
- El usuario envía información incompleta/insuficiente, que impide al analista realizar el correcto análisis transaccional, caso en el cual se procederá a indicarle aquello al usuario, y a rechazar la transacción, devolviendo el saldo a la billetera del usuario. **Como se indicó en un acápite anterior esto constituye una señal de alerta.**
- El usuario no toma contacto con el equipo de Cumplimiento y, pasados 3 días hábiles desde el día del requerimiento de la información, se procede a rechazar la transacción y el saldo es devuelto a la billetera del usuario.

# V. REPORTE DE OPERACIONES EN EFECTIVO (ROE)

En cumplimiento con lo determinado en el art. 5° de la Ley N° 19.913 y las Circulares de la UAF N° 49 del año 2012 y N° 52 del año 2015, VITA SOLUTIONS SPA, **declara que no realiza operaciones en efectivo**, equivalentes o no al umbral de los USD 10.000.- o su equivalente en pesos chilenos establecidos en la norma, ni por monto alguno inferior a este.

Lo anterior, puesto que el modelo de negocios sobre el que se construye Vita contempla la recarga virtual de una billetera con la cual se realizan las transferencias de dinero, opciones de recarga dentro de las que se encuentran cuentas bancarias y criptomonedas, y no considera efectivo o plataformas intermediarias de efectivo, ni lo hará en un futuro próximo.

Por esto, hacemos envío trimestral del Reporte de Operaciones en Efectivo Negativo (“ROE Negativo”) a la plataforma indicada para tal efecto por la Unidad de Análisis Financiero, y registramos tal circunstancia en cumplimiento de las obligaciones establecidas en la mentada normativa.

# VI. CONTRATACIÓN Y EVALUACIÓN DE TERCEROS RELACIONADOS

Es fundamental la prevención del lavado de activos dentro de VITA SOLUTIONS SPA, respecto de sus colaboradores como de terceros, por eso se requiere de la adopción de medidas suficientes y necesarias de control interno y externo para combatir el delito. Con dicha finalidad, se ha establecido un proceso que permite conocer al aliado comercial a través de una ficha de conocimiento del tercero con el que se quiere contratar algún servicio, esta información deberá ser debidamente completada y firmada por éste, para hacer la revisión de debida diligencia.

Además, como otra medida de debida diligencia, se contempla una declaración a través de las cláusulas incorporadas en los contratos que se celebran con terceros, como con proveedores, alianzas o partnerships, NDA, contratos de trabajo, de prestación de servicios, etc., y que contemplan: i) declaración de conocimiento de este Manual de Prevención de Delitos de LA/FT establecido desde la perspectiva de la Ley N° 19.913; ii) conocimiento del Modelo de Prevención de Delitos establecido desde la perspectiva de la Ley N° 20.393; iii) compromiso de no incurrir en conductas prohibidas por las leyes 19.913 y 20.393; iv) no comprometer la responsabilidad penal de la Empresa; v) obligación de entregar cualquier información que tengan sobre conductas sospechosas; vi) compromiso de entregar toda la información que se requiera en el marco de una alguna investigación interna.

# VII. CONTROL DEL MANUAL DE PREVENCIÓN DE LAVADO DE ACTIVOS Y FINANCIAMIENTO DEL TERRORISMO

La implementación de los procedimientos del manual de prevención de LA/FT en VITA SOLUTIONS SPA, permite mantener la efectividad y eficiencia de la prevención y adaptarnos a los cambios externos e internos. Se establecen como procedimientos de control:

- Revisión anual, o cuando se produzca una modificación legislativa relevante, de la Matriz de Riesgos sobre Lavado de Activos y Financiamiento del Terrorismo por el Comité de Prevención; lo anterior, con la finalidad de acualizar, modificar o eliminar aquellos riesgos identificados relacionados con el Lavado de Activos y el Financiamiento del Terrorismo. El Comité de Prevención informará al funcionario responsable sobre los resultados de esta evaluación.
- La unidad de auditoría interna -independiente del área de Cumplimiento y Legales- en la cual se incorporará en su planificación anual una revisión sobre aquellas áreas, procesos, subprocesos y/o etapas con mayor nivel de criticidad y riesgo de Lavado de Activos y Financiamiento del Terrorismo en el ámbito de la prevención, a objeto de analizar las acciones correctivas que mitiguen los riesgos asociados.

# 1. SANCIONES

Estas son medidas que aplicará la Empresa en los casos en que se incurra en incumplimiento de lo establecido en este Manual o en el caso en que se detectase un indicador de la comisión de delitos, con medidas disciplinarias proporcionales a la falta cometida, en concordancia con lo establecido en los procedimiento disciplinarios establecidos por Vita, esto es:

- Amonestación en forma verbal.
- Amonestación escrita, con copia a la Inspección del Trabajo y a la hoja de vida del trabajador.
- Multa que no podrá exceder una cuarta parte de la remuneración diaria del trabajador.
- Término del contrato de trabajo, cuando incurra además en alguna de las causales del artículo 160 del Código del Trabajo.

# 2. ACTIVIDADES PARA LA PREVENCIÓN DE DELITOS

## 2.1. Actividades de Detección

Estas actividades se refieren a las auditorías realizadas por el Oficial de Cumplimiento, cuyo propósito es realizar controles al Manual, a través de:

- Revisión de litigios.
- Revisión de denuncias.
- Coordinació de la investigación.

Adicionalmente, en la auditoría realizada por el Oficial de Cumplimiento, este tendrá a la vista la revisión de los procesos de monitoreo transaccional, que contempla todas las transacciones realizadas por los segmentos B2B y B2C y que hayan sido previamente revisadas por los operadores de Cumplimiento y por el analista de Cumplimiento.

## 2.2. Actividades de Respuesta

Estas contemplan la revisión de las actividades de control vulneradas a fin de fortalecer o reemplazarlas por nuevas actividades que puedan resultar más eficientes, para ello estas actividades de respuesta están divididas en:

- Evaluación de las denuncias que se pudieren presentar.
- Sanciones disciplinarias.
- Registro y seguimiento de denuncias y sanciones.
- Notificación de sanciones.
- Mejora de las actividades de control del Manual.

## 2.3. Actividades de Supervisión y Monitoreo del Manual

Estas corresponden de manera exclusiva y excluyente al Oficial de Cumplimiento, debido a que su objeto es la verificación del adecuado funcionamiento de las actividades de control definidas, así como, evaluar la necesidad de efectuar mejoras en el Manual.

# 3. PRINCIPALES RESPONSABLES

## 3.1. Oficial de Cumplimiento.

Es el funcionario responsable, designado por el Directorio, encargado de relacionarse con la UAF, de reportar operaciones sospechosas y de coordinar políticas y procedimientos de prevención y detección del lavado de activos y del financiamiento del terrorismo.

## 3.2. Directorio.

Entidad conformada por los altos cargos de la empresa, así como también algunos accionistas/inversionistas, al cual el Encargado de Prevención de Delitos pone en conocimiento de las medidas de prevención de delitos y sus correspondientes actualizaciones de forma anual, las cuales serán revisadas, analizadas y, finalmente, aprobadas o no por este órgano.

## 3.3. Comité de Prevención.

Comité conformado por el Oficial de Cumplimiento, y el Directorio de Vita quienes, en conjunto, realizan revisiones al Manual y a su implementación, proponen modificaciones y/o actualizaciones al mismo, de proceder, y toman decisiones relevantes sobre el curso de acción relativo a la implementación del Manual. El nombre de este Comité también puede ser Comité de Ética y Cumplimiento.

# 4. Funciones del Oficial de Cumplimiento.

La principal función del Oficial de Cumplimiento es la de implementar y controlar permanentemente la efectividad de un programa o modelo de Cumplimiento, sobre la base de políticas y procedimientos diseñados a partir de los riesgos normativos y reputacionales inherentes a la organización en la que ejerce sus funciones.

Adicionalmente, dentro de sus funciones podemos encontrar, entre otras:

1. Implementar las políticas de prevención y detección de LA/FT en la institución y velar por su cumplimiento.
2. Responsabilizarse por el cumplimiento de las obligaciones contenidas en la Ley 19913 y las circulares emitidas por la UAF.
3. Ser el punto de contacto entre su institución y la UAF.
4. Establecer los mecanismos de comunicación internos para recibir las alertas y operaciones sospechosas detectadas por las y los funcionarios.
5. Recibir los reportes internos de operaciones sospechosas de parte de los funcionarios de su institución a través del canal de comunicación establecido,

analizarlos y recabar más antecedentes que le permitan realizar un análisis completo.

6. Reportar a la brevedad posible en un ROS a la UAF, si luego del análisis llevado a cabo considera como sospechosa la operación.
7. Reportar a la UAF a través del ROE, en el período que le corresponda a su entidad de acuerdo a su tipo de institución, todas las operaciones superiores a 10.000 USD en efectivo.
8. Mantener actualizada la información registrada en la UAF respecto de cualquier cambio relevante en la situación legal de la entidad o de la información que haya registrado en el Servicio, lo cual debe realizar dentro de un plazo de 5 días hábiles contados desde la fecha en que se produjo dicho cambio.
9. Entregar a la UAF la información requerida en los procesos de fiscalización que esta desarrolle en su institución.
10. Mantener capacitado al personal de la institución en prevención y detección de LA/FT, cuya periodicidad mínima es anual.
11. Velar por la confidencialidad de la información en toda la organización, cuando esta esté vinculada a los reportes de operaciones sospechosas

# 5. Difusión y capacitación del Manual.

Como se indicó anteriormente, dentro de las funciones del Oficial de Cumplimiento están no solo la de elaborar los lineamientos y protocolos que conforman este Manual, sino que también tiene la obligación de difundirlo entre los colaboradores de Vita, y capacitarlos en las materias relevantes expuestas en él.

Para cumplir con aquello es que Vita cuenta con un programa de capacitaciones, a lo menos semestrales, realizadas por el equipo de Cumplimiento y Legales a todos los trabajadores de Vita, en el formato de una presentación digital y que también se compone de talleres y una breve evaluación luego de cada capacitación.

En las instancias de presentación digital y posterior evaluación, el área de Cumplimiento y Legales se encargará de confeccionar las mentadas presentaciones, las que contendrán distintas materias dependiendo de la época en que se realicen.

Así, se puede apreciar que la primera capacitación anual estará enfocada en las materias basales, debiendo contener, a lo menos, los siguientes temas:

- Definición de delitos relevantes para la empresa, con especial mención a los establecidos en la Ley N° 20.393 (con las respectivas modificaciones realizadas por la Ley N° 21.595) y Ley N° 19.913.
- Aplicación y extensión de dichos delitos dentro del ecosistema de la Empresa.
- Ejemplos y casos prácticos de delitos que son de relevancia para la Empresa.

- Resumen de actualizaciones normativas a nivel nacional en materias relevantes para la Empresa.
- Mención a la actualidad nacional normativa en los países estrechamente relacionados con la operación de la Empresa, como Perú, Argentina, Colombia, México, entre otros.
- Sanciones asociadas a los delitos ya mencionados y sus consecuencias para la Empresa y para sus colaboradores.
- Espacio dedicado a la realización de consultas por parte de los participantes.
- Breve evaluación.

La segunda capacitación anual estará enfocada al detalle de las consecuencias de los delitos en la actividad económica de las empresas como Vita, y, particularmente para Vita, conteniendo, a lo menos, los siguientes tópicos:

- Explicación del Sistema de Prevención de Delitos, haciendo mención a todos los documentos que lo conforman, su composición e importancia.
- Mención a la Cultura de Cumplimiento dentro de la Empresa: qué es, qué la compone, su importancia y aplicación.
- Definición, explicación y otorgamiento de ejemplos asociados a la señales de alerta dentro de la Empresa, tanto las generales, como las aplicables a las empresas de la plaza y, particularmente, las propias a Vita.
- Comentario sobre los procedimientos internos y controles asociados a la prevención de los delitos.
- Espacio para generar preguntas por parte de los asistentes a la capacitación, las que serán respondidas por el Encargado o por algún integrante del equipo de Legales y Cumplimiento.
- Breve evaluación.

# VIII. CÓDIGO DE ÉTICA

Vita posee una guía orientada a las conductas que sus colaboradores deben mantener, dirigida a todo el personal de la empresa, independientemente de la calidad jurídica o jerárquica de este; sin excepción alguna todos deberán observar y practicar lo estipulado en el Código en comento.

En este contexto, el incumplimiento de éste resultará una señal de alerta para la organización, por tal razón deberá informarse al Oficial de Cumplimiento para la aplicación del procedimiento de identificación del colaborador (haciendo control de las operaciones

asignadas y realizadas por este), y en su mérito aplicar las sanciones internas establecidas para tal situación, y eventualmente remitir sus antecedentes a la autoridad respectiva para la investigación y aplicación de las sanciones establecidas en la Ley N° 19.913, de tratarse de una conducta que además de infringir las conductas éticas constituyan dellitos de lavado de activos, financiamiento del terrorismo u otro precedente.

# IX. ACTUALIZACIÓN Y MODIFICACIÓN DEL MANUAL DE PREVENCIÓN

Este manual será revisado periódicamente para eventuales actualizaciones que requiera debido a la naturaleza de los servicios que ofrece VITA SOLUTIONS SPA, y a las diversas modificaciones que pudieren presentarse en la normativa nacional. Para ello se programa un chequeo anual, o previo si se presenta un cambio relevante que así lo requiera, con el fin de adaptar el manual de prevención a nuevas disposiciones y mejores prácticas en relación con la prevención de delitos de LA/FT que pudiesen implementarse.

| | |
|---|---|
| Área | Cumplimiento y Legales |
| Código | MPD19913 |
| Nombre | Manual de Prevención de Delitos de Lavado de Activos y Financiamiento del Terrorismo de la Ley N° 19.913 |

| Versión | Autor | | Fecha Descripción |
|---|---|---|---|
| 1.1 | Directorio[5] | Enero 2021 | Creación y aprobación |
| 1.2 | Directorio - CCO | Octubre 2021 | Modificación y aprobación |
| 2.1 | Directorio - CCO | Octubre 2022 | Modificación y aprobación |
| 2.2 | Directorio - CCO | Marzo 2023 | Modificación y aprobación. KYC de los usuarios persona jurídica, jurisdicciones prohibidas, actualización de industrias prohibidas, actualización de controles de monitoreo de transacciones y blockchain, |

[5] Por “Directorio” se entiende a las personas naturales que ostentan el cargo de Director en Vita Solutions SpA: don Jonder Moisés Zambrano Pérez, Presidente del Directorio; don Sebastián Ignacio Reyes Ronconi; y, don Joel Alfredo Zambrano Pérez, Secretario del Directorio y Gerente General. Los anteriores, reunidos junto al Oficial de Cumplimiento (CCO), don Damián Rubén Azócar Verdejo, constituyen el Comité de Ética y Cumplimiento o Comité de Prevención de la empresa.

| | | | |
|---|---|---|---|
| | | | reporte de operaciones sospechosas. |
| 3.1 | CCO | Septiembre 2024 | Modificación. Actualización de controles de monitoreo de transacciones y blockchain; proveedores de servicios de screening; delitos Ley de Delitos Económicos; programa de auditorías; actividades de detección; sanciones; control; terceros. |
| 3.2. | Directorio - CCO | Noviembre 2024 | Aprobación. |