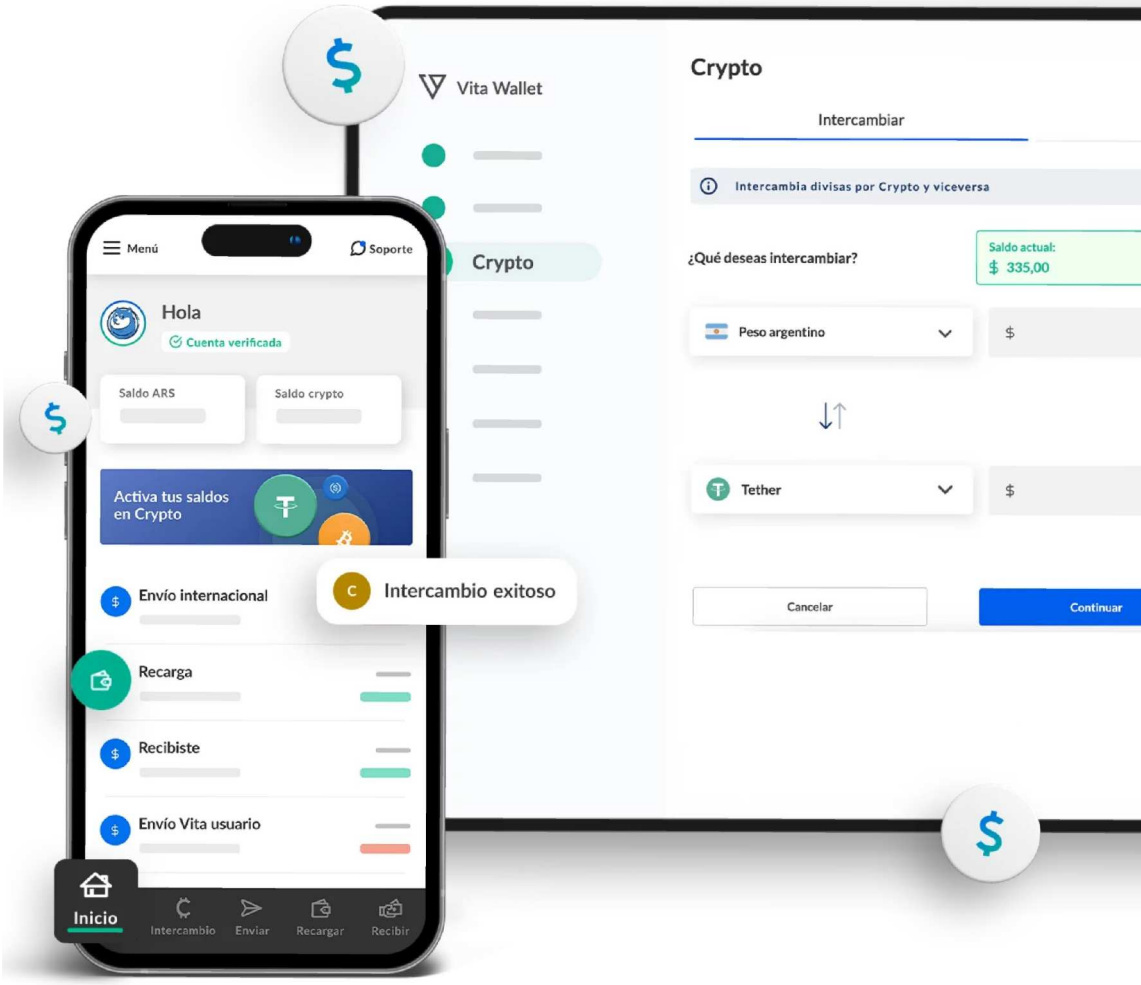
Vita Wallet

MANUAL DE PROCEDIMIENTOS

PREVENCIÓN DEL LAVADO DE ACTIVOS Y FINANCIACIÓN DEL TERRORISMO

VITA DIGITAL S.R.L.



APROBACIÓN DEL MANUAL.

OFICIAL DE CUMPLIMIENTO:	Yondri Roa Arellano
ELABORADO POR:	Vita Digital S.R.L.
APROBADO POR:	Directorio
FECHA DE APROBACIÓN:	Septiembre 2024
FECHA DE ACTUALIZACIÓN:	Septiembre 2024

CONSTANCIA DE REGISTRO

- CNV -

Registro de Proveedores de Servicios de Activos Virtuales (PSAV)

PERSONAS JURIDICAS

REGISTRO CNV N°	RAZON SOCIAL	CLAVE IDENTIFICACION	NUMERO DE IDENTIFICACION	SITIO WEB
9	Vita Digital SRL	CUIT	30717447243	https://vitawallet.io/ar/

Vita Digital S.R.L.- Proveedor de Servicios de Activos Virtuales (PSAV) inscripto bajo el N° 9 en el Registro de Proveedores de Servicios de Activos Virtuales de CNV.

Este registro es a los fines del control como Sujeto Obligado ante la Unidad de Información Financiera (UIF) y de todo otro ente regulador facultado a tal efecto, en el marco de sus competencias, y no implica licencia ni supervisión por parte de la COMISIÓN NACIONAL DE VALORES sobre la actividad realizada por el PSAV".

CONSTANCIA DE REGISTRO

- UIF -

SUJETOS OBLIGADOS REGISTRADOS

CUIT : 30717447243

Tipo de Sujeto Obligado: Proveedores de Servicios de Activos Virtuales

El número de CUIT/CUIL consultado corresponde a un Sujeto Obligado registrado y habilitado en el Sistema SRO de la Unidad de Información Financiera.

Fecha de consulta: 07/10/2024

CONTENIDO.

17. Revisión externa independiente / Auditoría externa e interna

18. Congelamiento administrativo de bienes o dinero

19. Política de contratación empleados

20. Política de evaluación de activos virtuales

21. Procedimiento desvinculación de clientes.

22. Tecnología de monitoreo.

1. Objetivos

El objetivo principal del presente manual es dar a conocer los procedimientos y actividades que debe desarrollar VITA DIGITAL S.R.L. (*en adelante "Vita"*) con relación al cumplimiento de las disposiciones legales vigentes, y los demás lineamientos que la Unidad de Información Financiera y la Comisión Nacional de Valores ha establecido sobre el tema en prevención, detección y erradicación del delito de lavado de activos y el financiamiento de delitos, constituyendo así una guía para el desarrollo de las actividades de empleados y clientes de Vita.

A. Alcance

El presente manual contendrá los procedimientos, lineamientos y medidas para prevenir el lavado de activos, financiamiento del terrorismo y otros delitos, de todos los productos y servicios que ofrece Vita, siendo aplicable a toda la operación, respecto de clientes permanentes u ocasionales, accionistas, directivos, funcionarios y empleados, prestadores de servicios, así como para las personas físicas y jurídicas con quienes se mantenga relaciones contractuales.

B. Conceptos LA y FT

El lavado de activos y la financiación del terrorismo son conductas delictivas que atentan no sólo la estabilidad de los sistemas democráticos y el desarrollo de sus economías, sino fundamentalmente la libertad de los ciudadanos.

La lucha contra estos delitos es una preocupación prioritaria del Estado Nacional, adoptándose consecuentemente las medidas regulatorias que tornen eficaces la prevención y represión de tales conductas.

En primer lugar resulta conveniente introducir los conceptos de lavado de dinero y financiación del terrorismo. Básicamente, y conforme las definiciones comúnmente divulgadas, el término “lavado de dinero”, se refiere a dar apariencia lícita a dinero obtenido de manera ilícita.

En tal sentido, resulta un proceso mediante el cual, los bienes de origen delictivo se integran al sistema económico legal con apariencia de haberse obtenido en forma lícita.

Respecto del segundo, y en línea con lo expresado por la Organización de Naciones Unidas (ONU), los actos, métodos y prácticas del terrorismo en todas sus formas y manifestaciones constituyen actividades cuyo objeto es la destrucción de los derechos humanos, las libertades fundamentales y la democracia, amenazando la integridad territorial y la seguridad de los Estados y desestabilizando los gobiernos legítimamente constituidos.

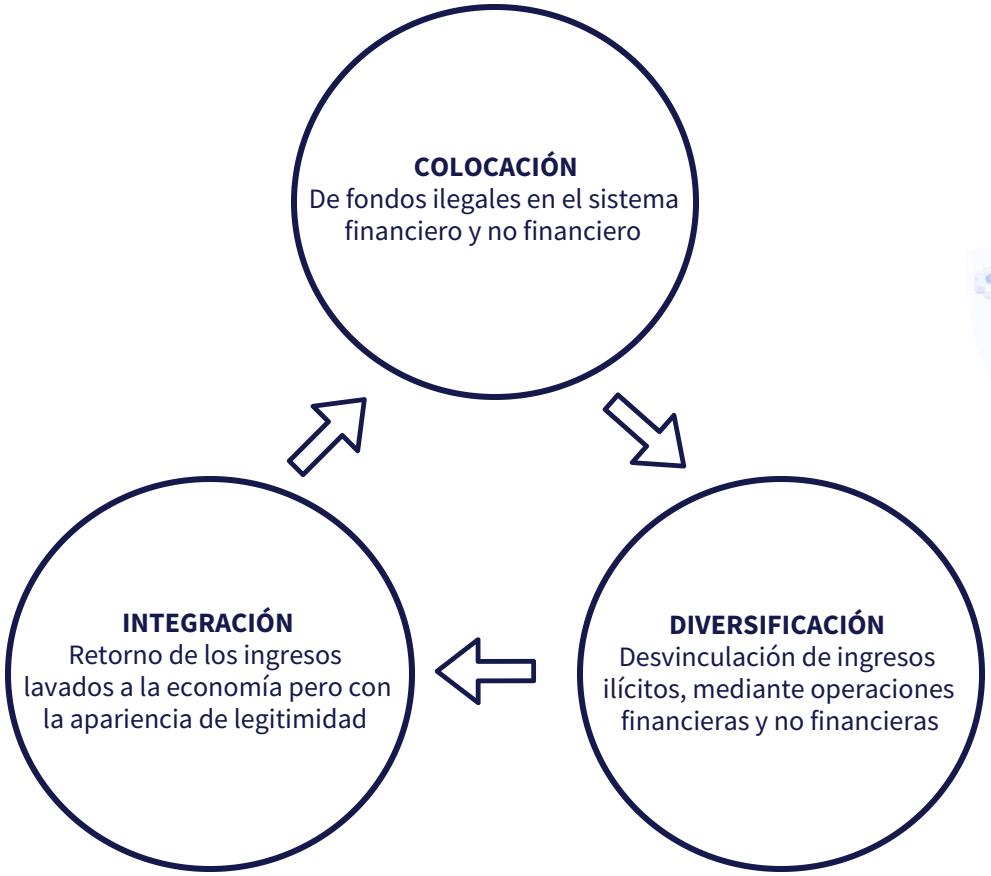
Reconociendo además, que el desarrollo, la paz, la seguridad, y los derechos humanos están interrelacionados y se refuerzan mutuamente. Para perpetrar actos de esta naturaleza, es preciso movilizar fondos con el objetivo de mantener redes clandestinas, células e individuos de la organización, comprar y adiestrar equipos, adquirir armas, organizar acciones complejas o comprar complicidades (Oficina de las Naciones Unidas contra la Droga y el Delito UNODC, 2010).

Ahora bien, tales conductas presentadas individualmente, tienen puntos de contacto. De conformidad con lo plasmado por la UIF en sus documentos de trabajo, ambos delitos son independientes y autónomos, ya que no en todos los casos el terrorismo necesita hacer uso del blanqueo de su dinero para alcanzar sus objetivos. En función de lo anterior, se puede señalar que la financiación del terrorismo puede ocurrir con bienes lícitos o ilícitos, mientras que en el blanqueo el origen de los fondos es siempre ilícito.

La expresión “lavar dinero” se refiere a una acción pasada ilegal que produjo activos, los cuales, se procuran integrar al sistema económico formal con la apariencia de haber sido obtenidos en forma lícita, en tanto que la expresión “financiar el terrorismo”, se refiere a una acción futura ilegal.

C. Proceso de lavado Activos.

El proceso de lavado de activos se compone de tres etapas:



D. Etapas para el financiamiento del terrorismo.

El proceso de lavado de activos se compone de tres etapas:

E. Marco legal

● E.1. ASPECTOS INTERNACIONALES

FAFT- GAFI (Finantial Action Task Force /Grupo de Acción Financiera Internacional)

Organismo gubernamental, que emite 40 recomendaciones a sus países miembros, su propósito es elaborar y promover medidas para combatir el blanqueo de capitales.

Grupo EGMONT

Instancia que reúne a las Unidades de Inteligencia Financiera UIF del mundo, a fin de discutir sobre las organizaciones especializadas en la lucha contra el lavado de dinero.

Organización de las Naciones Unidas (ONU)

El papel de la ONU en materia de lavado de activos se desempeña a partir de cuatro elementos básicos:

1. Convención de Viena de 1988.

2. Convención de Palermo de 2000.

3. Declaración Política y el Plan de Acción adoptados por la Asamblea General en junio de 1998, que subraya la importancia de fortalecer la cooperación internacional, regional y subregional para el combate del lavado de activos.

4. Programa Mundial contra el Lavado de Dinero.

Organización de Estados Americanos (OEA) y (CICAD)

La Unidad focaliza sus esfuerzos en proveer asistencia técnica y capacitación a todos los estados miembro en las medidas judiciales y financieras y en el control legal. A través del Grupo de Expertos, se elaboran Regulaciones Modelo sobre delitos de lavado de dinero relacionados con el tráfico de drogas y otros delitos.

Internacional l Grupo de Acción Financiera Latinoamericana (GAFILAT)

Organización intergubernamental de base regional que agrupa a 18 países latinoamericanos, los cuales son: Argentina, Cuba, Panamá, Bolivia, Ecuador, Paraguay, Brasil, Guatemala, Perú, Chile, Honduras, República Dominicana, Colombia, México, Uruguay, Costa Rica, Nicaragua.

● E.2. NORMATIVA NACIONAL

Ley 25.246 y modificatorias. Esta ley tiene por finalidad prevenir, detectar y erradicar el lavado de activos y la financiación de delitos, en sus diferentes modalidades.

¿De qué forma y en qué norma se encuentra tipificado el delito de lavado de activos?

El delito de lavado de activos ("LA") fue tipificado e incorporado al Código Penal mediante ley Nº 25.246 (B.O. 10/5/2000), modificada por ley Ley Nº 26.683 (B.O. 21/06/2011).

El delito se encuentra previsto en el artículo 303 del Código Penal (bajo el Título XIII referido a los "Delitos contra el Orden Económico y Financiero") estableciendo que la figura básica de LA implicará prisión de tres (3) a diez (10) años y multa de dos (2) a diez (10) veces del monto de la operación, al que convirtiere, transfiriere, administrare, vendiere, gravare, disimulare o de cualquier otro modo pusiere en circulación en el mercado, bienes provenientes de un ilícito penal, con la consecuencia posible de que el origen de los bienes originarios o los subrogantes adquieran la apariencia de un origen lícito, y siempre que su valor supere la suma de pesos trescientos mil ($ 300.000), sea en un solo acto o por la reiteración de hechos diversos vinculados entre sí.

CÓDIGO PENAL DE LA NACION "TITULO XIII

ARTICULO 303. -

1) Será reprimido con prisión de tres (3) a diez (10) años y multa de dos (2) a diez (10) veces del monto de la operación, el que convirtiere, transfiriere, administrare, vendiere, gravare, disimulare o de cualquier otro modo pusiere en circulación en el mercado, bienes provenientes de un ilícito penal, con la consecuencia posible de que el origen de los bienes originarios o los subrogantes adquieran la apariencia de un origen lícito, y siempre que su valor supere la suma de pesos trescientos mil ($ 300.000), sea en un solo acto o por la reiteración de hechos diversos vinculados entre sí.

2) La pena prevista en el inciso 1 será aumentada en un tercio del máximo y en la mitad del mínimo, en los siguientes casos:

a) Cuando el autor realizare el hecho con habitualidad o como miembro de una asociación o banda formada para la comisión continuada de hechos de esta naturaleza;

b) Cuando el autor fuera funcionario público que hubiera cometido el hecho en ejercicio u ocasión de sus funciones. En este caso, sufrirá además pena de inhabilitación especial de tres (3) a diez (10) años. La misma pena sufrirá el que hubiere actuado en ejercicio de una profesión u oficio que requirieran habilitación especial.

ARTICULO 304.-
Cuando los hechos delictivos previstos en el artículo precedente hubieren sido realizados en nombre, o con la intervención, o en beneficio de una persona de existencia ideal, se impondrán a la entidad las siguientes sanciones conjunta o alternativamente:

1. Multa de dos (2) a diez (10) veces el valor de los bienes objeto del delito.

2. Suspensión total o parcial de actividades, que en ningún caso podrá exceder de diez (10) años.

3. Suspensión para participar en concursos o licitaciones estatales de obras o servicios públicos o en cualquier otra actividad vinculada con el Estado, que en ningún caso podrá exceder de diez (10) años.

4. Cancelación de la personería cuando hubiese sido creada al solo efecto de la comisión del delito, o esos actos constituyan la principal actividad de la entidad.

5. Pérdida o suspensión de los beneficios estatales que tuviere.

6. Publicación de un extracto de la sentencia condenatoria a costa de la persona jurídica. Para graduar estas sanciones, los jueces tendrán en cuenta el incumplimiento de reglas y procedimientos internos, la omisión de vigilancia sobre la actividad de los autores y partícipes, la extensión del daño causado, el monto de dinero involucrado en la comisión del delito, el tamaño, la naturaleza y la capacidad económica de la persona jurídica. Cuando fuere indispensable mantener la continuidad operativa de la entidad, o de una obra, o de un servicio en particular, no serán aplicables las sanciones previstas por el inciso 2 y el inciso 4.

(Artículo incorporado por art. 5º de la Ley Nº 26.683 B.O. 21/06/2011).

ARTICULO 305.-
El juez podrá adoptar desde el inicio de las actuaciones judiciales las medidas cautelares suficientes para asegurar la custodia, administración, conservación, ejecución y disposición del o de los bienes que sean instrumentos, producto, provecho o efectos relacionados con los delitos previstos en los artículos precedentes. En operaciones de lavado de activos, serán decomisados de modo definitivo, sin necesidad de condena penal, cuando se hubiere podido comprobar la ilicitud de su origen, o del hecho material al que estuvieren vinculados, y el imputado no pudiere ser enjuiciado por motivo de fallecimiento, fuga, prescripción o cualquier otro motivo de suspensión o extinción de la acción penal, o cuando el imputado hubiere reconocido la procedencia o uso ilícito de los bienes.

Los activos que fueren decomisados serán destinados a reparar el daño causado a la sociedad, a las víctimas en particular o al Estado. Sólo para cumplir con esas finalidades podrá darse a los bienes un destino específico. Todo reclamo o litigio sobre el origen, naturaleza o propiedad de los bienes se realizará a través de una acción administrativa o civil de restitución. Cuando el bien hubiere sido subastado sólo se podrá reclamar su valor monetario.

ARTICULO 306.-
1. Será reprimido con prisión de cinco (5) a quince (15) años y multa de dos (2) a diez (10) veces del monto de la operación, el que directa o indirectamente recolectare o proveyere bienes o dinero, con la intención de que se utilicen, o a sabiendas de que serán utilizados, en todo o en parte:

a) Para financiar la comisión de un delito con la finalidad establecida en el artículo 41 quinquies;

b) Por una organización que cometa o intente cometer delitos con la finalidad establecida en el artículo 41 quinquies;

c) Por un individuo que cometa, intente cometer o participe de cualquier modo en la comisión de delitos con la finalidad establecida en el artículo 41 quinquies.

2. Las penas establecidas se aplicarán independientemente del acaecimiento del delito al que se destinara el financiamiento y, si éste se cometiere, aún si los bienes o el dinero no fueran utilizados para su comisión.

3. Si la escala penal prevista para el delito que se financia o pretende financiar fuera menor que la establecida en este artículo, se aplicará al caso la escala penal del delito que se trate.

4. Las disposiciones de este artículo regirán aún cuando el ilícito penal que se pretende financiar tuviere lugar fuera del ámbito de aplicación espacial de este Código, o cuando en el caso del inciso b) y c) la organización o el individuo se encontraren fuera del territorio nacional, en tanto el hecho también hubiera estado sancionado con pena en la jurisdicción competente para su juzgamiento.
(Artículo incorporado por art. 5° de la Ley N° 26.734 B.O. 28/12/2011)

Cabe destacar por otra parte, las modificaciones al Código Penal que a continuación se transcriben:

ARTICULO 41 quinquies.-
Cuando alguno de los delitos previstos en este Código hubiere sido cometido con la finalidad de aterrorizar a la población u obligar a las autoridades públicas nacionales o gobiernos extranjeros o agentes de una organización internacional a realizar un acto o abstenerse de hacerlo, la escala se incrementará en el doble del mínimo y el máximo. Las agravantes previstas en este artículo no se aplicarán cuando el o los hechos de que se traten tuvieren lugar en ocasión del ejercicio de derechos humanos y/o sociales o de cualquier otro derecho constitucional.
(Artículo incorporado por art. 3° de la Ley N° 26.734 B.O. 28/12/2011)

REGULACIÓN LOCAL EN MATERIA DE CRIPTO-ACTIVOS

- **LEY 25.246**

Encubrimiento y Lavado de Activos de origen delictivo. Unidad de Información Financiera. Deber de informar. Sujetos obligados.
ARTICULO 20. — Están obligados a informar a la Unidad de Información Financiera (UIF), de conformidad con las normas que dicte dicho organismo, los siguientes sujetos:

13. Los proveedores de servicios de activos virtuales.

- **RESOLUCIÓN CNV 994/2024**

PROVEEDORES DE SERVICIOS DE ACTIVOS VIRTUALES (PSAV). REGISTRO.
ARTÍCULO 1°.- Las personas humanas y jurídicas:

a) Residentes o constituidas en la Argentina que realicen una o más de las actividades u operaciones comprendidas en el artículo 4° bis de la Ley N° 25.246 y sus modificatorias, deberán inscribirse en el "Registro de PSAV" (el "Registro"), habilitado por la Comisión a tal fin, con anterioridad a la realización de dichas actividades u operaciones.

b) Residentes o constituidas fuera de la Argentina que realicen una o más de las actividades u operaciones comprendidas en el artículo 4° bis de la Ley N° 25.246 y sus modificatorias, deberán inscribirse en el Registro con anterioridad a la realización de dichas actividades u operaciones, siempre que las realicen bajo cualquiera de las modalidades mencionadas en el artículo 3° del presente Capítulo.

Quedan exceptuados de la obligación de inscripción en el Registro, los Proveedores de Servicios de Activos Virtuales ("PSAV") que realicen las actividades u operaciones comprendidas en el artículo 4° bis de la Ley N° 25.246 y sus modificatorias siempre que dichas actividades u operaciones no superen, de manera agregada, un monto equivalente a UNIDADES DE VALOR ADQUISITIVO -actualizables por CER – Ley N° 25.827- TREINTA Y CINCO MIL (UVA 35.000) por mes calendario.

A efectos de su determinación, deberá aplicarse a la totalidad de las actividades u operaciones, registradas en el mes calendario, el valor de la UVA correspondiente al último día de dicho mes.

- **RESOLUCIÓN UIF 49/2024**

CAPÍTULO I. OBJETO Y DEFINICIONES.

ARTÍCULO 1°.- Objeto.

La presente resolución tiene por objeto establecer los requisitos mínimos para la identificación, evaluación, monitoreo, administración y mitigación de los riesgos de lavado de activos, financiación del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva (LA/FT/FP) que los Sujetos Obligados previstos en el inciso 13 del artículo 20 de la Ley N° 25.246 y sus modificatorias, deberán adoptar y aplicar para gestionar, de acuerdo con sus políticas, procedimientos y controles, el riesgo de ser utilizado por terceros con objetivos criminales de LA/FT/FP.

CAPÍTULO II. SISTEMA DE PREVENCIÓN DE LA/FT/FP DEL SUJETO OBLIGADO.

ARTÍCULO 3°.- Sistema de Prevención de LA/FT/FP.

El Sujeto Obligado deberá implementar un Sistema de Prevención de LA/FT/FP, con un enfoque basado en riesgo, que contendrá todas las políticas, procedimientos y controles a los fines de identificar, evaluar, monitorear, administrar y mitigar eficazmente los riesgos de LA/FT/FP a los que se encuentra expuesto y cumplir con las obligaciones exigidas por la normativa vigente.

Dicho Sistema deberá tener en cuenta las Evaluaciones Nacionales de Riesgos de LA/FT/FP, sus actualizaciones, otros documentos publicados o diseminados por autoridades públicas competentes en los que se identifiquen riesgos vinculados con el sector y aquellos riesgos identificados por el propio Sujeto Obligado.

2. Compromiso asumido

La compañía se compromete a cumplir con las leyes relativas a la prevención y represión del lavado de dinero y la financiación de actividades terroristas. El objetivo principal de las leyes es definir y tipificar como delito el lavado de los ingresos con el fin de privar a los delincuentes de los beneficios de sus delitos.

En consecuencia, estamos obligados a establecer políticas y procedimientos para prevenir las actividades de lavado de dinero. Los procedimientos implementados por Vita son los siguientes:

- Identificación y debida diligencia de los clientes mediante la implementación de un enfoque basado en el riesgo.

- Mantenimiento de registros en relación con la identidad de los clientes.

- Presentación de informes a una persona competente designada para recibir y considerar información que genere conocimiento o sospecha de que un cliente está involucrado en actividades de lavado de dinero.

- Control interno y gestión de riesgos con el objetivo de prevenir actividades de lavado de dinero.

- Examen detallado de cada transacción que por su naturaleza se considera vulnerable al lavado de dinero. Especialmente para transacciones complicadas o inusualmente grandes que tienen lugar sin un objetivo financiero o legal obvio.

- Entrenamiento y formación de los empleados de manera regular y periódica para que conozcan los procedimientos mencionados anteriormente para prevenir el lavado de dinero y la legislación relacionada con el lavado de dinero.

A. Política

● A.1. OBLIGACIONES DEL DIRECTORIO

Las obligaciones del directorio en relación con esta política son las siguientes:

√ Determinar, registrar y aprobar los principios de política general de Vita en relación con la prevención del lavado de dinero y el financiamiento del terrorismo.

√ Comunicación a todos los empleados de Vita que tienen la responsabilidad de la aplicación de las prácticas, medidas, procedimientos y controles que se han determinado.

√ Asegurar que se apliquen todos los requisitos de la Ley y qué se introduzcan sistemas y controles apropiados, efectivos y suficientes para cumplir con el requisito antes mencionado.

√ Asegurar que cualquier persona asignada con el deber de implementar los procedimientos para la prevención del lavado de dinero y el financiamiento del terrorismo tenga acceso completo y oportuno a todos los datos e información que conciernen a la identidad de los clientes y otros archivos relevantes e información mantenida por Vita para ser fácilmente utilizado en la ejecución efectiva de sus funciones.

√ Asegurar que todos los empleados conozcan a las personas a las que se les asignaron los deberes de implementar los procedimientos de lavado de dinero y que sepan a quien informar cualquier dato relacionado con actividades de las que tengan conocimiento o sospecha que puedan estar relacionados con el lavado de dinero y financiamiento del terrorismo .

B. Oficial de Cumplimiento

Es el integrante del Directorio, designado por éste como máximo responsable operativo de las políticas de Prevención del Lavado de Activos y Financiamiento del Terrorismo, para cuyo ejercicio debe contar con absoluta independencia, autonomía y acceso pleno a la información necesaria para el desarrollo de sus funciones.

Deberá comunicarse a la UIF el nombre y apellido, tipo y número de documento de identidad, cargo en el órgano de administración, fecha de designación y número de C.U.I.T. (clave única de identificación tributaria) o C.U.I.L. (código único identificación laboral), los números de teléfono, fax, dirección de correo electrónico y lugar de trabajo de dicho Oficial de Cumplimiento. Esta comunicación debe efectuarse de acuerdo con lo dispuesto por la Resolución UIF Nº 50/11 (o la que en el futuro la complemente, modifique o sustituya) y además, por escrito en la sede de la UIF, acompañándose toda la documentación de respaldo.

El Oficial de Cumplimiento deberá constituir domicilio, donde serán válidas todas las notificaciones efectuadas. Una vez que haya cesado en el cargo deberá denunciar el domicilio real, el que deberá mantenerse actualizado durante el plazo de CINCO (5) años contados desde el cese.

Cualquier sustitución que se realice del mismo deberá comunicarse fehacientemente a la UIF dentro de los QUINCE (15) días de realizada, señalando las causas que dieron lugar al hecho, continuando la responsabilidad del Oficial de Cumplimiento hasta la notificación de su sucesor a la UIF.

Es posible, si así lo decide el Directorio, designar un Oficial de Cumplimiento Suplente. En tal caso, se deberá comunicar esa circunstancia a la UIF de acuerdo a las disposiciones contenidas en la Resolución UIF Nº31/2012.

Los Sujetos Obligados deberán comunicar a la UNIDAD DE INFORMACIÓN FINANCIERA, dentro de los CINCO (5) días de acaecidos los hechos mencionados en el párrafo precedente, la entrada en funciones del Oficial de Cumplimiento suplente, los motivos que la justifican y el plazo durante el cual se encontrará en funciones.

El Oficial de Cumplimiento tiene a su cargo las siguientes **funciones**:

- **Velar** por el cumplimiento de las políticas establecidas por el Directorio para prevenir, detectar y reportar operaciones que puedan estar vinculadas a los delitos de Lavado de Activos y Financiamiento del Terrorismo.

- **Diseñar e implementar** los procedimientos y controles, necesarios para prevenir, detectar y reportar las operaciones que puedan estar vinculadas a los delitos de Lavado de Activos y Financiamiento del Terrorismo.

- **Diseñar e implementar** políticas de capacitación para los funcionarios y empleados de la concesionaria, considerando la naturaleza de las tareas desarrolladas y elaborar el cronograma anual de capacitación.

- **Actualizar** el Manual y los Instructivos.

- **Analizar** las operaciones realizadas para detectar eventuales operaciones sospechosas.

- **Formular** los reportes sistemáticos y de operaciones sospechosas a la UIF y dar cumplimiento a los requerimientos efectuados por esa Unidad.

- **Llevar el registro** del análisis y gestión de riesgo de operaciones inusuales detectadas (que contenga e identifique aquellas operaciones que por haber sido consideradas sospechosas hayan sido reportadas).

- **Dar cumplimiento** a los requerimientos efectuados por la UIF en ejercicio de sus facultades legales.

- **Controlar** la observancia de la normativa vigente en materia de Prevención de Lavado de Activos y Financiamiento del Terrorismo.

- **Asegurar** la adecuada conservación y custodia de la documentación.

- Prestar especial atención al riesgo que implican las relaciones comerciales y operaciones relacionadas con países o territorios donde no se aplican, o no se aplican suficientemente, las Recomendaciones del FATF-GAFI (www.fatfgafi.org), y con países o territorios calificados como de baja o nula tributación (“paraísos fiscales”) según lostérminos del Decreto Nº 1037/00 y sus modificatorios, respecto de las cuales deben aplicarse medidas de debida diligencia reforzadas.

- Prestar especial atención a las nuevas tipologías de Lavado de Activos y Financiamiento del Terrorismo a los efectos de establecer medidas tendientes a prevenirlas, detectarlas y reportar toda operación que pueda estar vinculada a las mismas, como asimismo a cualquier amenaza de Lavado de Activos o de Financiamiento del Terrorismo que surja como resultado del desarrollo de nuevas tecnologías que favorezcan el anonimato y de los riesgos asociados a las relaciones comerciales u operaciones que no impliquen la presencia física de las partes.

DESIGNACIÓN DEL OFICIAL DE CUMPLIMIENTO

Los Sujetos Obligados que se encuentren constituidos como personas jurídicas, deberán designar un Oficial de Cumplimiento, conforme lo dispuesto en el artículo 20 bis de la Ley Nº 25.246 y sus modificatorias y en el Decreto Nº 290/07 y su modificatorio.

El Oficial de Cumplimiento será responsable de velar por la observancia e implementación de los procedimientos y obligaciones establecidos en virtud de esta resolución y de formalizar las presentaciones ante la UNIDAD DE INFORMACION FINANCIERA.

El Oficial de Cumplimiento deberá constituir domicilio, donde serán válidas todas las notificaciones efectuadas. Una vez que haya cesado en el cargo deberá denunciar el domicilio real, el que deberá mantenerse actualizado durante el plazo de CINCO (5) años contados desde el cese.

Cualquier sustitución que se realice del mismo deberá comunicarse fehacientemente a la UNIDAD DE INFORMACION FINANCIERA dentro de los QUINCE (15) días de realizada, señalando las causas que dieron lugar al hecho, continuando la responsabilidad del Oficial de Cumplimiento hasta la notificación de su sucesor a esta UNIDAD DE INFORMACION FINANCIERA.

El Oficial de Cumplimiento debe gozar de absoluta independencia y autonomía en el ejercicio de las responsabilidades y funciones que se le asignan, debiendo garantizársele acceso irrestricto a toda la información que requiera en cumplimiento de las mismas.

Los Sujetos Obligados podrán designar asimismo un Oficial de Cumplimiento suplente, quien desempeñará las funciones del titular en caso de ausencia, impedimento o licencia de este último. A estos fines deberán cumplirse los mismos requisitos y formalidades que para la designación del titular.

Los Sujetos Obligados deberán comunicar a esta UNIDAD DE INFORMACIÓN FINANCIERA, dentro de los CINCO (5) días de acaecidos los hechos mencionados en el párrafo precedente, la entrada en funciones del Oficial de Cumplimiento suplente, los motivos que la justifican y el plazo durante el cual se encontrará en funciones.

3. Política y Procedimiento de Perfiles Transaccionales & Monitoreo.

A. Perfil Transaccional

Se debe asignar a todo Cliente un Perfil Transaccional prospectivo respecto a las operaciones futuras, confeccionado conforme a la información y documentación brindada por el Cliente y/o que haya podido obtener Vita por sí.

Dicho Perfil debe estar basado en el entendimiento del propósito y la naturaleza esperada de la relación comercial, la información transaccional y la documentación relativa a la situación económica, patrimonial y financiara del Cliente, conforme a los procesos de debida diligencia que le corresponda aplicar.

El perfil será determinado en base al análisis de riesgo de la Entidad, de modo tal que permita la detección oportuna de Operaciones Inusuales y Operaciones Sospechosas realizadas por el Cliente.

El Perfil será calibrado y ajustado con posterioridad conforme con las operaciones efectivamente realizadas por el Cliente.

El respaldo documental del Perfil Transaccional será conforme al nivel de riesgo:

- Riesgo Bajo: Información suministrada por el Cliente o qué hubiera podido obtener la Entidad, conservando las evidencias correspondientes con arreglo de la debida diligencia simplificada.

- Riesgo Medio y Alto: Documentación detallada en los puntos de Debida Diligencia y Debida Diligencia Reforzada.

El responsable del Área de Prevención de lavado de Dinero analiza el objetivo de inversión y del análisis de capacidad patrimonial y financiera del Cliente, establece su perfil de riesgo y límite operativo, de modo tal de permitir la detección oportuna de Operaciones Inusuales y Operaciones Sospechosas realizadas por el Cliente.

B. Análisis y Procesos

Es obligación del responsable de cada Cliente, mantener informado al Oficial de Cumplimiento a los efectos que éste resuelva los cursos de acción a seguir, incluyendo el posible reporte cómo operación sospechosa a la UIF.

Cuando se detecten operaciones consideradas inusuales de acuerdo con una valoración prudencial y objetiva, o cuando se realicen transacciones significativas, o cuando se produzcan cambios relativamente importantes en la forma de operar de un Cliente deberá solicitarse la información adicional que se considere necesaria para justificar o no la situación que se presente.

Deben agotarse todas las instancias, incluyendo las averiguaciones o pedidos de antecedentes por medios externos.

Por lo dicho, al surgir de un control y/o una alerta una Operación Inusual, el Área de Prevención de lavado de Dinero podrá recabar información adicional por Internet u otros medios, recibida la mayor cantidad de información posible analiza la operación y la autoriza o no, para este caso podrá requerir más documentación e información de respaldo del Cliente, para justificar adecuadamente la operatoria alertada, procediendo a la actualización de la información del Cliente como su Perfil Transaccional en caso de que ello sea necesario.

En caso de mantenerse la inusualidad se preparará un informe con el análisis efectuado para el Oficial de Cumplimiento.

Mientras se mantenga la relación comercial con el Cliente o si esta fuera rota por éste en forma intempestiva o que diera lugar a sospechas, deberán llevarse a cabo las siguientes acciones:

a) Verificar que los Clientes no se encuentren incluidos en los listados de terroristas y/u organizaciones terroristas de acuerdo con lo dispuesto por la UIF.

b) Verificar si los Clientes reúnen la condición de Personas Expuestas Políticamente de acuerdo con lo dispuesto por la UIF.

c) Verificar que las operaciones realizadas por el Cliente se ajustan al riesgo que le fuera asignado.

Cuando de los controles especiales antes descriptos y/o del análisis de la inusualidad realizada por el Área de Prevención de Lavado de Dinero, el Oficial de Cumplimiento concluyere que a su juicio hubieran realizado o tentado realizar operaciones sospechosas, deberá dar cumplimiento al reporte de operación sospechosa.

C. Registro interno de Operaciones Inusuales

El área de Prevención de Lavado de dinero, conforme los puntos que anteceden, analizan las Operaciones Inusuales, dicho análisis serán registradas en un registro interno “ad hoc”, el que contendrá al menos, los siguientes datos:
Identificación de la transacción

- Fecha, hora y procedencia de la alerta u otro sistema de identificación de la transacción a analizar
- Analista responsable de su resolución
- Medidas llevadas a cabo para la resolución de la alerta
- Decisión final motivada, incluyendo validación del supervisor o instancia superior, fecha y hora de la decisión final.

Asimismo, se deberán custodiar los legajos documentales íntegros de soporte de tales registros.

4. Enfoque basado en riesgos

A. Matriz de riesgo

Se establecerá una matriz de riesgos que permita una debida diligencia en base a lo siguiente:

- ALCANCE:

El alcance de la matriz de riesgo será aplicado a todos los clientes vigentes permitiendo su perfilamiento previo a la suscripción, así como durante su relación comercial.

- FORMA:

La matriz de riesgo será levantada combinado el estudio de mercado anual, junto con los factores y criterios de riesgo establecidos para cada ramo.

- METODOLOGÍA:

La metodología desarrollada es en base a una valoración que se les otorga a todos los clientes vigentes en virtud de factores y criterios de riesgo. Los factores de riesgo son aquellas características que permiten medir la exposición al riesgo de lavado de activos, financiamiento del terrorismo y otros delitos. Para Vita estos factores son: clasificación cliente, actividad económica, nacionalidad, lugar de residencia, forma de pago, entre otros.

Criterios de riesgo son aspectos de cada factor, el cual nos permite 'caracterizar' al factor de riesgo, es decir, son parámetros que miden la exposición de cada factor al riesgo de lavado de activos.

La calificación de los mismos ha sido desarrollada numéricamente en una escala del 1 al 3, siendo 1 un cliente de menor probabilidad de riesgo y 3 un cliente cuya probabilidad es mayor; es decir, la calificación es directamente proporcional al riesgo de Lavado de Activos, Financiamiento del Terrorismo y otros Delitos.

Con la matriz de riesgo se pretende establecer un "scoring" de clientes en base al grado de exposición al riesgo de Lavado de Activos y Financiamiento del Terrorismo y otros Delitos que esto representa para Vita.

La matriz de riesgo de clientes se va a elaborar para todos los clientes vigentes categorizados por su tipo de identidad como **Personas Naturales** y **Personas Jurídicas**.

PERFIL DE COMPORTAMIENTO - PROBABILIDAD

El perfil de comportamiento o probabilidad de riesgo, conforme lo establece la normativa vigente es aquel que resulta de la cuantificación de los factores y criterios de riesgo para todos los clientes vigentes.

Los principales factores establecidos son los siguientes:

1. Clasificación cliente.
2. Actividad Económica.
3. Nacionalidad.
4. Lugar de residencia.
5. Forma de fondeo.

Para cada factor se obtendrá una calificación de riesgo del 1 al 3, la cual se utilizará posteriormente para obtener el perfil de comportamiento o probabilidad del riesgo de lavado de activos por cliente.

B. Análisis de riesgo de Usuarios

Es una parte importante del programa de PLD de nuestra Empresa obtener la información necesaria sobre cada usuario para permitirnos evaluar el riesgo potencial presentado por ese usuario con el fin de identificar e informar la actividad sospechosa de manera oportuna.

Cuando la Empresa está abriendo una nueva cuenta para un usuario, la calificación de riesgo y la debida diligencia que se realiza forman parte del perfil del usuario y se divide en tres **categorías:**

- Riesgo bajo: la puntuación baja de un usuario se define como aquella que presenta un menor nivel de riesgo asociado con el lavado de dinero o el financiamiento del terrorismo. Este usuario no tiene un impacto significativo en el riesgo general de la Empresa.

- Riesgo medio: se define como uno que podría ser vulnerable al lavado de dinero o al financiamiento del terrorismo. Sin embargo, debido a la naturaleza de los servicios ofrecidos por la Empresa o los productos y servicios utilizados por el usuario, el riesgo de lavado de dinero y financiamiento del terrorismo es moderado.

- Riesgo alto: un puntaje alto de los usuarios se define como uno que es más vulnerable al lavado de dinero o al financiamiento del terrorismo debido al tipo de usuario y/o tipo de servicio/producto utilizado por el usuario.

CATEGORÍAS

Riesgo bajo: La calificación de bajo riesgo debe limitarse a los usuarios que no presentan ningún factor de alto riesgo. Solo los usuarios que cumplan con los siguientes factores pueden considerarse de bajo riesgo a los fines de esta verificación:

• Persona natural;

• Local, residente y que realiza negocios cara a cara; •La operaciones realizadas no superan el monto mensual establecido por la compañía;

• No realiza operaciones en efectivo;

• El esquema societario no es complejo: no hay personas jurídicas o estructuras tales como fideicomisos como vehículos de inversión o como parte de estructuras más complejas; y

• No hay participación de intermediarios.

Los usuarios tienen una clasificación de riesgo personalizada y continuarán siendo así en el futuro. Todas las relaciones y operaciones con los usuarios se realizan de forma online y no cara a cara, lo que significa que la probabilidad de que se utilice la calificación de “Bajo riesgo” es mínima.

Riesgo medio: Los sistemas desarrollado por la Empresa y los factores de mitigación demuestran que el apetito por el riesgo de Vita es de “Riesgo Medio” porque el sistema está diseñado para aceptar principalmente usuarios con esta calificación, con mínimas excepciones (en las que se deberá realizar DDE, debida diligencia extendida).

Como se indica en la evaluación de Alto Riesgo a continuación, se consideran factores de alto riesgo específicos y, en la mayoría de los casos, el usuario no cumplirá con el apetito de riesgo general de Vita dada la información suministrada inicialmente.

Nuestra política de "Conozca a su cliente" satisface nuestro apetito de Riesgo Medio, que puede ser revisado y actualizado periódicamente de acuerdo con las circunstancias, la tecnología y la legislación.

Alto riesgo: Los usuarios que presentan mayores riesgos de lavado de dinero o financiamiento del terrorismo presentan una mayor exposición de nuestra Empresa; las políticas, procedimientos y procesos de debida diligencia se mejoran como resultado de eso. La debida diligencia extendida (DDE) para usuarios de mayor riesgo es especialmente crítica para comprender sus transacciones de forma anticipada y para implementar un sistema de monitoreo de actividades sospechosas que aumente el cumplimiento y reduzca los riesgos de la Empresa. Los usuarios de mayor riesgo y sus transacciones deben revisarse más de cerca y con mayor frecuencia durante el término de su relación con la Empresa.

Los usuarios se clasifican como de alto riesgo en función de los siguientes indicadores:

• Estructuras de negocios complicadas.

• Fuente de fondos desconocida o montos elevados de operación.

ESTRUCTURA DE NEGOCIOS COMPLICADA
√ Riesgo -> Dificultad para identificar el beneficiario final y la fuente de los fondos que se procesan.

√ Política -> Los riesgos se mitigan solo permitiendo personas físicas; implica el envío de identificación, comprobante de domicilio y foto de autenticidad por parte del usuario.

FUENTE DE FONDOS
√ Riesgo -> Dificultad para identificar el origen de los fondos cuando el usuario tiene la intención de realizar operaciones por 100.000 ARS en un mes o 400.000 ARS en un año.

√ Política -> Los riesgos se mitigan solicitando documentación que demuestre el origen de los fondos (declaraciones de impuestos, recibos de sueldo) y no permitiendo recibir transferencias de terceros (solo se aceptan transferencias bancarias desde una cuenta a nombre del usuario).

C. Procedimientos de evaluación de riesgos y Proceso de verificación de cuenta.

El proceso en punto a la verificación de la identidad y prueba de vida se realiza mediante la integración de Onfido (onboarding biométrico y revisión documental).

En caso de que el usuario envíe erróneamente 3 veces seguidas la información mencionada, deberá envíar un formulario con la siguiente información personal: identificación, factura de servicios públicos con su nombre y foto “selfie” con su identificación y una nota escrita a mano.

El operador revisará el formulario enviado por el usuario y verificará que la información coincida con los documentos cargados. Cuando toda la información está correcta, el operador verifica las siguientes afirmaciones y marca una casilla para cada una de ellas:

•El solicitante ha presentado su solicitud a través del sitio web de Vita.

•El solicitante es una persona humana.

•El solicitante desea operar cripto-activos dentro de los límites preestablecidos de Vita.

•El solicitante ha presentado su propia información y ha presentado la debida diligencia.

•La fuente de fondos solicitante es una fuente conocida.

Este proceso, sea manual o automático, establece una calificación de riesgo para el usuario y esta información se puede cambiar en cualquier momento en el perfil del usuario en nuestro sistema, recalculando su calificación automáticamente de nuevo, utilizando los criterios descritos anteriormente en “Categorías".

A continuación se indica cómo el algoritmo calcula la clasificación de riesgo:

• **Riesgo bajo**: el usuario cumple con los 6 puntos indicados anteriormente y se lo conoce personalmente.

• **Riesgo medio**: el usuario cumple con los 6 puntos indicados anteriormente y NO se lo conoce personalmente.

•**Riesgo alto**: el usuario no cumple con los 6 puntos indicados anteriormente.

Esta revisión se realiza una vez al año para cada usuario.

A continuación se indica cómo el algoritmo calcula la clasificación de riesgo:

Se mostrará un recordatorio cuando la última revisión exceda el período de 1 año y se notificará a un operador. Incluso si el recordatorio falla, la fecha de la última revisión siempre está visible en el perfil del usuario. Cuando un usuario modifica el análisis de riesgo, se actualiza la fecha de la última revisión.

RESPONSABILIDAD

Será responsabilidad de Oficial de Cumplimiento determinar en conjunto con el área de riesgos los factores y ponderaciones de riesgo y la categorización de la base de clientes conforme a los factores y ponderaciones establecidos.

Será responsabilidad del área de Cumplimiento la ejecución de una debida diligencia ampliada sobre los clientes que hayan sido categorizados con riesgo alto.

Categorización de clientes - Perfil transaccional

Resultado	Riesgo
1	Bajo_1
2	Bajo_2
3	Bajo_3
4	Medio_1
5	Medio_2
6	Medio_3
7	Medio_4
8	Alto_1
9	Alto_2
10	Alto_3
10 - Reject	No aceptar cliente/ desvincular

A efecto de asignar la nota de categorización de los clientes se tomará en cuenta los siguientes elementos que serán calificados en base a la descripción que abajo se detalla:

FACTOR DE RIESGO	PONDERACIÓN
Esquema de Supervisión	30%
Fuentes de ingreso	30%
Vinculación con PEP	20%
Jurisdicción	20%
TOTAL	100%

Los factores mencionados anteriormente deberán ser evaluados de acuerdo a los siguientes parámetros:

-> Esquema de Supervisión/ Sujeto Obligado (30%)
En caso que el cliente no se encuentre supervisado directamente en su actividad económica principal por un ente regulador, tanto a nivel local como en su país de origen, se asignará una nota de 10. En caso que se encuentre bajo un esquema de supervisión por un ente regulador, se asignará una nota de 3.

-> Fuentes de ingreso (30%)
En caso que el cliente declare otras fuentes de ingreso distintas a las de su actividad económica principal que no están debidamente documentadas, el Departamento de Compliance podrá asignar una nota entre 4 y 10. En caso que las fuentes de ingreso provengan exclusivamente de su actividad económica principal se podrá asignar una nota entre 1 y 4.

-> Vinculación con PEP (20%)
En caso que un cliente declare una relación patrimonial de conformidad a lo establecido en la “Política de identificación de clientes PEP”, y fuese de nacionalidad extranjera se asignará una nota de 10, mientras que para las PEP nacionales se asignará una nota de 9. En caso contrario, se asignará un riesgo 1.

-> Jurisdicción (20%)
En caso que un cliente tenga su sede principal de negocios fuera del territorio latinoamericano se asignará una nota de 10. En caso que su sede principal de negocios esté en un país latinoamericano, excluyendo Panamá se asignará una nota generalmente de 4 y en específico para cada jurisdicción ver el cuadro expuesto infra. En caso que su sede principal se encuentre en Argentina se asignará una nota de 1. Respecto a la nacionalidad de las personas humanas, en caso que sea argentina el puntaje será 1, mientras que si fuere extranjera se asignará una nota de 8.

El Encargado de Cumplimiento será responsable de verificar la información del cliente y deberá asignar la nota de categorización en el Registro del cliente en base a los criterios establecidos en el presente apartado, así como disponer sobre el requerimiento de información de Debida Diligencia Reforzada para el caso de clientes clasificados como Riesgo Alto.

Referencias cfr. variables		
Viariables		**Puntaje**
Actividad Económica	Empleado Privado	**1**
	Empleado Público	**8**
	Trader	**7**
	Monotributista	**3**
	Antigüedad > 3 años	**2**
	Antigüedad < 3 años	**4**
	Banca Privada	**10**
	Opera fondos de terceros	**10**
	Jubilado/Pensionado	**3**
	Estudiante	**3**
	Marihuana/Cannabis, sustancias medicinales y/o químicas no permitidas	10 - Reject
	Armas de fuego y artículos relacionados.	10 - Reject

	Pagos o cobros por servicios personales ilegítimos o inaceptables ejemplo, prostitución, comisión de venganzas o asesinatos, sobornos, comisiones ilegales, coimas, etc.).	10 - Reject
	piratería y pirateo informático y cualquier infracción intencionada o por negligencia grave de los derechos de autor o de propiedad intelectual de terceros	10 - Reject
	Comercializaci ón de listas o bases de datos personales.	10 - Reject
	Pago de rescates por secuestros virtuales o físicos.	10 - Reject
	Juegos de azar, apuestas y otras actividades que impliquen apostar dinero sobre el resultado de un partido, una carrera u otros acontecimiento s impredecibles.	10 - Reject

	Negocios intensivos en efectivo, servicios de cambio de divisas o negocios con metales preciosos.	10 - Reject
	Comercialización de contenidos relacionados con la pornografía y la trata de personas.	10 - Reject
Persona Jurídica	S.A/S.R.L./S.A.U.	**4**
	S.A.S.	**8**
	LLC (US)	**5**
	Limited en paraísos fiscales	**8**
	Posee Manual y Políticas PLA/FT	**4**
	>1 < 3 capas para UBO	**7**
	≥ 3 capas para UBO	**9**
	ONG/Fundacion	**9**

	Samoa Americana, Anguila, Bahamas, Islas Vírgenes Británicas, Costa Rica, Fiyi, Guam, Islas Marshall, Palaos, Rusia, Samoa, Trinidad y Tobago, Islas Turcas y Caicos, Islas Vírgenes de los EE.UU, Vanuatu.	8
	Miembros de la UE	3
	Gran Bretaña	3
	Suiza	5
	Estados Unidos	7
	Chile	2
	Uruguay	5
	Colombia	5
	Venezuela	4
	Brasil	3
	Perú	3
	Bahrein	4
	Granada	5
	Anituga y Barbuda	5
	Mexico	5
	Guatemala	5
	Aruba	5
	República Dominicana	5
	Jamaica	5
	Barbados	5
	Santa Lucía	5
	Honduras	5

	Cuba	5
	San Cristobal y Nuebes	6
	Nicaragua	7
	Haiti	8
	Paraguay	8
	Bolivia	7
	Ecuador	5
	El Salvador	5
Sujetos Obligados	Si	3
	No	10
PEP	Extranjera	10
	Nacional	9
	No	1
Nacionalidad Persona Física	Argentina	1
	Extranjera	8

5. Medidas de debida diligencia - . . Política de conozca a su cliente

Desde el comienzo de la relación con el cliente, se recopila la siguiente información:

Datos a requerir - Cliente persona humana

- Nombre y apellido completo;
- Lugar y fecha de nacimiento;
- Número DNI;
- Número de CUIL o CUIT;}
- Ciudad y país de residencia;
- Dirección y número de teléfono del domicilio;
- Dirección del correo electrónico;
- Detalle de los ingresos netos diferentes a los originados en la actividad principal, especificando la fuente;
- Declaración de origen lícito de recurso.
- Cualquier otro requisito que la RES UIF indique.

Datos a requerir - Cliente persona jurídica

- Razón social;
- CUIT;
- Copia de la escritura de constitución y de sus reformas, de existir éstas;
- Objeto social;
- Ciudad y país del domicilio de la persona jurídica;
- Dirección, número de teléfono y dirección de correo electrónico; Actividad económica;
- Nombres y apellidos completos del representante legal o apoderado;
- Número de documento de identificación;
- Dirección y número de teléfono del domicilio del representante legal o del apoderado
- Declaración de origen lícito de recursos.
- DDJJ - Beneficiarios finales.
- Cualquier otro requisito que la RES UIF indique.

ARTÍCULO 23.- Reglas de identificación y verificación de clientes personas humanas.

Cada Sujeto Obligado deberá contemplar como requisitos mínimos de identificación de sus clientes personas humanas, los siguientes:

a) Nombre y apellido completo, tipo y número de documento que acredite identidad.

La identidad del cliente deberá ser verificada utilizando documentos, datos o información de registros públicos y/u otras fuentes confiables; con resguardo de la evidencia correspondiente de tal proceso y de la copia del documento que acredite la identidad. A tales fines se aceptarán como documentos válidos para acreditar la identidad, el documento nacional de identidad (DNI) emitido por autoridad competente nacional, y la Cédula de Identidad o el Pasaporte otorgados por autoridad competente de los respectivos países emisores.

b) Nacionalidad, fecha y lugar de nacimiento.

c) Código único de identificación laboral (CUIL), Clave única de identificación tributaria (CUIT), Clave de identificación (CDI), o la clave de identificación que en el futuro sea creada por la Administración Federal de Ingresos Públicos (AFIP), o su equivalente para personas extranjeras, en caso de corresponder.

d) Domicilio real (calle, número, localidad, provincia, país y código postal).

e) Número de teléfono y dirección de correo electrónico.

f) Actividad laboral o profesional principal.

g) Dar cumplimiento a lo dispuesto en la Resolución UIF referida a PEP vigente en la materia.

h) Dar cumplimiento a lo dispuesto en la Resolución UIF referida a prevención de financiación del terrorismo.

Los requisitos previstos en el presente artículo resultarán de aplicación, en caso de existir, al apoderado, tutor, curador, representante, garante, y al autorizado, quienes deberán aportar, además de la información y documentación contemplada en el presente artículo a fin de identificarlos y verificar su identidad, el documento que acredite tal relación o vínculo jurídico para verificar que la persona que dice actuar en nombre del cliente esté autorizada para hacerlo.

ARTÍCULO 24.- Reglas de identificación y verificación de clientes personas jurídicas.

Cada Sujeto Obligado deberá identificar a los clientes personas jurídicas y verificar su identidad a través de los documentos acreditativos de su constitución y personería, obteniendo los siguientes datos:

a) Denominación o razón social.

b) Fecha y número de inscripción registral.

c) CUIT, CDI, o Clave de Inversores del Exterior (CIE), o la clave de identificación que en el futuro fuera creada por la AFIP, o su equivalente para personas extranjeras, en caso de corresponder.

d) Copias del instrumento de constitución y/o estatuto social actualizado, a través del cual se deberá verificar la identificación del cliente persona jurídica, utilizando documentos, datos o información de fuentes confiables; con resguardo de la evidencia correspondiente de tal proceso.

e) Domicilio legal (calle, número, localidad, provincia, país y código postal).

g) Actividad realizada.

h) Identificación de los representantes legales y/o apoderados, conforme las reglas para la identificación de personas humanas previstas en la presente resolución.

i) Nómina de los integrantes del órgano de administración u órgano equivalente.

j) Titularidad del capital social. En los casos en los cuales la titularidad del capital social presente un alto nivel de atomización por las características propias, se tendrá por cumplido este requisito mediante la identificación de los integrantes del consejo de administración o equivalente y/o aquellos que ejerzan el control efectivo de la persona jurídica.

k) Identificación de beneficiarios finales y verificación de la identidad de los beneficiarios finales, de conformidad con la normativa vigente.

Cuando el cliente sea una sociedad que realiza oferta pública de sus valores negociables, listados en un mercado local o internacional autorizado y la misma esté sujeta a requisitos sobre transparencia y/o revelación de información, no deberán cumplirse los requisitos de los incisos j) y k), debiendo acreditar tal circunstancia.

l) Dar cumplimiento a lo dispuesto en la Resolución UIF referida a PEP vigente en la materia, en relación con los beneficiarios finales.

m) Dar cumplimiento a lo dispuesto en la Resolución UIF referida a prevención de financiación del terrorismo vigente, en relación con los beneficiarios finales.

Vita ha adoptado todos los requisitos legales en relación con la identificación del cliente y los procedimientos de debida diligencia. En particular, los procedimientos de debida diligencia se aplican en los siguientes casos:

- Al establecer una relación comercial.

- Al realizar transacciones mensuales por un valor de **$5.000.000** (cinco millones de pesos argentinos) o más, ya sea que la transacción se lleve a cabo en una sola operación o en varias operaciones que parecen estar vinculadas.

- Al realizar transacciones anuales por un valor de **$10.000.000** (diez millones pesos argentinos) o más, ya sea que la transacción se lleve a cabo en una sola operación o en varias operaciones que parecen estar vinculadas.

- Cuando existe una sospecha de lavado de dinero o financiamiento del terrorismo, independientemente del monto de la transacción.

- Cuando existen dudas sobre la veracidad o adecuación de los datos de identificación del cliente obtenidos previamente

A. Política de aceptación de los clientes

La política de aceptación del cliente se determina e implementa bajo criterios particulares relacionados con el perfil de riesgo del cliente. En particular, los factores que especifican la categoría de riesgo a la que se atribuye un cliente son los siguientes:

√ Naturaleza de la actividad empresarial;

√ País de origen;

√ Naturaleza de la transacción comercial;

√ Origen de los fondos.

En base a los factores anteriores, Vita puede rechazar inicialmente la solicitud del cliente o establecer una relación comercial con el cliente clasificándolo como de riesgo bajo, medio o alto.

B. Debida diligencia del cliente

Se aplican procedimientos simplificados para clientes de bajo riesgo.

Los siguientes tipos de clientes se consideran de Alto riesgo, por lo tanto se aplican medidas reforzadas:

•Instituciones de crédito o financieras.

•Sociedades que cotizan y cuyos valores se admiten en un mercado regulado y empresas que cotizan en bolsa de otros países y que están sujetos a requisitos de divulgación coherentes con la legislación local.

•Autoridades públicas nacionales.

•Personas políticamente expuestas.

•Empresas en las cuales su esquema societario no esta claro.

Cabe señalar que Vita recabará la información suficiente para establecer si el cliente califica como cliente de bajo riesgo. Dicha información se relaciona con la identidad del cliente, su perfil económico y el nivel de las transacciones con el objetivo de determinar las inusuales o de sospecha.

C. Debida diligencia mejorada del cliente

Vita aplicará medidas mejoradas de debida diligencia del cliente en situaciones que por su naturaleza pueden presentar un mayor riesgo de lavado de dinero o financiamiento del terrorismo.

No se aceptan los siguientes tipos de clientes, ya que pueden considerarse de alto riesgo:

•Con alta complejidad de la estructura de propiedad de las personas jurídicas.

•Con acciones al portador.

•Desde países de alto riesgo o desde países conocidos por alto nivel de corrupción o crimen organizado o tráfico de drogas.

D. Otros asuntos relacionados con la debida diligencia - y los procedimientos de notificación

1) Momento de la identificación

La identificación del cliente tendrá lugar antes del establecimiento de una relación comercial o de la realización de una transacción.

2) Renovación de la identificación del cliente

Las revisiones de los registros existentes se llevarán a cabo cada 3 años, asegurando así que los documentos, datos o información mantenidos se mantengan actualizados. Los procedimientos de debida diligencia del cliente se aplicarán no solo a todos los clientes nuevos, sino también en los momentos adecuados a los clientes existentes sobre una base sensible al riesgo. Además, las medidas, los procedimientos y los controles se mantendrán bajo revisión periódica para que los riesgos resultantes de los cambios en las características de los clientes existentes, nuevos clientes, servicios e instrumentos financieros se administren y contrarresten de manera efectiva.

3) Cuentas anónimas o numeradas

Vita tiene prohibido mantener cuentas anónimas o numeradas. Además, deberá prestar especial atención a cualquier amenaza de lavado de dinero o financiamiento del terrorismo que pueda surgir de productos o transacciones que puedan favorecer el anonimato y tomar medidas para evitar su uso.

4) Debida diligencia de terceros

Vita puede confiar en terceros para cumplir con los requisitos de debida diligencia del cliente. Sin embargo, la responsabilidad final de cumplir esos requisitos seguirá siendo de Vita.

5) Mantenimiento de registros

Vita conservará los siguientes documentos e información para su uso en cualquier investigación o análisis posible de lavado de dinero o financiamiento del terrorismo por parte de las autoridades nacionales:

•El nombre y la dirección de los clientes y las copias o registros de documentos de identificación oficiales (como pasaportes, documentos de identidad o registros de conducir).

•Los detalles de la cuenta desde la cual se enviaron o recibieron fondos.

Vita conservará la información obtenida como resultado del análisis de debida diligencia del cliente por un período de al menos 5 años después de que la relación comercial con el cliente haya finalizado.

6) Empleados que informan la cadena

Los empleados deberán cooperar e informar sin demora cualquier cosa que les llegue a su conocimiento en relación a transacciones para las cuales existe una leve sospecha relacionada con el lavado de dinero o el financiamiento del terrorismo. Vita se asegurará de que los empleados sean plenamente conscientes de esa obligación de informar y de que se les haya presentado un programa satisfactorio de educación y capacitación.

7) Información y Debida Diligencia de Beneficiarios Finales

En cumplimiento a la RES UIF N° 112/2021 y el resto de la normativa en materia de prevención de LA y FT, toda cuenta empresa deberá remitir previamente a su creación la DDJJ de beneficiarios finales.

Además de los datos y documentos señalados en los procedimientos de debida diligencia en el momento que el beneficiario (s) pretenda ejercer sus derechos, deben obtener la siguiente información:

i)Acreditar origen de fondos;
ii)Aportar documentación del origen de fondos.

Vita Wallet

DECLARACIÓN JURADA DE BENEFICIARIO FINAL.

Lugar y fecha: ..../..../.....

Denominación de la entidad: ……..

En cumplimiento de lo dispuesto por las políticas de prevención de Lavado de Dinero y Financiamiento del Terrorismo, el que suscribe en mi carácter de representante de la firma indicada; por la presente, declaro bajo juramento que:

Nombre y apellido	Nº DNI	Nacionalidad	Domicilio real	Cantidad de acciones	% de acciones

reviste/n el carácter de beneficiario/s final/es, dueños o controladores de las acciones/ cuotas sociales emitidas, que no existen otros propietarios o controladores más que los declarados y que de haber otros en el futuro, se notificará en un periodo no mayor de 30 días contados a partir de la fecha de modificación.----------

Asimismo, declaro bajo juramento que los datos consignados en la presente son correctos, completos y fiel expresión de la verdad.

(Firma)

(Aclaración)

6. Debida Diligencia PEPs

En cumplimiento a la RES UIF N° 35/2023 y las normas de prevención, la compañía, establecerá procedimientos más estrictos al inicio de las relaciones contractuales y durante el monitoreo de sus operaciones. El inicio y continuación de la relación comercial con personas políticamente expuestas implica una debida diligencia reforzada y debe contar con la autorización de la alta gerencia, entendiéndose como la alta gerencia a:

1. Presidente Ejecutivo

2. Unidad de Cumplimiento

3. Gerentes Comerciales de cada unidad comercial de la compañía.

Si durante la relación contractual un cliente o beneficiario se convierte en persona políticamente expuesta, la continuación de la relación comercial debe ser sometida a aprobación de la alta gerencia.

La persona calificada por la empresa como políticamente expuesta, será considerada como tal después de tres (3) años de haber cesado en las funciones que desempeñaba.

La empresa debe realizar las gestiones tendientes a determinar si los montos de las inversiones guardan relación con las actividades y capacidad económica de estos clientes, es decir, que la operatividad de las personas políticamente expuestas se ajuste a los perfiles operativos y de comportamiento previamente levantados.

La compañías también aplicarán las medidas constantes, si uno o más de los accionistas de uno de sus clientes es una persona políticamente expuesta.

En cumplimiento a la Ley de Prevención, Detección y Erradicación del Delito de Lavado de Activos y del Financiamiento de Delitos vigente, Las relaciones comerciales con personas expuestas políticamente (PEP), deberán ser objeto de procedimientos de debida diligencia ampliada, la compañía, deberá tomar medidas razonables, al inicio y durante el monitoreo de las relaciones comerciales o contractuales, para identificar si el cliente, socio, donante, aportante, según sea el caso, o el beneficiario final es una persona expuesta políticamente (PEP) e implementar procedimientos de control y seguimiento per-

manentes más exigentes respecto de transacciones o actos contractuales que estos realicen.

El Oficial de Cumplimiento, deberá elaborar un perfil basado en la políticas "Conozca a su cliente" y efectuar las gestiones tendientes a determinar si el origen de los fondos y patrimonio del cliente, socio, donante, aportante, según sea el caso, guarda relación con las actividades y capacidad económica de éste, es decir, que la transacción o el acto contractual realizado por las personas expuestas políticamente (PEP) se ajuste a los perfiles transaccionales y de comportamiento previamente levantados, también aplicarán las medidas que correspondan, sí uno o más de los accionistas mayoritarios de uno de sus clientes, socios, donantes, aportantes, según sea el caso, es una persona expuesta políticamente.

FAMILIARES Y PERSONAS RELACIONADAS

Las relaciones comerciales o contractuales que involucren al cónyuge o a las personas unidas bajo el régimen de unión de hecho reconocido legalmente; o, a familiares comprendidos hasta el segundo grado de consanguinidad o primero de afinidad; a personas naturales o jurídicas de cualquier naturaleza, con las cuales una persona expuesta políticamente (PEP), se encuentre asociada o vinculada societariamente, o sus colaboradores cercanos, deberán ser sometidas a los mismos procedimientos de debida diligencia ampliada.

7. Monitoreo de Operaciones

A. Monitoreo continuo de operaciones

La Empresa tiene procedimientos establecidos para realizar el monitoreo y la revisión continua de las transacciones y la DDU, Debida Diligencia del Usuario.

B. Monitoreo de transacciones

Vita cuenta con un sistema interno y los servicios integrados de TRM Labs que permite monitorear cada transacción realizada en la plataforma, junto con la integración de los servicios de Onfido y Neitcom para el cruce de listas.

El sistema está diseñado para garantizar que todas las transacciones se encuentren dentro de los límites establecidos y, por lo tanto, la Empresa no está expuesta a ese tipo de riesgo.

El límite está establecido para evitar el trato con clientes de alto riesgo. Si un cliente le pide a la Empresa que aumente sus límites transaccionales, entonces podemos realizar una DDE (Debida Diligencia Extendida) y autorizar o rechazar la solicitud.

Nuestro personal operativo revisa las transacciones diariamente y verifica que cada usuario haya enviado la documentación solicitada para evitar fraudes.

Esto se hace solicitando al usuario documentación adicional al realizar sus primeras transacciones. Esta documentación es básicamente una imagen del comprobante de pago al lado de su identificación. Esto ayuda a la Empresa a evitar contracargos si un usuario afirma que no ha enviado la transferencia a nuestra cuenta bancaria.

Esta información se registra en el perfil del usuario y está disponible para que cada operador la verifique.

C. Monitoreo de debida diligencia

Actualmente podemos verificar toda la documentación enviada por un usuario simplemente usando nuestro panel de administración, donde podemos ver toda la actividad de dicho usuario.

D. Frecuencia del monitoreo

La documentación enviada por los usuarios como parte de la política de “Conozca a su cliente” debe revisarse al menos 1 cada 2 años.

Las relaciones de alto riesgo requieren un monitoreo intensivo más frecuente. La documentación enviada por clientes de mayor riesgo debe revisarse al menos una vez al año.

Para mantener los documentos actualizados solicitaremos que el cliente complete información extra durante el proceso de verificación.

Se encuentra agregado como parte del proceso de verificación, la solicitud de la fecha de vencimiento de la identificación, de forma tal poder parametrizar la información y recibir alertas cuando un documento venza.

<table>
<tr><th>Procedimientos</th><th>Factor de análisis</th><th>Acción</th><th>Área responsable</th></tr>
<tr><td rowspan="2">Mecanismos recopilación información cliente</td><td>Evaluación al inicio de la relación comercial</td><td rowspan="3">Revisión de los consignados en formulario de vinculación junto con sus documentos complementarios solicitados</td><td rowspan="2">Comercial</td></tr>
<tr><td>Evaluación sobre los cambios de información del cliente</td></tr>
<tr><td rowspan="2">Análisis del perfil operativo</td><td>Análisis actividad económica</td><td rowspan="2">Comercial</td></tr>
<tr><td>Análisis operativo histórica</td><td>Revisión histórica</td></tr>
<tr><td rowspan="2">Análisis del perfil del comportamiento</td><td>Análisis de características propias y habituales</td><td rowspan="3">Monitoreo transaccional a través del análisis de reportes del sistema informático</td><td rowspan="2">Compliance</td></tr>
<tr><td>Análisis de modo de utilización de servicios</td></tr>
<tr><td>Análisis del monitoreo de operaciones</td><td>Análisis de la operatividad del cliente comparando perfil operativo versus perfil del comportamiento</td><td>Compliance</td></tr>
<tr><td>Análisis de operaciones que no guardan relación con el perfil operativo</td><td>Recopilación de mas información, documentación</td><td>Monitoreo transaccional a través del análisis del sistema informático, análisis de coincidencias de listas, análisis de prensa y otros</td><td>Compliance</td></tr>
</table>

RES UIF 49/24 CAPÍTULO IV. MONITOREO, ANÁLISIS Y REPORTE.

ARTÍCULO 33.- Perfil Transaccional.
La información y documentación solicitadas deberán permitir la confección de un perfil transaccional prospectivo (ex ante), sin perjuicio de las calibraciones y ajustes posteriores, de acuerdo con las operaciones efectivamente realizadas. Dicho perfil estará basado en el entendimiento del propósito y la naturaleza esperada de la relación comercial, la información transaccional y la documentación relativa a la situación económica, patrimonial, financiera y tributaria que hubiera proporcionado el Cliente o que hubiera podido obtener el Sujeto Obligado, conforme los procesos de Debida Diligencia que corresponda aplicar en cada caso.

Dicho perfil será determinado en base al análisis de riesgo del Sujeto Obligado de modo tal que permita la detección oportuna de Operaciones Inusuales y Operaciones Sospechosas realizadas por el Cliente.

ARTÍCULO 34.- Monitoreo de la operatoria.

El Sujeto Obligado deberá realizar un monitoreo continuo de la operatoria del cliente y asegurar que sus transacciones sean consistentes con el conocimiento que se tiene del cliente, su perfil y su nivel de riesgo asociado, teniendo en cuenta lo siguiente:

a) Se establecerán reglas de control de operaciones y alertas automatizadas, de tal forma que el Sujeto Obligado pueda monitorear apropiadamente y en forma oportuna la ejecución de operaciones y su adecuación al perfil de sus clientes y su nivel de riesgo asociado.

b) Para el establecimiento de alertas y controles se tomarán en consideración tanto la propia experiencia de negocio, como las tipologías y pautas de orientación que difunda la UIF y/u otros organismos internacionales de los que forme parte la República Argentina relacionados con la prevención de LA/FT/FP, entre ellos deberán valorarse especialmente, las siguientes circunstancias que se describen a mero título enunciativo:

i) La realización de operaciones secuenciales o transferencias de Activos Virtuales simultáneas sin razón económica que lo justifique.

ii) La realización de operaciones o transacciones de los clientes que por su magnitud, habitualidad o periodicidad excedan las prácticas usuales o no guarden relación con su perfil.

iii) Los montos inusualmente elevados, la complejidad y las modalidades no habituales de las operaciones que realicen los clientes.

iv) Cuando transacciones de similar naturaleza, cuantía, modalidad o simultaneidad, hagan presumir que se trata de una operación fraccionada a los efectos de evitar la aplicación de los controles de monitoreo y/o alerta.

v) Cuando los clientes se nieguen a proporcionar información, datos o documentos requeridos por el Sujeto Obligado, con constancia fehaciente de su pedido, o bien cuando se detecte que la información suministrada por los mismos se encuentre alterada, sea o pueda ser apócrifa.

vi) Situaciones en las cuales los Clientes presionen e insistan en que una determinada operación se realice evitando los trámites predefinidos.

vii) Situaciones en las cuales se utilice una cuenta para depositar fondos de terceros.

viii) Situaciones en las cuales se detecta que una persona suplantare, se apoderare o intentare suplantar la identidad de una persona humana medie o no su consentimiento, utilizando los datos de identificación de ésta.

ix) Toma de conocimiento que indican que un cliente está siendo investigado o procesado por delitos de LA/FT/FP, u otros relacionados.

x) Triangulación de transferencias de Activos Virtuales entre el Cliente, sus familiares, sociedades y terceros relacionados sin justificación económica.

xi) Operaciones de volumen elevado de personas situadas en la Zona de Seguridad de Fronteras establecidas por el Decreto N° 253/18, que no guarden relación con las prácticas usuales.

xii) Cuando existan operaciones de distintas cuentas asociadas o vinculadas con un mismo dispositivo electrónico o cuando exista una cuenta asociada a varios dispositivos electrónicos, sin justificación de dicha situación.

xiii) Cuando existieran operaciones inconsistentes con las prácticas habituales, teniendo en especial consideración si su actividad principal está vinculada con la operatoria "off shore" y/o con países determinados como de baja o nula tributación por las autoridades competentes.

xiv) Las solicitudes de Clientes donde el origen de los fondos, bienes u otros activos no está claro o no es consistente con el tipo de actividad declarada.

xv) La utilización de cuentas con reducida o nula actividad que transaccionen altos volúmenes en un corto período de tiempo.

xvi) Operatoria con Activos Virtuales que traten de impedir su trazabilidad u obtener mayor anonimato.

xvii) Operaciones de clientes relacionadas a cuentas con exposición a sitios identificados como de alto riesgo en herramientas de trazabilidad.

xviii) Situaciones de las que, mediante la combinación parcial de algunas pautas establecidas en los incisos precedentes u otros indicios, pudiera presumirse la configuración de conductas que excedan los parámetros normales y habituales de la actividad considerada.

c) Los parámetros aplicados a los sistemas de monitoreo implementados tendrán carácter de confidencial excepto para quienes actúen en el proceso de monitoreo, control, revisión, diseño y programación de los mismos y aquellas personas que los asistan en el cumplimiento de sus funciones. La metodología de determinación de reglas y de parámetros de monitoreo deberá estar documentada.

d) Los organismos nacionales, provinciales, municipales, entes autárquicos y toda otra persona jurídica de carácter público, no se encuentran exentos del monitoreo por parte del Sujeto Obligado, el cual se realizará en función del riesgo que éstos y sus operaciones presenten, con foco especial en el destino de los fondos. En tal sentido, se deberá prestar especial atención a aquellas operaciones cuyo destinatario no sea también un Organismo o Ente de carácter público, o impliquen retiros de dinero en efectivo significativos o que los retiros se efectúen de manera fraccionada con el aparente propósito de evitar los controles de monitoreo y/o alerta.

Serán objeto de análisis todas las Operaciones Inusuales. El Sujeto Obligado deberá profundizar el análisis de Operaciones Inusuales con el fin de obtener información adicional, en caso de ser necesario, que corrobore o revierta la/s inusualidad/es detectada/s, procediendo, en caso de corresponder, a la actualización de la información del cliente y de su perfil.

ARTÍCULO 35.- Registro de Operaciones Inusuales.

El Sujeto Obligado deberá llevar un Registro de todas las Operaciones Inusuales, en el cual constarán como mínimo, los siguientes datos:

a) Denominación y nivel de riesgo asociado al cliente.

b) perfil del cliente.

c) identificación de la operación y/o transacción (producto y monto operado).

d) fecha, hora y procedencia de la alerta u otro sistema de identificación de la operación y/o transacción a analizar.

e) tipo de inusualidad (descripción).

f) analista encargado del estudio.

g) medidas llevadas a cabo para la resolución de la alerta.

h) fecha y decisión final motivada.

Se deberá conservar el soporte documental de tal registro, de conformidad con las reglas previstas en la presente.

ARTÍCULO 36.- Reportes de Operaciones Sospechosas.

Cada Sujeto Obligado deberá reportar las Operaciones Sospechosas a la UIF. Los reportes deberán:

a) Incluir el detalle de todos los datos y documentos que permitan a la UIF utilizar apropiadamente dicha información. Los reportes serán realizados en las condiciones técnicas previstas en la resolución UIF vigente en la materia; con entrega o puesta a disposición del referido Organismo de todos los documentos o informaciones de soporte que justifiquen la decisión de reporte.

b) Estar fundados y contener una descripción de las razones y/o inusualidades por las cuales el Sujeto Obligado considera que la/s operación/es presenta/n tal carácter.

c) Enviarse a la UIF, una vez analizada la/s operación/es, sin demora alguna, contando con un plazo de:

i. VEINTICUATRO (24) HORAS, computadas a partir de la fecha en que el Sujeto Obligado concluya que la operación reviste tal carácter en los casos de Lavado de Activos. Asimismo, la fecha de reporte no podrá superar los NOVENTA (90) días corridos contados desde la fecha en que la Operación Sospechosa de Lavado de Activos fue realizada o tentada.

ii. VEINTICUATRO (24) HORAS, computadas a partir de la fecha de la operación realizada o tentada en los casos de Financiación de Terrorismo.

iii. VEINTICUATRO (24) HORAS, computadas a partir de la fecha de la operación realizada o tentada en los casos de Financiamiento de la Proliferación de Armas de Destrucción Masiva.

d) Ser confidenciales, por lo que no podrán ser exhibidos a los revisores externos independientes ni a los organismos de control de la actividad, excepto en los casos en que la CNV actúe en algún procedimiento de supervisión in situ, en el marco de la colaboración que ese organismo de contralor específico preste a esta UIF. En tales circunstancias, tanto el Sujeto Obligado como la CNV deberán garantizar la confidencialidad de la información y su cadena de custodia.

Sin perjuicio de ello, los revisores externos independientes, podrán acceder a la información necesaria para evaluar el funcionamiento del sistema de monitoreo y alertas, y los procedimientos de análisis de Operaciones Inusuales y Operaciones Sospechosas. La información proporcionada deberá omitir todo contenido que posibilite identificar a los involucrados en las operaciones.

CAPÍTULO V. OTRAS REGLAS.

ARTÍCULO 37.- Información de Transferencias de Activos Virtuales ***entre PSAV****.*

Los Sujetos Obligados deberán cumplir con la identificación del ordenante y del beneficiario de las transacciones alcanzadas por la regla de viaje, en los términos establecidos por los Estándares Internacionales del Grupo de Acción Financiera Internacional y en la modalidad que la UIF establezca para el intercambio y la validación de dicha información.

ARTÍCULO 38.- ***Depósitos en efectivo.***

Cada Sujeto Obligado deberá establecer un seguimiento reforzado sobre los depósitos que se realicen en efectivo.

En tal sentido, en aquellos depósitos por importes iguales o superiores a SEIS (6) Salarios Mínimos, Vitales y Móviles, los Sujetos Obligados deberán identificar a la persona que efectúe la operación, en los términos establecidos en la presente Resolución, requiriéndole información y dejando constancia de ello, si es realizada por sí o por cuenta de un tercero, en cuyo caso, se procederá a recabar el nombre completo y/o denominación social de este último, y el número de documento o clave de identificación fiscal (CUIT, CUIL o CDI), según corresponda.

Aquellas operaciones que se realicen utilizando algún medio de identificación con clave provisto previamente por el Sujeto Obligado al depositante, tales como tarjetas magnéticas, o los efectuados en cuentas recaudadoras, quedarán exceptuados del procedimiento de identificación de la persona que lo efectúa, debiendo no obstante registrarse por cuenta de quién es efectuada la transacción.

Cada Sujeto Obligado deberá tomar medidas tendientes a mitigar los riesgos de aquellas actividades que operen altos volúmenes de dinero en efectivo a fin de aplicar medidas de Debida Diligencia Reforzada en caso que el Sujeto Obligado lo estime necesario en base a su análisis de riesgo.

8. Cruce de listas

El Oficial de Cumplimiento deberá utilizar el siguiente insumo para el cruce de listas Nacionales e Internacionales, dejando evidencia documentada de la validación.

El departamento de Cumplimiento asegurará el monitoreo y actualización de las listas. Para ello se acompaña anexo con el listado de listas y circulares controladas a través de los servicios de Neitcom.

CUADRO DE LISTAS

Del Procedimientos de cruce de listas

Mensualmente el área de Cumplimiento alimentará en el sistema transaccional de la compañía las listas publicas y demás listas negras que las entidades tanto nacionales como internacionales proporcionen a través de sus sitios oficiales a fin de contar con alertas automáticas que permitan la debida diligencia y toma de decisiones oportunas en casos de coincidencias.

Una vez obtenida las coincidencias se elaborará un análisis transaccional que permitirá detectar posibles inusualidades, estos resultados serán elevados al oficial de cumplimiento para la toma de decisiones o resoluciones que devengan de este.

Prevención delitos cambiarios

A nivel nacional se procede a la verificación de clientes con operaciones asociadas a exportaciones e importaciones e incumplimiento de regulación penal cambiaria, confrontando contra listas de exportadores e importadores del BCRA, CANCILLERIA y/o AFIP, ello como Incorporación de plan para controles en materia cambiaria.

Procedimiento para el Reporte de coincidencias de listas OFAC

En cumplimiento a lo dispuesto cualquier coincidencia con listas OFAC, será reportada de forma inmediata a la Unidad de Información Financiera, a través del formulario de ONLINE UIF, dicho formulario será instrumentado por el área de Cumplimiento de la compañía y suscrito por el Representante Legal.

Tipo de lista	Tipo de Control	Frecuencia cruce	Frecuencia de monitoreo
OFAC	Automático y/o Manual	Verificación	Diario
ONU	.. ..	Verificación	Diario
Capturas	.. ..	Verificación	Diario
Datos personales	.. ..	Requerimiento	Diario
Listas de terrorismo oficiales *	.. ..	Verificación	Diario
Informes comerciales	.. ..	Requerimiento	Diario
PEPs y jefes de gobierno mundiales	.. ..	Verificación	Diario

***** Incluye: Lista de Organización de las Naciones Unidas - Bank of England Sanctions List - Los más Buscados por Interpol - Lista de los Terroristas más buscados por el FBI - OSFI - Canadian Sanctions List - Policía Federal Argentina Buscados - Lista de Fugitivos de la agencia DEA - BCRA y Ministerio de relaciones exteriores comercio internacional culto (•) - entre otras.

- https://www.cancilleria.gob.ar/es/argentinatradenet/directorio-de-exportadores - **Directorio de exportadores.**
- http://www.bcra.gov.ar/SistemasFinancierosYdePagos/Registro_exportadores_importadores.as - **Registro de información cambiaria de exportadores e importadores de bienes.**

Se acompaña anexo brindado por Neitcom con la totalidad de listas y circulares.

9. Capacitación:

La Unidad de Cumplimiento, deberá diseñar programas y coordinar planes de capacitación sobre prevención de lavado de activos, financiamiento del terrorismo y otros delitos para todo el personal. Tales programas deberán cumplir con las condiciones descriptas en la Resolución UIF 49/24.

ARTÍCULO 18.- Capacitación.

Los Sujetos Obligados deberán contar con un plan de capacitación anual el cual debe contar con un enfoque específico en la materia con la finalidad instruir a su personal sobre las normas regulatorias de LA/FT/FP vigentes, así como respecto a las políticas, procedimientos y controles del Sistema de Prevención de LA/FT/FP y su adecuada implementación a los fines de administrar y mitigar eficazmente los riesgos identificados.

Todos los directores, gerentes, empleados y colaboradores del Sujeto Obligado serán incluidos en dicho plan de capacitación, considerando la exposición a los riesgos de LA/FT/FP, de acuerdo con sus funciones y/o tareas.

La capacitación en materia de prevención de LA/FT/FP deberá ser continua, actualizada y complementarse con la información relevante que transmita la UIF.

Los empleados del Sujeto Obligado, tengan o no contacto directo con los clientes, deberán recibir formación genérica y formación específica en materia de prevención de LA/FT/FP en relación con sus funciones y/o tareas desarrolladas, y a la adecuada implementación de las políticas, y procedimientos y controles del Sistema de Prevención de LA/FT/FP.

El Oficial de Cumplimiento titular y suplente, así como también los empleados y colaboradores del área a su cargo, deberán ser objeto de una formación de mayor profundidad y con contenidos especialmente ajustados a sus funciones y/o tareas.

Los directores, gerentes y empleados que se incorporen al Sujeto Obligado deberán recibir una capacitación sobre los alcances del Sistema de Prevención de LA/FT/FP que se encuentra en marcha, de acuerdo con las funciones que les correspondan, en un plazo máximo de SESENTA (60) días hábiles a contar desde la fecha de su ingreso.

Cada Sujeto Obligado deberá reservar la constancia de las capacitaciones recibidas y llevadas a cabo, y de las evaluaciones efectuadas al efecto, que deberán encontrarse a disposición de la UIF y de la CNV.

El plan de capacitación deberá comprender, como mínimo, los siguientes temas:

a) Definición de los delitos de LA/FT/FP.

b) Normativa nacional y estándares internacionales vigentes sobre prevención de LA/FT/FP.

c) Políticas, procedimientos y controles del Sistema de Prevención de LA/FT/FP del Sujeto Obligado, su adecuada implementación a los fines de la administración y mitigación de los riesgos de LA/FT/FP, enfatizando en temas específicos tales como la Debida Diligencia.

d) Riesgos de LA/FT/FP a los que se encuentra expuesto el Sujeto Obligado, conforme el propio informe técnico de autoevaluación de riesgos, las Evaluaciones Nacionales de Riesgos de LA/FT/FP, sus actualizaciones y otros documentos en los que se identifiquen riesgos vinculados con el sector que resulten pertinentes.

e) Tipologías o tendencias de LA/FT/FP detectadas por el Sujeto Obligado, y las difundidas por la UIF, el GAFI o el Grupo de Acción Financiera de Latinoamérica (GAFILAT).

f) Alertas y controles para detectar Operaciones Inusuales, y los procedimientos de determinación y comunicación de Operaciones Sospechosas, enfatizando en el deber de confidencialidad del reporte.

g) Roles y responsabilidades del personal en materia de prevención de LA/FT/FP del Sujeto Obligado.

Tipo de Empleados	Tipo de Capacitación	Alcance	Metodología	Frecuencia	Evaluación	Metodología de Evaluación
Empleados Nuevos	Prevención Lavado de Activos, Financiamiento del Terrorismo y Código de Ética	A todos los empleados nuevos	Presencial	Al momento de su vinculación	Escrita	Preguntas de selección múltiple, con una nota mínima de 70/100, caso contrario se somete a repetir el examen.
Empleados vigentes		A todos los colaboradores	Presencial / On line	Anual	Escrita / On line	

10. Procedimientos de reportes Internos

Es responsabilidad de cualquier colaborador de la Compañía, reportar al Oficial de Cumplimiento, cualquier operación inusual de acuerdo a los parámetros establecidos por las normativas vigentes en la materia, y por las señales de alerta definidas por la Compañía, a través de correo electrónico junto con los documentos de soporte que correspondan. Una vez recibida la información por parte del Oficial de Cumplimiento, será analizada y evaluada para posterior reporte de los casos que corresponda al Comité de Cumplimiento.

11. Reporte Externo

El Oficial de Cumplimiento principal o suplente, deberán remitir a la UIF los siguientes tipos de reporte: **Reporte de Operaciones Sospechosas**.

La Ley de Prevención, Detección del Delito de Lavado de Activos y del Financiamiento de Delitos, se entenderá por operaciones o transacciones económicas inusuales, injustificadas o sospechosas, los movimientos económicos, realizados por personas naturales o jurídicas, que no guarden correspondencia con el perfil económico y financiero que éstas han mantenido en la entidad reportarte y que no puedan sustentarse.

12. Plazo para el reporte

i. VEINTICUATRO (24) HORAS, computadas a partir de la fecha en que el Sujeto Obligado concluya que la operación reviste tal carácter en los casos de Lavado de Activos. Asimismo, la fecha de reporte no podrá superar los NOVENTA (90) días corridos contados desde la fecha en que la Operación Sospechosa de Lavado de Activos fue realizada o tentada.

ii. VEINTICUATRO (24) HORAS, computadas a partir de la fecha de la operación realizada o tentada en los casos de Financiación de Terrorismo.

iii. VEINTICUATRO (24) HORAS, computadas a partir de la fecha de la operación realizada o tentada en los casos de Financiamiento de la Proliferación de Armas de Destrucción Masiva.

13. Confidencialidad

CONFIDENCIALIDAD DEL REPORTE

Los Reportes de Operaciones Sospechosas, no podrán ser exhibidos a los clientes ni a terceras personas, conforme a lo dispuesto en el artículo 21 inciso c. y 22 de la Ley Nº 25.246 y sus modificatorias; y sólo podrán exhibirse a los correspondientes Organismos de Fiscalización y Control cuando actúen en algún procedimiento de supervisión, fiscalización e inspección in situ, en el marco de la colaboración que esos Organismos de Contralor deben prestar a esta UNIDAD DE INFORMACIÓN FINANCIERA, en los términos del artículo 14 inciso 7. de la Ley Nº 25.246 y sus modificatorias.

d) Ser confidenciales, por lo que no podrán ser exhibidos a los revisores externos independientes ni a los organismos de control de la actividad, excepto en los casos en que la CNV actúe en algún procedimiento de supervisión in situ, en el marco de la colaboración que ese organismo de contralor específico preste a esta UIF. En tales circunstancias, tanto el Sujeto Obligado como la CNV deberán garantizar la confidencialidad de la información y su cadena de custodia.

Sin perjuicio de ello, los revisores externos independientes, podrán acceder a la información necesaria para evaluar el funcionamiento del sistema de monitoreo y alertas, y los procedimientos de análisis de Operaciones Inusuales y Operaciones Sospechosas. La información proporcionada deberá omitir todo contenido que posibilite identificar a los involucrados en las operaciones.

14. Multas por sanciones administrativas

LEY 25.246

ARTICULO 23. —
1. Será sancionado con multa de cinco (5) a veinte (20) veces del valor de los bienes objeto del delito, la persona jurídica cuyo órgano ejecutor hubiera recolectado o provisto bienes o dinero, cualquiera sea su valor, con conocimiento de que serán utilizados por algún miembro de una asociación ilícita terrorista, en el sentido del artículo 213 quáter del Código Penal.

Cuando el hecho hubiera sido cometido por temeridad o imprudencia grave del órgano o ejecutor de una persona jurídica o por varios órganos o ejecutores suyos, la multa a la persona jurídica será del veinte por ciento (20%) al sesenta por ciento (60%) del valor de los bienes objeto del delito.

2. Cuando el órgano o ejecutor de una persona jurídica hubiera cometido en ese carácter el delito a que se refiere el artículo 22 de esta ley, la persona jurídica será pasible de multa de cincuenta mil pesos ($ 50.000) a quinientos mil pesos ($ 500.000).
(Artículo sustituido por art. 18 de la Ley Nº 26.683 B.O. 21/06/2011)

ARTICULO 24. —
1. La persona que actuando como órgano o ejecutor de una persona jurídica o la persona de existencia visible que incumpla alguna de las obligaciones ante la Unidad de Información Financiera (UIF) creada por esta ley, será sancionada con pena de multa de una (1) a diez (10) veces del valor total de los bienes u operación a los que se refiera la infracción, siempre y cuando el hecho no constituya un delito más grave.

2. La misma sanción será aplicable a la persona jurídica en cuyo organismo se desempeñare el sujeto infractor.

3. Cuando no se pueda establecer el valor real de los bienes, la multa será de diez mil pesos ($ 10.000) a cien mil pesos ($100.000).

15. Reserva de documentación

En cumplimiento a la norma de prevención vigente, Los accionistas, miembros del directorio, ejecutivos, funcionarios y empleados, representantes legales, contralores, auditores externos, apoderados, asesores, así como las personas naturales y jurídicas no podrán dar a conocer a persona no autorizada y en especial a las personas que hayan efectuado o intenten efectuar operaciones inusuales e injustificadas, que se ha comunicado sobre dichas operaciones a las autoridades competentes y guardarán absoluta reserva al respecto.

Igualmente, quedan prohibidos de poner en conocimiento de clientes o personas no autorizadas los requerimientos de información realizados por autoridad competente o que dicha información ha sido proporcionada.

El no cumplimiento a esta disposición, obliga al funcionario o empleado que conozca de ella a llevarla a conocimiento del oficial de cumplimiento, quién a su vez, previo análisis, comunicará el hecho al comité de cumplimiento, organismo que dará a esta información el mismo tratamiento que a un reporte de operación inusual e injustificada, informando los nombres de los funcionarios o empleados que hubieran transgredido esta prohibición.

16. Comité de Prevención AML

Mensualmente y cada vez que los integrantes lo comuniquen, el Comité deberá reunirse para el tratamiento de cuestiones relacionadas a la temática Prevención de Lavado de Dinero y Financiamiento del Terrorismo.

Los temas que se traten, como lo resuelto deberá hacerse constar en su correspondiente Acta.

17. Revisión externa independiente / Auditoría externa e interna

Además del Proceso de Autoevaluación aludido anteriormente, el artículo 19 de la Resolución UIF 49/24 establece acciones de “Revisión Externa Independiente”/”Auditoría Externa”.

Bianualmente, y en cumplimiento de lo requerido por el mismo, se procederá a la contratación de un R.E.I. en los términos dispuestos a continuación por la UIF N° 67 E/2017 o aquellas que la modifiquen, complementen o sustituyan.

El R.E.I., dentro de los CIENTO VEINTE (120) días corridos desde el plazo establecido para el envío del “Informe Técnico” de la Autoevaluación de Riesgos (30 de abril de cada año), deberá emitir un informe sobre la calidad y eficacia del Sistema de PLA y FT aplicado por Vita Digital S.R.L.

ARTÍCULO 19.- Evaluación del Sistema de Prevención de LA/FT/FP.

La evaluación del Sistema de Prevención de LA/FT/FP se llevará a cabo en dos niveles, a saber:

a) Revisión externa independiente: se encontrará a cargo de un revisor externo independiente designado de conformidad con la Resolución UIF vigente en la materia, quien deberá emitir un informe anual en el que se pronuncie sobre la calidad y efectividad del Sistema de Prevención de LA/FT/FP del Sujeto Obligado, y comunicar los resultados en forma electrónica a la UIF dentro de los CIENTO VEINTE (120) días corridos contados desde el vencimiento del plazo establecido para el envío de la autoevaluación.

b) Auditoría interna: la auditoría interna del Sujeto Obligado deberá incluir en sus programas anuales las áreas relacionadas con el Sistema de Prevención de LA/FT/FP, sin perjuicio de las revisiones externas que correspondan. El Oficial de Cumplimiento tomará conocimiento de los mismos, sin poder participar en las decisiones sobre el alcance y las características de dichos programas anuales.

Los resultados obtenidos de las revisiones indicadas en los incisos a) y b) anteriores, deberán incluir la identificación de deficiencias, la descripción de mejoras a aplicar y los plazos para su implementación y serán puestos en conocimiento del Oficial de Cumplimiento, quien deberá notificar debidamente de ello al órgano de administración o máxima autoridad del Sujeto Obligado.

La claridad del artículo transcripto, exime cualquier tipo de explicación al respecto, por lo que Vita tiene en cuenta sus exigencias y la necesidad de su fiel cumplimiento.

AUDITORÍA Y PROCEDIMIENTOS DE CONTROL INTERNO

Se realizará una Auditoría Interna anual para evaluar el cumplimiento de las obligaciones vinculadas a la PLA y FT.

La auditoría interna analiza el cumplimiento efectivo de los procedimientos y políticas de PLA y FT.

Para llevar a cabo su labor, la Auditoría Interna realiza un relevamiento sobre las actividades que efectúan las áreas y personas involucradas, y sobre el cumplimiento de sus obligaciones, como ser, el conocimiento adecuado de los Clientes cuando se dan de alta, la determinación del “Perfil Transaccional” de los mismos, el monitoreo de las Operaciones, el sistema de alertas, el análisis de las Operaciones Inusuales y el procedimiento llevado a cabo en caso de advertirse una Operación Inusual hasta llegar a la confirmación o no de una sospecha en los términos del artículo 21, inciso b, de la LLA.

Los resultados que arrojen los procedimientos de auditoría serán comunicados al O.C.

En el caso de que se detecten deficiencias sobre la implementación y cumplimiento de las políticas de PLAyFT, se adoptarán las medidas necesarias para corregirlas.

18. Congelamiento administrativo de bienes o dinero

Vita dará cumplimiento a lo exigido en los artículos 3, 4, 10 y 11 de la Resolución UIF No 29/2013 que a continuación se transcriben:

“Capítulo II. Congelamiento administrativo de bienes o dinero relativo a personas físicas o jurídicas o entidades designadas por el Consejo de Seguridad de las Naciones Unidas de conformidad con la resolución 1267 (1999) y sus sucesivas, previo al RFT.

Artículo 3.- Cuando se verifique alguna de las circunstancias expuestas en el artículo 1 incisos a), b) o c) de la Resolución UIF No 29/2013,se procederá de conformidad con lo establecido en el artículo 9° del Decreto No 918/12.*

**Decreto No 918/2012, Art. 9o — SUJETOS OBLIGADOS CORRESPONDIENTES A LOS SECTORES 1 BANCARIO, CAMBIARIO, DEL MERCADO DE CAPITALES Y DE SEGUROS. Los sujetos obligados correspondientes a los sectores bancario, cambiario, del mercado de capitales y de seguros, deberán verificar el listado de personas físicas o jurídicas o entidades designadas por el Consejo de Seguridad de las Naciones Unidas de conformidad con la Resolución 1267 (1999) y sus sucesivas actualizaciones. En el supuesto de verificar que un cliente se encuentre incluido en el referido listado, los mencionados sujetos obligados deberán efectuar, en el acto e inaudita parte, el congelamiento de los bienes o dinero involucrados en las operaciones cuando se verifique alguna de las circunstancias expuestas en el artículo 3o del presente. Asimismo, deberán informar, inmediatamente, a la UNIDAD DE INFORMACIÓN FINANCIERA (UiF) la aplicación de la medida de congelamiento y emitir, sin demora alguna, un Reporte de Operación Sospechosa de Financiación del Terrorismo.*

“Capítulo III. Congelamiento administrativo de bienes o dinero dispuesto por la UIF respecto de personas físicas o jurídicas o entidades designadas por el consejo de seguridad de las Naciones Unidas de conformidad con la Resolución 1267 (1999) y sussucesivas, o vinculadas con las acciones delictivas previstas en el artículo 306 del Código Penal.
Artículo 4.- Recibida la notificación de la resolución de la UIF que dispone el congelamiento administrativo de bienes o dinero,se procederá de la siguiente forma:

a) Congelar todo bien, dinero o crédito que fuese propiedad de las personas físicas o jurídicas o entidades sobre las cuales se ha dictado el congelamiento administrativo, o cuyo destinatario o beneficiario sea una de las mencionadas personas;

b) Informar los resultados de la aplicación de la resolución que dispuso el congelamiento administrativo, dentro de las VEINTICUATRO (24) horas de notificada,sólo en los casos en que se hayan congelado bienes, dinero o créditos;

c) Cotejar las bases de Clientes a los efectos de informarsi ha realizado Operaciones con las personasfísicas o jurídicas o entidadessobre las que hubiera recaído la medida de congelamiento administrativo;

d) A los efectos indicados en los puntos a) y b) precedentes, Vita utilizará elsistema denominado 'Reporte Orden de Congelamiento', implementado por la UIF al efecto;

e) Congelar asimismo, en los términos del punto a) precedente, todo bien, dinero o crédito que pudiera ser detectado, ingresado, recibido, etc., con posterioridad a la notificación de la medida de congelamiento y durante la vigencia de la resolución de la UIF que dispuso el congelamiento;

f) En elsupuesto previsto en el apartado e) precedente,se procederá conforme lo indicado en el punto d); y

g) Abstenerse de informar a sus Clientes o a terceros los antecedentes de la resolución que dispusiere el congelamiento administrativo de bienes, dinero o créditos. En todo caso, solo se indicará que los mismosse encuentran congelados en virtud de lo dispuesto en el artículo 6° de la Ley No 26.734, en el Decreto No 918/12 y en la resolución de la UIF que haya dispuesto el congelamiento."

"Artículo 10.- La resolución que disponga el congelamiento administrativo de bienes o dinero podrá disponer medidas adicionales, a las indicadas en los artículos precedentes, que deberán cumplimentar los Sujetos Obligados de acuerdo a las particularidades de cada caso".

"Artículo 11.- En los casos que la resolución que disponga el congelamiento administrativo de bienes o dinero se hubiera motivado en alguna de las circunstancias expuestas en el artículo 1° inciso 1) de la presente, la misma regirá mientras las personasfísicas o jurídicas o entidades designadas por el CONSEJO DE SEGURIDAD DE LAS NACIONES UNIDAS de conformidad con la Resolución 1267 (1999) y sus sucesivas, permanezca en el citado listado, o hasta tanto sea revocada judicialmente.

Si la resolución que dispone el congelamiento administrativo de bienes o dinero se hubiera motivado en alguna de las circunstancias expuestas en el artículo 1° inciso 2) de la presente, la medida se ordenará por un plazo no mayor a SEIS (6) meses prorrogable por igual término, por única vez. Cumplido el plazo, y de no mediar resolución judicial en contrario, el congelamiento cesará. Si la medida fuera prorrogada por esta Unidad, o revocada o rectificada judicialmente, esta UNIDAD DE INFORMACIÓN FINANCIERA notificará talsituación a los Sujetos Obligados."

Asimismo, con relación a lo que compete al congelamiento administrativo de bienes y dinero que disponga la UIF, Vita tendrá presente también lo expresado en el Decreto No 918/2012, esencialmente lo indicado en los artículos 2 y 6, que a continuación se transcriben:

"Artículo 2. — DEFINICIONES. A los efectos de la presente norma,se entenderá por:

a) Congelamiento administrativo: la inmovilización de los bienes o dinero, entendida como la prohibición de transferencia, conversión, disposición o movimiento de dinero u otros bienes.

b) Bienes o dinero: bienes, fondos o activos, cualquiera sea su naturaleza, procedencia y forma de adquisición, así como los documentos o instrumentos que sean constancia de su titularidad o de un interéssobre esos bienes, fondos o activos —de conformidad a lo establecido en el artículo 1.1 del CONVENIO INTERNACIONAL PARA LA REPRESION DE LA FINANCIACIÓN DEL TERRORISMO (Ley No 26.024)— y los intereses, dividendos o cualquier otro valor o ingreso que se devengue o sea generado por esos bienes, fondos o activos; siempre que íntegra o conjuntamente sean propiedad o estén bajo control, directa o indirectamente, de personas o grupos designados por el Consejo de Seguridad de las Naciones Unidas de conformidad con la Resolución 1267 (1999) y sus sucesivas o que puedan estar vinculados a las acciones delictivas previstas en el artículo 306 del CODIGO PENAL.

c) Sujetos obligados: las personas físicas o jurídicas enumeradas en el artículo 20 de la Ley No 25.246 y sus modificatorias".

"Artículo 6. — NOTIFICACIÓN DE LA RESOLUCIÓN QUE DISPONE EL CONGELAMIENTO ADMINISTRATIVO. La UNIDAD DE INFORMACIÓN FINANCIERA (UIF) procederá a notificar inmediatamente alsujeto obligado la Resolución que disponga el congelamiento administrativo, a través de alguno de lossiguientes medios:

a) Notificación por vía electrónica: La Resolución se comunicará alsujeto obligado mediante correo electrónico dirigido a la dirección denunciada al momento de su inscripción ante la UNIDAD DE INFORMACIÓN FINANCIERA (UIF). b) Notificación personal.

c) Notificación mediante cédula o telegrama.

d) Cualquier otro medio de notificación fehaciente."

PROCEDIMIENTO DE CONGELAMIENTO – Decreto No 918/2012

Conforme lo dispuesto por el Decreto N° 918/2012, el procedimiento de congelamiento resultará el siguiente:

- Recibido el pedido de congelamiento, el O.C. lo remitirá a la Gerencia de Operaciones , para que proceda a verificar los números de DNI/CUIL/CUIT contra la base de Clientes.

- Realizada la verificación correspondiente, y de resultar negativa, se procederá a registrar electrónicamente la consulta realizada, la cual contendrá el DNI/CUIL/CUIT consultado, y el resultante registro de devolución efectuado bajo la leyenda de -No se pudo encontrar un Usuario que coincida con los datos ingresados-;

- Por cada resolución se conformará una carpeta digital y en ella se conservarán tanto las verificaciones realizadas como la misma notificación;

- La resolución también se imprimirá y se archivará en una carpeta física donde se resguardarán;

- En caso de que la búsqueda arrojase un resultado positivo, la Gerencia de Operaciones procederá a remitir un correo al O.C. informándolo de tal circunstancia para que este notifique a la UIF dentro del plazo establecido por la normativa vigente;

- Al mismo tiempo, y sin solución de continuidad, la Gerencia de Operaciones requerirá a la Gerencia que proceda, al inmediato bloqueo operativo del Cliente;
- Las medidas procederán durante el periodo de vigencia que marque la resolución respectiva;

- En caso de que la UIF envíe algún tipo de indicación o tarea a cumplir, se procederá de forma inmediata a su ejecución;

- La resolución se cargará dentro del sistema de “Altas” para que quien estuviese informado requiriese una tarjeta o intentase adherir un establecimiento al sistema no pueda hacerlo; y

- Las resoluciones se cargarán por el periodo requerido dándose de baja de forma automática a su vencimiento, salvo que se recibiese un periodo de prórroga.

Ante dicha notificación por parte la UIF, Vita procederá a congelar los fondos -sean representados por moneda fiduciaria (pesos argentinos) o por activos virtuales- de la cuenta de la persona física o jurídica implicada en el lavado de activos. A tal efecto, dichos fondos serán transferidos a la cuenta bancaria o billetera controlada por el juzgado que fuere indicada a través de la correspondiente resolución.

Asimismo, cuando sea procedente la UIF ordenará al Banco Central de la República Argentina, a la Superintendencia de Seguros de la Nación, a la Comisión Nacional de Valores y a los registros correspondientes y/o a los organismos que resulten competentes, el congelamiento administrativo de todos los activos vinculados a las acciones delictivas previstas en los artículos 305 y 306 del CP.

19. Política de contratación empleados

La Entidad ha adoptado sistemas adecuados de preselección para asegurar normas estrictas de contratación de empleados y de monitoreo de su comportamiento, proporcionales al riesgo vinculado con las tareas que los empleados lleven a cabo, conservando constancia documental de la realización de tales controles.

Vita cuenta con un área específica de Recursos Humanos la que ha adoptado una adecuada política de reclutamiento o contratación de personal, para ocupar puestos directamente relacionados con o vinculados a la apertura de cuentas y realización de operaciones, estará orientado a asegurar que el personal cuente con la integridad y capacidades necesarias para el correcto desempeño de sus labores.

El proceso de búsqueda y selección de personal comprenderá la verificación de las calificaciones, experiencia, referencias y membresías a cuerpos profesionales de los postulantes o interesados en el puesto, como así también sus antecedentes penales o criminales.

En particular, se valorará si los postulantes o interesados registran antecedentes en relación con actividades de prevención lavado de activos, financiación del terrorismo o delitos de naturaleza económica.

20. Política de evaluación de activos virtuales

Para poder detectar de modo más eficiente los riesgos que involucra la operatoria con cripto activos, es necesario definir algunos términos de los mecanismos que implican un riesgo en la materia. Las monedas virtuales descentralizadas (también conocidas como criptomonedas) se distribuyen, son de código abierto, monedas virtuales peer-to-peer basadas en matemáticas que no tienen una autoridad administrativa central y no tienen monitoreo o supervisión central. Ejemplos, son las monedas ofrecidas para su compra-venta a través de la plataforma de Vita: Bitcoin (BTC), Ether (ETH), Litecoin (LTC), Ripple (XRP), Bitcoin Cash (BCH), entre otras.

Entonces, entendemos que Criptomoneda se refiere a una moneda virtual convertible descentralizada basada en matemáticas que está protegida por criptografía, es decir, incorpora principios de criptografía para implementar una economía de información distribuida, descentralizada y segura. La criptomoneda se basa en claves públicas y privadas para transferir valor de una persona (individuo o entidad) a otra, y debe firmarse criptográficamente cada vez que se transfiere. La seguridad, la integridad y el equilibrio de los libros de contabilidad de criptomonedas están garantizados por una red de partes que desconfían mutuamente (en Bitcoin, denominados mineros) que protegen la red a cambio de la oportunidad de obtener una tarifa distribuida aleatoriamente (en Bitcoin, una pequeña cantidad de bitcoins recién creados, llamados "recompensa de bloque" y, en algunos casos, también tarifas de transacción pagadas por los usuarios como incentivo para que los mineros incluyan sus transacciones en el siguiente bloque). Se han definido cientos de especificaciones de criptomonedas, en su mayoría derivadas de Bitcoin, que utiliza un sistema de prueba de trabajo para validar transacciones y mantener la cadena de bloques. Si bien Bitcoin proporcionó el primer protocolo de criptomoneda completamente implementado, existe un interés creciente en desarrollar métodos de prueba alternativos y potencialmente más eficientes, como los sistemas basados en prueba de participación.

Anonimizador (herramienta de anonimización) se refiere a herramientas y servicios, como redes oscuras y mezcladores, diseñado para ocultar la fuente de una transacción de Bitcoin y facilitar el anonimato. (Ejemplos: Tor (darknet); Dark Wallet (darknet); Bitcoin Laundry (mixer).

Mixer (herramienta de lavado de activos, tumbler) es un tipo de anonimizador que oscurece la cadena de transacciones en la cadena de bloques al vincular todas las transacciones en la misma dirección de bitcoin y enviarlas juntas de manera que parezca que se enviaron desde otra dirección. Un mezclador o tumbler envía transacciones a través de una serie compleja y semialeatoria de transacciones ficticias que hace que sea extremadamente difícil vincular monedas virtuales específicas (direcciones) con una transacción en particular. Los servicios de mezclador funcionan al recibir instrucciones de un usuario para enviar fondos a una dirección de bitcoin en particular. Luego, el servicio de mezcla "combina" esta transacción con otras transacciones del usuario, de modo que no queda claro a quién pretendía el usuario que se dirigieran los fondos. (Ejemplos: Bitmixer.io; SharedCoin; Blockchain.info; Bitcoin Laundry; Bitlaunder; Easycoin).

Tor (originalmente, The Onion Router) es una red subterránea distribuida de computadoras en el Internet que oculta las verdaderas direcciones IP y, por lo tanto, las identidades de los usuarios de la red, al enrutar comunicaciones/transacciones a través de múltiples computadoras en todo el mundo y envolverlas en numerosas capas de cifrado. Tor hace que sea muy difícil ubicar físicamente las computadoras que alojan o acceden a sitios web en la red. Esta dificultad puede verse exacerbada por el uso de tumblers o anonimizadores adicionales en la red Tor. Tor es una de varias redes informáticas distribuidas clandestinas, a menudo denominadas darknets, cypherspace, Deep web o redes anónimas, que las personas utilizan para acceder al contenido de una manera diseñada para ocultar su identidad y la actividad de Internet asociada.

Dark Wallet son monederos virtuales que funcionan como extensiones de los navegadores (disponibles en Chrome y potencialmente en Firefox) a efectos de garantizar el anonimato de las transacciones con criptomonedas mediante la incorporación de las siguientes funciones: autoanonimizador (mezclador), comercialización descentralizada, plataformas de micromecenazgo (“Crowdfunding”), plataformas de valores, e información y acceso a mercados online en la “Red oscura” (Dark web).

Salto de cadenas (Chain hopping): es un método utilizado para entorpecer la trazabilidad de transacciones con AV, que consiste en "saltar" de una criptomoneda a otra (y, por consiguiente, de una Blockchain a otra) utilizando distintas plataformas de intercambio de AV.

Intercambios atómicos (Atomic swaps): son una variante del "salto de cadenas" a través de contratos inteligentes digitales, que permiten intercambiar una criptomoneda por otra sin recurrir a intermediarios centralizados, como las plataformas de intercambio de AV. Se llevan a cabo entre monedas que operan con diferentes blockchains, y pueden concretarse "off-chain", esto es: por fuera de la Blockchain de cada criptomoneda. El contrato requiere que ambas partes confirmen la recepción de los fondos dentro de un lapso predeterminado mediante una función hash criptográfica.

Si dentro del período establecido una de las partes no confirma la transacción, la misma es anulada y los fondos no son intercambiados.

Combinación o mezcla de monedas (CoinJoin o Coin Mixing): es una técnica de anonimización que se concreta mediante un contrato inteligente digital en el que las partes acuerdan comprometer sus AV en una nueva transacción, en la que cada una termina con la misma cantidad de criptomonedas con la que ingresó, pero en la que las direcciones utilizadas se entremezclan para dificultar la trazabilidad.

Firma de círculo (Ring signature): es un método de anonimización que consiste en el uso de una modalidad de firma digital grupal, conforme la cual cada miembro del grupo cuenta con su propia clave, pero al utilizarla no puede saberse cuál de todas ellas se usó para confirmar una determinada transacción con AV.

Como consecuencia de detectar la utilización de cualesquiera de las herramientas con fines delictivos mencionadas, el comité de cumplimiento y prevención de lavado de activos informará tanto a la UIF como a cualquier otra entidad competente y procederá la desvinculación del cliente de conformidad al procedimiento que a continuación se esboza.

21.Procedimiento de desvinculación de clientes

En caso que:

- (i) las herramientas de monitoreo ut supra mencionadas arrojen un resultado negativo del perfil del cliente (e.i. persona sancionada, nivel de riesgo alto por encontrarse vinculado a operaciones en la dark web o utilización de anonimizadores, mixers, etc.);

- (ii) por ordenamiento judicial o administrativo por parte de la UIF se informe la participación o vinculación de un usuario en delitos de lavado de activos o financiamiento de terrorismo; y/o

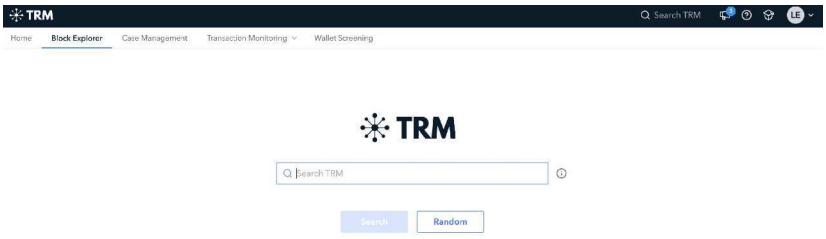
- (iii) el comité de cumplimiento y prevención de lavado de activos detecte falencias en la documentación aportada por el cliente para demostrar el origen de los fondos (sean falsas, incorrectas o denoten irregularidades); se conformará una carpeta digital plasmando todos los datos del usuario y los motivos que generaron el suficiente nivel de sospecha, ordenando la Alta Gerencia la inmediata desvinculación del cliente.

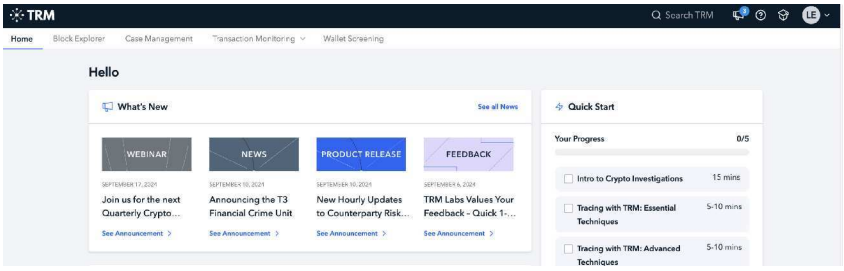
22. Tecnología de monitoreo de criptoactivos integrada vía API con un sistema de alertas automatizado corriendo 24/7

Contamos con Tecnología de monitoreo de criptoactivos integrada vía API con un sistema de alertas automatizado corriendo 24/7. A través de los softwares de punta brindados por Onfido y Neitcom, perfilamos, analizamos y extraemos conclusiones sobre el comportamiento de nuestros usuarios.

El mismo nos permite organizar, graficar y clasificar las operaciones en nuestra plataforma, para determinar patrones de conducta ordinarios y extraordinarios.
A su vez, las transacciones que operamos son verificadas con TRM Labs, una herramienta que analiza las transacciones de Criptomonedas y su trazabilidad en la cadena de bloques (blockchain) sobre la cual operan.

Las características de trazabilidad, inmutabilidad y publicidad de cada transacción realizada en el blockchain, le permiten a esta solución tecnológica realizar los análisis que eventualmente pueden conectar direcciones de criptomonedas vinculadas a actividades ilícitas específicas.





PREVENCIÓN DEL LAVADO DE ACTIVOS Y FINANCIAMIENTO DEL TERRORISMO

Vita Wallet