

GUÍA GENERAL ALA/CFT

2020



VIRU TĒRĀ MBA'EREPY
IPOTÍ'YVA OJEJOKO HAGUĀ
SĀMBYHYHA
TAPICHA ATY VIRU REHE OÑANGAREKO PORĀVA
SECRETARÍA DE
**PREVENCIÓN DE LAVADO
DE DINERO O BIENES**
UIF - UNIDAD DE INTELIGENCIA FINANCIERA

 **GOBIERNO
NACIONAL**

*Paraguay
de la gente*

INDICE

ABREVIATURAS	2
INTRODUCCIÓN	3
1. AUTOEVALUACIÓN DE RIESGOS	4
1.1. Criterios mínimos de autoevaluación	4
1.2. Metodología de Evaluación	5
1.2.1. Diseño de la Metodología	6
<i>I. Identificación de los factores e indicadores de riesgo</i>	6
<i>II. Medición de los riesgos</i>	9
<i>III. Mitigantes</i>	10
1.2.2. Implementación	11
1.2.3. Valoración	11
1.3. Cuadro que expone la Metodología de Autoevaluación de Riesgos	12
2. SISTEMA DE CONTROL Y ADMINISTRACIÓN DE RIESGOS	12
3. DEBIDA DILIGENCIA DEL CONOCIMIENTO DEL CLIENTE	13
3.1. Medidas de DDC aplicables a todos los clientes	14
3.2. Regímenes de DDC	15
<i>I. General</i>	15
<i>II. Simplificado</i>	16
<i>III. Ampliado</i>	16
3.3. Calificación de riesgos aplicable a Clientes	17
3.4. Etapas de la DDC	18
4. MANTENIMIENTO DE REGISTROS	19
5. DEPENDENCIA EN TERCEROS	20
6. RELACIONES DE CORRESPONSALÍA	21
7. REPORTES DE OPERACIONES SOSPECHOSAS	21
8. PAUTAS FINALES	22

ABREVIATURAS

BF	Beneficiario Final
DDC	Debida Diligencia del Cliente
EBR	Enfoque Basado en Riesgos
ENR	Evaluación Nacional de Riesgos
FT	Financiamiento del Terrorismo
GAFI	Grupo de Acción Financiera Internacional
LA	Lavado de Activos
LA/FT	Lavado de Activos y Financiamiento del Terrorismo
OS	Organismo Supervisor
PEP	Persona Expuesta Políticamente
ROS	Reporte de Operaciones Sospechosas
SEPRELAD	Secretaría de Prevención de Lavado de Dinero o Bienes
SO	Sujetos Obligados
UIF	Unidad de Inteligencia Financiera

INTRODUCCIÓN

La presente guía se encuentra basada en los estándares internacionales establecidos por el Grupo de Acción Financiera Internacional (GAFI), reconocidas estas como las 40 recomendaciones, sus notas interpretativas y los parámetros de la metodología de evaluación; y tiene por objeto orientar complementariamente a los Sujetos Obligados (SO) en la elaboración de los procesos dirigidos al desarrollo, adopción y ejecución de los métodos y sistemas que le permitan aplicar adecuadamente el Enfoque Basado en Riesgos (EBR), implementando las políticas pertinentes con el fin de identificarlo, medirlo y monitorearlo, dando cumplimiento a las disposiciones establecidas por la SEPRELAD.

1. AUTOEVALUACIÓN DE RIESGOS

La implementación de una autoevaluación de riesgos permite identificar y medir su propia exposición, a efectos de corregir de manera oportuna las deficiencias de sus procedimientos.

Conforme a la metodología y los procedimientos correspondientes, cada SO establecerá los procesos que se llevarán a cabo para la identificación, medición y mitigación de los riesgos a los que se encuentra expuesto, para lo cual deberá elaborar sus indicadores, en base a diversas fuentes de información, entre las que considerará la Evaluación Nacional de Riesgos (ENR) y sus actualizaciones, que la SEPRELAD (UIF) da a conocer por medio de su página web.

Al efecto, los SO deberán contar con políticas, controles y procedimientos, aprobados por su máxima autoridad, que les permitan manejar y mitigar los riesgos que han sido identificados.

La implementación de tales políticas, controles y procedimientos deberá ser monitoreada de manera periódica, realizando las mejoras, cuando corresponda; y adoptar medidas intensificadas para gestionar y mitigar los riesgos, cuando las resultas evidencien exposición a riesgos mayores.

Los SO solo pueden adoptar medidas simplificadas para manejar y mitigar los riesgos cuando, de la culminación de las evaluaciones se han identificado riesgos menores, y bajo ningún supuesto se pueden implementar medidas simplificadas cuando haya sospecha de LA/FT.

Es obligación de los SO documentar adecuadamente las evaluaciones de riesgos desarrolladas, siendo responsabilidad de cada Organismo Supervisor, asegurar el cumplimiento de las obligaciones relacionadas a la evaluación, verificación, actualización del riesgo por medio de la supervisión.

1.1. Criterios mínimos de autoevaluación

Si bien la norma encomienda que sean los SO quienes definan su proceso de autoevaluación, partiendo de la base de que no todos poseen el mismo nivel operativo, cantidad de clientes, perfiles, modelo de negocios, etc., existen ciertos criterios que deberían ser considerados como pauta básica y mínima para la adecuada identificación de los riesgos, entre los cuales se encuentran:

- a. Documentar sus evaluaciones de riesgo.

- b. Considerar todos los factores de riesgo¹ pertinentes de manera a determinar cuál es el nivel de riesgo general y los tipos apropiados de mitigación a aplicar.
- c. Mantener actualizadas estas evaluaciones.
- d. Contar con mecanismos apropiados para suministrar información de evaluación del riesgo a las autoridades competentes, en los plazos y formas que les sea requerida.

Los SO tienen el deber de evaluar el nivel de exposición a los riesgos de LA/FT asociados a diferentes factores, entre los que se encuentran nuevos productos, tecnologías, y/o servicios que eventualmente se dispongan a ofrecer, así como factores propios identificados en la operativa y modalidad del negocio.

En esta evaluación corresponde tomar en cuenta, además de los criterios que considere el propio SO, el canal de distribución del producto y/o servicio ofrecido, así como otros atributos asociados a los factores de riesgo de LA/FT.

Esta evaluación también será realizada cuando los SO decidan implementar o utilizar nuevas tecnologías en los procesos de comercialización de los productos y/o servicios ofrecidos, o se realice un cambio en un producto existente que modifica su nivel de exposición al riesgo de LA/FT.

Todas estas evaluaciones, una vez identificados los riesgos a los que se encuentren expuestos, se establecen para que el SO desarrolle las medidas apropiadas para manejar y mitigarlos.

1.2. Metodología de Evaluación

A efectos de implementar adecuadamente el proceso de autoevaluación, los SO deberán diseñar una Metodología adecuada a sus características para desarrollarla, pudiendo apoyarse en matrices y otras herramientas idóneas, a los efectos de medir y evaluar los riesgos, de manera a comprenderlos para determinar las medidas acordes a los niveles de materialización y gravedad del impacto.

Atendiendo a tal condición, podrán analizar y tener en consideración los siguientes aspectos:

¹ La determinación de los factores de riesgo que deben ser considerados por cada sector son los identificados en cada una de sus reglamentaciones, las cuales, de manera general abarcan, como mínimo, a los clientes, países o áreas geográficas, productos, servicios, transacciones o canales de envío.

1.2.1. Diseño de la Metodología

Para el desarrollo de la Metodología de Evaluación, independientemente a los factores que el SO considere prudente observar, deberían tenerse en cuenta los siguientes criterios:

- a. Identificar los factores de riesgo inherentes a cada actividad desarrollada, así como sus indicadores, analizando cómo y en qué medida estos eventualmente podrían vulnerar el sistema, dando lugar a la posibilidad de comisión de hechos punibles de LA/FT o algunos de sus delitos precedentes.
- b. Abarcar, en el análisis de identificación de los factores, la totalidad de los productos y servicios con los que opera, incluidos los tipos de clientes, canales de distribución, áreas geográficas, transacciones e infraestructura tecnológica.
- c. Implementar un método para la medición de los riesgos, que básicamente implica el análisis cuantitativo que establezca una relación entre los factores e indicadores de riesgo y la asignación de un valor a estos, en función a la descripción que se haga sobre la importancia que ha de implicar y el grado de probabilidad de que el riesgo se materialice.
- d. Establecer cuáles serán los mitigantes que se aplicarán, a fin de reducir las posibilidades o probabilidades de que los riesgos se materialicen.

Se espera que la Metodología describa el proceso utilizado para identificar, evaluar, analizar y mitigar los riesgos a los cuales se encuentra expuesto el SO, de acuerdo con la naturaleza y dimensión de su actividad comercial y los distintos factores de riesgo en cada una de sus líneas de negocio.

I. Identificación de los factores e indicadores de riesgo

Para evaluar la exposición al riesgo respecto de cada factor deberán considerarse, entre otros elementos, los siguientes:

a. Clientes

Como criterio general, la admisión de un cliente requiere la adecuada acreditación de su identidad y la recopilación de los datos necesarios para la asignación de un perfil que establezca el nivel de riesgo, lo que a su vez, determinará el procedimiento de Debida Diligencia aplicable a cada caso en concreto.

En primer lugar, y en función a la información obtenida, se deberá realizar un primer análisis para descartar que el potencial cliente represente algún supuesto que requiera especial

atención, como ser, de manera ejemplificativa, la utilización de un nombre ficticio, o la determinación de que éste actúa por cuenta de otra persona.

Verificada la identidad del cliente, se establecerá la calificación que corresponda, la asignación del perfil y el nivel de Debida Diligencia que, en principio, será administrado.

Una vez que la relación comercial se encuentre en curso, corresponde establecer la periodicidad con la que se actualizarán los datos, a fin de comprobar que no existan causales que ameriten la recalificación del cliente, la aplicación de procedimientos específicos, o incluso en algunos casos, la conclusión de la relación comercial ya iniciada.

Por tanto, al inicio de la relación, así como en el transcurso de la misma, considerarán cuanto menos los siguientes indicadores:

- Tipo de clientes²
- Porcentaje de participación de cada tipo de cliente en el conjunto total de los mismos.
- Sector de actividad³
- Características del tipo de servicio que contrató o pretende contratar, así como la operación que desea realizar
- Origen de los fondos declarados y su consistencia y verosimilitud con la documentación presentada
- Nacionalidad.⁴

Tales indicadores serán considerados para establecer las variables de categorización de los clientes, a fin de establecer si el riesgo que representan es bajo, medio o alto, a fin de aplicar medidas de control acordes.

b. Zona Geográfica

² Indicación si refiere a personas físicas, personas o estructuras jurídicas, sobre todo si tienen particularidades que traen inmersos criterios específicos, como PEPs, etc.

³ A modo ejemplificativo de este indicador, y la implementación de la Evaluación Nacional de Riesgos en el proceso de autoevaluación, se indica que respecto al sector inmobiliario, *“se trata de un sector que ha tenido un notable desarrollo en los últimos años, acompañando el crecimiento del país. Sin embargo, la presencia de actores extranjeros que invierten sumas considerables de dinero en el mismo, hace que, sin dejar de estimular actividades que son beneficiosas para el país, se realicen estudios específicos para determinar su posible utilización para la comisión de ilícitos y adoptar las medidas necesarias para su prevención y detección”*. En ese contexto, se deberían considerar los riesgos vinculados a los productos relacionados al financiamiento e inversión de estas actividades.

⁴ Considerar también en este indicador a los ciudadanos de nacionalidades de países sobre los que rigen sanciones económicas por parte de organismos internacionales, o aquellos designados en las diversas listas públicas de sanciones financieras relacionadas al terrorismo y su financiamiento.

Es de significativa importancia la ubicación desde donde o hacia donde se realizan las operaciones canalizadas a través del SO; es decir, habrá de tomarse en cuenta la ubicación de la casa matriz, las sucursales, agencias o asimiladas a cualquiera de ellas, así como también el lugar de domicilio del cliente, el del lugar de la realización de las actividades de éste, y las particularidades geográficas de cada operación que realiza, sean estas a nivel nacional o internacional.

La realización de un relevamiento de información por cada una de las zonas geográficas antes mencionadas, permitirá al SO determinar el nivel de riesgo al que pueden verse expuestos, para lo cual deberán considerar como mínimo los siguientes indicadores:

- Actividades económicas comunes en la zona⁵
- Porcentaje de participación de cada zona en los activos e ingresos del SO
- Presencia de actividades delictivas y sus índices de ocurrencia⁶
- Señales de alerta y ROS vinculados a cada zona
- Actividades o actos terroristas de los cuales se tenga noticia, aunque solo lo fueran en forma de sospecha
- Zonas de frontera
- Países con medidas deficientes en materia de LA/FT.

c. Productos

El análisis de autoevaluación debe implicar la totalidad de los productos y servicios con los que operan los SO, describiéndose adecuadamente las características de cada uno de ellos. Corresponde prestar atención a aquellos que puedan posibilitar un mayor grado de dificultad en el conocimiento de la identidad del cliente o usuario, las operaciones de altos volúmenes de dinero mediante transferencias, entre otros.

El proceso deberá ser realizado también cuando el SO pretenda el ofrecimiento de un nuevo producto que implique la utilización de nuevas tecnologías, debiendo llevar a cabo la evaluación con anterioridad a su lanzamiento.

Indicadores:

⁵ Al hablar de actividades comunes a la zona, se hace referencia a la ganadería, agricultura, comercio exterior, entre otros.

⁶ Por ejemplo, estadísticas emitidas por organismos y entidades gubernamentales oficiales, obrantes en fuentes públicas, o zonas específicas indicadas en la Evaluación Nacional de Riesgos.

- Naturaleza y características de los productos⁷
- El medio de pago utilizado.
- La participación de cada producto en el total de los activos e ingresos del SO
- Señales de alerta y ROS vinculados a cada producto.

d. Canales de Distribución

Se deben analizar también los canales de distribución de los productos con los que los SO ponen a disposición de sus clientes o usuarios los servicios, determinando por medio de indicadores la susceptibilidad de que estos puedan ser utilizados para la realización de operaciones de LA/FT.

Además, en este criterio se considerarán los casos en que los SO implementen nuevas tecnologías para la distribución de sus productos o servicios, debiendo realizar la evaluación de manera previa a su implementación o utilización.

Indicadores:

- Naturaleza y características de cada canal
- La participación de cada canal en el total de los activos e ingresos del SO
- Señales de alerta y ROS vinculados a cada canal.

II. Medición de los riesgos

Una vez individualizados los factores e indicadores de riesgo, el siguiente paso consiste en asignarles una cuantificación, en atención a la importancia que le es atribuida de manera consistente con la descripción y comprensión de las probabilidades de materialización del riesgo.

El método escogido deber ser lo suficientemente flexible, de modo a que permita ajustarlo cuando la dinámica operacional así lo amerite. Para medir o evaluar el riesgo, los SO deben establecer un rango o escala de calificación a cada indicador.

A modo de ejemplo, una herramienta básica para realizar una medición, puede ser implementada a través de una Matriz de Riesgos del tipo 3x3, constituida sobre 3 niveles para la probabilidad de ocurrencia del hecho y la gravedad del impacto para el SO.

⁷ Se deben tomar como características del producto si estos facilitan un mayor grado de anonimato, falta de identificación del cliente o de alguna persona involucrada en la operación, entre otros.

Dicho modelo puede aplicarse para el mapeo de los riesgos ya sea de manera individual o en conjunto, de acuerdo a la metodología adoptada y los factores aplicables.

Ejemplo de Matriz de Riesgo 3x3

PROBABILIDAD	3	TOLERANCIA DEL RIESGO(4)	ADVERSIÓN AL RIESGO(5)	ADVERSIÓN AL RIESGO(6)
	2	APETITO DE RIESGO(3)	TOLERANCIA DEL RIESGO(4)	ADVERSIÓN AL RIESGO(5)
	1	ACEPTACIÓN DE RIESGO(2)	APETITO DE RIESGO(3)	TOLERANCIA DEL RIESGO(4)
	0			
		1	2	3
IMPACTO				

Un ejemplo de medición conforme a la Matriz de Riesgos puede ser la siguiente:

RIESGO	MEDICIÓN	POLITICA DE RIESGOS
	0 a 2	ACEPTACIÓN DEL RIESGO
BAJO	2,1 a 3	APETITO DE RIESGO
MEDIO	3,1 a 4	TOLERANCIA DEL RIESGO
ALTO	4,1 a 6	ADVERSIÓN AL RIESGO

Es importante recalcar que las recomendaciones internacionales y las reglamentaciones de SEPRELAD no prescriben una metodología para la realización de las autoevaluaciones, ni una determinada herramienta de apoyo, razones por las cuales su diseño, así como la política de gestión de los riesgos, son realizados por el SO.

Los SO deben documentar adecuadamente el proceso, el resultado de su medición o evaluación y el porqué de la asignación del rango, así como las áreas que han proporcionado los datos analizados.

III. Mitigantes

Seguidamente, ya con los factores e indicadores debidamente identificados, así como la asignación de los rangos de riesgo, con base a tal conocimiento, deberán establecerse los controles, periodicidad, estructuras internas, medidas, criterios, políticas y procedimientos a ser implementados, así como los recursos que estarán avocados a la tareas que éstas

impliquen, con el objeto de anular o disminuir significativamente la exposición del SO a los riesgos de LA/FT.

A modo de ejemplo, se citan algunos medios que pueden ser considerados por los SO, como mitigantes:

- **Capacitación:** Incluyendo a los niveles jerárquicos superiores, así como a los demás niveles, de acuerdo a la periodicidad prevista en la norma, previéndose que los temas a ser abordados sean coherentes con la envergadura de los SO y con las políticas y procedimientos que pretende ejecutar, así como la eventual actualización de las normas, guías y otros documentos de referencia en materia de LA/FT.
- **Auditorías Internas/Externas:** Las que deberán estar debidamente focalizadas en la revisión y evaluación de la ejecución de las políticas y procedimientos en materia de prevención de LA/FT, que tenga por objeto de la detección oportuna de las deficiencias eventuales y la consecuente aplicación de medidas correctivas para mitigarlas.
- **Controles Internos:** Los que se podrán implementar de acuerdo a la naturaleza y forma,⁸ a modo de ejemplo de manera bimestral, trimestral o semestral, para determinar si el impacto de los riesgos definidos en el sistema y su probabilidad siguen siendo los identificados, y si existen nuevos riesgos que no han sido detectados e incluidos.

1.2.2. Implementación

Esta fase consiste en la puesta en marcha de la Metodología diseñada, a efectos de que el SO tenga conocimiento del grado de exposición al riesgo que posee, con base a las calificaciones otorgadas a cada uno de los indicadores definidos. Para la adecuada mitigación de los riesgos, se requiere también la verificación de los resultados obtenidos mediante su desarrollo.

1.2.3. Valoración

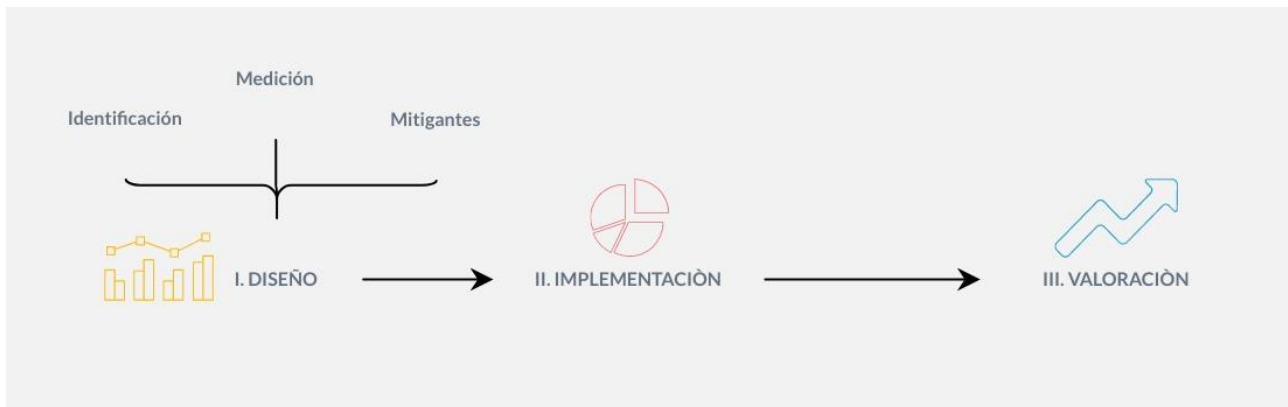
Esta fase implica la pertinente revisión respecto a la eficiencia y eficacia del sistema preventivo diseñado, y las necesidades de eventuales correcciones que deban realizarse

⁸ En cuanto a la naturaleza del riesgo, se podrían implementar procedimientos de control preventivos (sobre la causa del riesgo y su agente generador, con el fin de disminuir la posibilidad de que se materialice). Respecto a su forma, podrían ser controles manuales (ejecutadas por personas responsables de un proceso dentro de la entidad) o controles automatizados (aplicados por medio de un soporte diseñado para detectar, prevenir, corregir errores, sin que interfiera el factor humano en el proceso).

con base en las experiencias recogidas, la dinámica y evolución natural de las actividades de los SO.

A tales efectos resulta recomendable la realización de un seguimiento por cada factor e indicador, en relación a los criterios, medidas, procedimientos y políticas aplicados, que propicien la detección temprana de la materialización de los riesgos, o la corrección de las deficiencias en los procesos de su administración.

1.3. Cuadro que expone la Metodología de Autoevaluación de Riesgos



2. SISTEMA DE CONTROL Y ADMINISTRACIÓN DE RIESGOS

De manera a prevenir e impedir ser utilizados como medio o canal para la realización de hechos que impliquen LA/FT o sus hechos punibles precedentes, es importante que los SO desarrollen e implementen un Sistema de Control y Administración de Riesgos de LA/FT que sea compatible con la empresa o negocio, y sea consistente con su estructura y sus procesos.

Las diversas normas de la SEPRELAD señalan como elementos básicos para componer un Sistema de Control y Administración de Riesgos eficiente a los siguientes:

- **Código de Ética y Conducta;** que constituyen pautas de comportamiento que deben seguir las personas vinculadas directa o indirectamente al SO. Estas pautas se traducen en parámetros que deben ser observados por los directivos, empleados y terceros asociados, complementando las demás obligaciones que se encuentran en los reglamentos internos, contratos individuales y otros procedimientos que dicte el SO.
- **Control Interno;** cuyo objetivo primordial es determinar de manera primaria la efectividad en la administración de los riesgos del SO. Comprende un plan de

verificación del conjunto de métodos y procedimientos aplicados, que aseguran que los controles implementados son apropiados y suficientes para prevenir el LA/FT

- **Auditoría Externa;** ejecutada por un profesional ajeno e independiente del SO, encargado de evaluar los controles y procedimientos internos y verificar que las políticas y procedimientos aplicados cumplen con las normativas de prevención de LA/FT.⁹
- **Comité de Prevención;** constituido como un órgano de apoyo al Oficial de Cumplimiento dentro de la estructura del SO.
- **Oficial de Cumplimiento;** encargado de velar por el funcionamiento efectivo, eficiente y oportuno del Sistema de Control y Administración de Riesgos, coordinando el desarrollo de los programas internos destinados a su observancia.¹⁰

La implementación de cada uno de los elementos se realiza atendiendo a la organización del SO, teniendo en cuenta si es persona física o jurídica.

3. DEBIDA DILIGENCIA DEL CONOCIMIENTO DEL CLIENTE

La Debida Diligencia de Conocimiento del Cliente (DDC) se establece a través de un conjunto de normas, medidas y procedimientos tendientes a obtener la información que permita conocer la identidad de un cliente o su beneficiario final, establecer su perfil transaccional y verificar que sus operaciones sean compatibles con dicho perfil.

Los criterios de DDC serán aplicados a los clientes que actúen en carácter particular, como personas físicas, o como mandantes o representantes de personas y estructuras jurídicas.

Los regímenes de DDC son implementados por los SO en virtud a la identificación, evaluación continua y entendimiento de los riesgos de lavado de activos/financiamiento del terrorismo a los que se encuentran expuestos, a fin de administrarlos y mitigarlos.

El régimen a ser implementado será determinado por la calificación de riesgos de LA/FT del cliente, en base a los parámetros identificados, los cuales permitirán un mayor control,

⁹ De acuerdo a las directrices otorgadas por la SEPRELAD, el profesional, o en su caso la firma contratada para la realización de la Auditoría Externa deberá encontrarse inscripto en el Registro de Auditores Externos Especializados en prevención de LA/FT.

¹⁰ Las diversas normativas dirigidas a los SO indican que el Oficial de Cumplimiento designado debe, mínimamente, tener relación directa, pertenecer al rango jerárquico superior, gozar de autonomía e independencia en el ejercicio de sus funciones, sin tener a su cargo otras actividades que pudieren generar conflicto de intereses. Para algunos SO es requisito esencial la formación profesional, siendo necesaria también la capacitación en LA/FT,

intensidad y rigurosidad en aquellos clientes que reúnen ciertas características, así como, en contrapartida, la reducción de ellos cuando corresponda.

Por ejemplo, los SO que desarrollan actividades en el sector asegurador, deberán incorporar en el análisis que compone la DDC al beneficiario de una póliza de seguro de vida como un factor para determinar si corresponde aplicar un mayor nivel de medidas.

Las categorizaciones procedimentales son aplicadas en virtud a los riesgos identificados, relativos a los tipos de clientes, países, zonas geográficas, productos y servicios utilizados, transacciones o canales de envío, entre otros, pudiendo ser estos analizados de manera conjunta o por separado, aumentando o disminuyendo el riesgo potencial que representan, impactando así en el nivel apropiado de medidas de DDC.

Entre los ejemplos de estas variables se encuentran:

- El propósito de una cuenta o relación
- El nivel de activos o la dimensión de las transacciones realizadas por un cliente
- La regularidad o duración de la relación comercial.

Los riesgos mayores implican la implementación de medidas con carácter intensificado en su manejo y mitigación. Tales medidas son ejecutadas bajo criterios específicos designados por el regulador, o en consideración a aquellos determinados por el propio SO.

Los riesgos menores involucran acciones o medidas con carácter simplificado. La evaluación que los determina comprende el análisis de todos los factores indicados en la norma, revisadas a priori con carácter general, para luego establecer los mitigantes de manera abreviada.

3.1. Medidas de DDC aplicables a todos los clientes

Los SO, en sus procesos de DDC, en consonancia con las disposiciones establecidas en cada reglamentación emitida para el sector deberán tomar las siguientes medidas:

- a. Identificar al cliente (se trate de una persona física o jurídica o de una estructura jurídica) y verificar la identidad usando documentos, datos o información confiable y de una fuente independiente (datos de identificación).¹¹

¹¹ De manera específica, cuando se establezca una relación con una persona jurídica, el Sujeto Obligado debe identificarla como tal, verificando esa identidad con las documentaciones de respaldo que resulten pertinentes, y que le permitan entender la naturaleza de la actividad del cliente y su estructura accionaria o de control.

- b. Verificar que una persona que dice actuar en nombre del cliente esté autorizada para hacerlo, e identificar y verificar la identidad de esa persona.
- c. Identificar al beneficiario final y tomar las medidas razonables para verificar a este beneficiario final usando la información pertinente o datos obtenidos mediante fuentes confiables, de tal manera que el SO esté convencido de que sabe quién es el beneficiario final.
- d. Entender y, según corresponda, obtener información sobre el propósito y el carácter que se pretende dar a la relación comercial.

3.2. Regímenes de DDC

Los Sujetos Obligados deben aplicar las medidas de DDC teniendo en cuenta 3 niveles:

I. General

La aplicación de un régimen de DDC con carácter general implica el desarrollo de procedimientos con carácter continuo y permanente, aplicables a las operaciones o transacciones que son desarrolladas por sus clientes.

Las acciones comprendidas en un régimen de tal naturaleza comprenden, de manera indicativa, entre otras, las siguientes:

- a. La identificación del cliente y la verificación de la identidad respaldada documentos, datos o información confiable y de una fuente independiente (datos de identificación)
- b. La determinación de los mandantes o representantes, cuando sean utilizados como ejecutores de las operaciones en nombre de quien sería el beneficiario final
- c. El entendimiento del propósito y el carácter que se pretende dar a la relación¹²
- d. El monitoreo relativo a las operaciones y las condiciones bajo las cuales se ha establecido la relación con el cliente
- e. La actualización de los datos de manera periódica, conforme los plazos determinados por el SO en función a las características del cliente, además de los factores de riesgo asociados al mismo
- f. El respaldo documental como sustento de las transacciones efectuadas

¹² El carácter de la relación puede ser determinado por factores como la periodicidad con la que opera el cliente. De manera ejemplificativa, si la operativa es continua o periódica, se puede catalogar al cliente como permanente.

- g. La verificación de las declaraciones relativas al origen de los fondos, actividad económica y otros criterios relativos a la identificación.

II. Simplificado

La implementación de un régimen simplificado implica una calificación, cuando corresponda, de un nivel de exposición y riesgo bajo de los clientes, lo cual permite atenuar el rigor de ciertas medidas ser impulsadas, pudiendo proceder, entre otras medidas, a:

- a. Reducción de los requerimientos documentales, pudiendo recurrir a otras fuentes (abiertas o cerradas) para su correspondiente verificación
- b. Menor frecuencia en la actualización de los datos de identificación
- c. Eximición de la solicitud de antecedentes que sustenten el volumen de ingresos
- d. Reducción del grado de monitoreo y análisis de las transacciones
- e. Verificación de la identidad del cliente y beneficiario final con posterioridad al establecimiento de la relación, cuando corresponda.

Las medidas de DDC simplificadas no son aceptables cuando exista una sospecha de lavado de activos o financiamiento del terrorismo, o se apliquen en escenarios específicos de mayor riesgo.

III. Ampliado

En la implementación de los procesos de DDC, los SO deben analizar, en la medida de lo posible, los antecedentes y el propósito de las transacciones complejas, inusuales, grandes y todos los patrones no habituales de operaciones que no tengan un propósito aparente económico o lícito, para incorporarlos en este régimen.

Cuando los riesgos de LA/FT sean mayores, deben aplicarse medidas intensificadas de DDC, a tono con los riesgos identificados, traducidas en el incremento del grado y naturaleza del monitoreo de la relación, a fin de determinar si esas transacciones o actividades parecen inusuales o sospechosas.

Entre los ejemplos de medidas intensificadas de DDC que se pueden aplicar a relaciones de mayor riesgo se pueden citar:

- a. Incrementar la frecuencia en la revisión de la actividad transaccional del cliente y la actualización de su información
- b. Aplicar medidas adicionales de identificación y verificación

- c. Monitorear continuamente las operaciones que realice el cliente, incrementando la cantidad y la duración de los controles aplicados, y selección de los patrones de transacciones que necesitan un mayor examen
- d. Obtener información, y cuando resulte aplicable documentación respaldatoria del origen de los fondos, actividad económica, propósito de las operaciones, carácter de la relación, u otros que el SO considere pertinentes.

Los SO deben gestionar los riesgos en base a los regímenes aplicables a cada cliente, realizando revisiones de manera periódica a efecto de recategorizarlos.

3.3. Calificación de riesgos aplicable a Clientes

De manera a determinar el régimen dentro del cual correspondería calificar a un cliente, el SO puede implementar una Matriz de Riesgos, analizando indicadores inherentes a la naturaleza del factor.

La finalidad de la Matriz es medir el nivel de riesgos individual de los clientes, sean estos nuevos o establecidos e independientemente a su naturaleza, a fin de aplicar medidas correctivas o mitigar los efectos adversos o indeseados.

Conforme los parámetros establecidos en las diversas reglamentaciones emitidas por la SEPRELAD, y las pautas otorgadas por la presente guía, se expone de manera ejemplificativa el siguiente sistema de calificación de riesgos:

MEDICIÓN	CALIFICACIÓN DE RIESGOS LA/FT	IMPACTO	TRATAMIENTO DE LOS RIEGOS LA/FT	
			REGIMEN DE DDC	CONTROLES O MITIGANTES (Eje.)
0 a 1	BAJO	LEVE	DDC SIMPLIFICADA	Controles de alertas y actualización de documentaciones con frecuencia reducida
1,1 a 2	MEDIO	MODERADO	DDC GENERAL	Controles de alertas y actualización de documentos con frecuencia moderada
2,1 a 3	ALTO	GRAVE	DDC AMPLIADA	Monitoreo constante de alertas y operaciones, actualización de documentos con mayor sistematicidad y periodicidad

Estas herramientas pueden ser desarrolladas en los procesos de vinculación o aceptación de clientes, implementado un modelo lineal, construido sobre tres niveles de calificación, conforme a las probabilidades resultantes del análisis de los factores y sub-factores de riesgos, previas ponderaciones de acuerdo a los criterios desarrollados por el SO, considerando las Evaluaciones Nacionales y Sectoriales, las propias autoevaluaciones del SO e informaciones obtenidas de otras fuentes que deberán ser documentadas.

3.4. Etapas de la DDC

El procedimiento de DDC se divide en 3 etapas, siendo estas la de identificación, la de verificación y por último, la etapa de monitoreo.

Cuando el Sujeto Obligado no pueda cumplir con la DDC en las etapas de identificación y/o verificación al comienzo de la relación comercial, debe abstenerse de iniciarla.

En cuanto a la etapa de verificación,¹³ es tarea del SO verificar la autenticidad de la información proporcionada por el cliente, de manera a poder clasificarlo adecuadamente o determinar el perfil que será asignado al mismo.

En caso de que exista imposibilidad de realizar la adecuada identificación del cliente por falta de información, es decir, una inviabilidad de efectuar la DDC, correspondería terminar la relación comercial, sin que tal decisión este supeditada a la existencia de un ROS, sino a los factores ya señalados.

En la etapa de monitoreo, como culminación de la DDC, se efectúa una comparación entre lo determinado en una primera instancia y lo efectivamente operado por el cliente, con el propósito de que, en caso de que surjan variaciones o posibles inconsistencias, se analice el ajuste del perfil o la acción que el SO considere en el marco de su enfoque basado en riesgos.

En el marco de los estándares internacionales sobre la lucha contra el lavado de activos, el financiamiento del terrorismo y de la proliferación,¹⁴ se contemplan tres situaciones en las cuales, ante la imposibilidad de completar adecuadamente el proceso de DDC, se determinan consecuencias concretas.

- a. No abrir la cuenta o no iniciar la relación comercial
- b. No realizar la transacción u operación, y
- c. Cerrar la cuenta o terminar la relación.

En este contexto, el SO debe considerar hacer un reporte de operación sospechosa en relación con el cliente en base a los supuestos que surge en el marco del proceso señalado.

La no apertura, el cierre o la no realización de una operación no se encuentran vinculadas a la existencia de un ROS, sino a la imposibilidad de realizar la Debida Diligencia de

¹³ Para este punto es importante recordar que se permite a los Sujetos Obligados iniciar la relación comercial y efectuar operaciones ordenadas por el cliente antes de que la etapa de verificación se encuentre debidamente culminada, en el marco de sus procedimientos de gestión de riesgos.

¹⁴ Recomendación 10 del GAFI.

Conocimiento del Cliente. Por ende, la emisión de un Reporte de Operación Sospechosa es una consecuencia, no una causa de lo señalado.

Es importante advertir que, además de los 3 supuestos señalados, también se dispone de otra acción alternativa, vinculada a la posibilidad de que los SO, en función a indicios o sospechas de que la operativa del cliente se encuentre relacionada a eventuales hechos de LA/FT o sus delitos precedentes, opten por no aplicar las medidas de DDC y remitan directamente el reporte de operaciones sospechosas a la UIF.

Otro factor a tener en cuenta en la realización de la DDC es la calificación del régimen aplicable, que puede ser simplificado, ampliado o general, según la naturaleza de las personas, sean estas físicas o jurídicas, y sus características particulares.

4. MANTENIMIENTO DE REGISTROS

El mantenimiento de los registros consta de dos supuestos a ser tenidos en cuenta:

- a. En primer lugar, el registro de operaciones, en los que se deben conservar los datos de todas las transacciones, sean estas nacionales o internacionales, que fueren realizadas a través del SO
- b. En segundo lugar, los registros obtenidos a través de las medidas de DDC, consistentes en archivos de clientes, cuentas, correspondencia comercial, entre otros, y los resultados de los análisis realizados.

En ese sentido, los SO deben conservar los registros de las operaciones¹⁵ de forma precisa y completa, durante cinco años desde que se ha efectuado la operación, o ha finalizado la relación con el cliente.

Igualmente, deben mantener todos los registros obtenidos a través de las medidas de Debida Diligencia de Conocimiento del Cliente,¹⁶ durante al menos 5 (cinco) años después de finalizada la relación comercial o desde la fecha de la transacción ocasional.

¹⁵ Por ejemplo:

- Supuesto a: Si el SO posee una relación comercial vigente hasta la fecha (año 2020) con un cliente desde el año 2010, debe conservar los registros de las operaciones que este realizó desde el año 2015 hasta el año 2020 (computando un periodo de 5 años). En cambio, si la relación comercial con tal cliente culminó en el año 2019, el SO solo tiene la obligación de la guarda de los registros de las transacciones hasta el año 2024; es decir, por 5 (cinco) años computados desde la finalización de la relación comercial.
- Supuesto b: El SO debe conservar los registros de las operaciones que un cliente haya realizado en el año 2016, hasta el año 2021. Es decir, 5 años computados desde que la operación haya sido efectuada, independientemente a que este haya vuelto o no a operar con el SO.

¹⁶ Por ejemplo: En caso de que un cliente se desvincule del SO en el año 2015, esta debe conservar toda la información y documentos sobre la identificación, las que justifiquen las operaciones realizadas, las

Esta disposición tiene el objeto de permitir la reconstrucción de las transacciones, si fuere necesario, a efectos de suministrar pruebas suficientes en el eventual caso de que se promueva algún proceso judicial por actividades delictivas.

Al efecto, los SO deben garantizar que toda la información y registros de transacciones de DDC se ponga con celeridad a disposición de las autoridades competentes, en los plazos y formas que les sea requerida.

5. DEPENDENCIA EN TERCEROS

La dependencia en terceros constituye una figura de delegación por parte de los SO de ciertas cuestiones que hacen a la ejecución de la Debida Diligencia de Conocimiento del Cliente, como ser:

- a. Identificación del cliente
- b. Identificación del beneficiario final
- c. Comprensión de la naturaleza de su actividad económica o comercial.

Esta delegación podrá realizarse siempre y cuando la reglamentación aplicable al SO lo permita.

Durante la relación de delegación o dependencia, el Sujeto Obligado delegante acordará la ejecución de acciones que le permitan obtener la información necesaria sobre las medidas de Debida Diligencia desarrolladas a sus clientes; para ello asegurará que el tercero proporcionará sin demora y a solicitud las documentaciones de respaldo relativa a los requisitos de DDC, y que haya implementado medidas de mantenimiento de los registros recabados.

La dependencia también puede realizarse con terceros que residan en otros países, siempre y cuando el SO verifique que el país de procedencia no representa un nivel de riesgo importante.

A modo de ejemplo, el SO deberá verificar que el país de procedencia del tercero designado no se encuentre individualizado como “no cooperante” por el GAFI, sujeto a sanciones financieras por parte de organismos internacionales o sometido a contramedidas aplicadas por el Paraguay.

documentaciones que han sido analizadas para los ajustes del perfil de riesgo y perfil transaccional, entre otros, hasta el año 2020.

Igualmente, por ejemplo, si se trata de un cliente que realizó una operación de compra de divisas en el año 2013, la entidad debió conservar los registros de esa operación hasta el año 2018.

En caso de que la delegación se realice entre SO que componen un mismo grupo financiero o económico, la Máxima Autoridad del grupo velará por la observancia de las siguientes condiciones:

- a. La aplicación de los requisitos de DDC, mantenimiento de registros y cumplimiento de las políticas y procedimientos de prevención de LA/FT
- b. La verificación de la implementación de las políticas preventivas
- c. La consideración de los riesgos a los que se encuentra expuesto el país en las medidas de mitigación implementadas por el grupo.

6. RELACIONES DE CORRESPONSALÍA

Las relaciones de corresponsalía son las que se establecen para transacciones de valores o transferencias de fondos a favor de una institución financiera o a los clientes de esta. Conforme el GAFI, este tipo de vínculos se da entre una entidad financiera (usualmente un banco, denominado “banco corresponsal”, a otra (el “banco representado”).

En los casos que resulte viable iniciar relaciones de corresponsalía, es oportuno que los SO que pretendan éstas incorporen procedimientos que le permitan determinar que las instituciones no han sido constituidas como bancos pantalla o las cuentas administradas por estas no son utilizadas por este tipo de entidades, en ningún caso.

7. REPORTES DE OPERACIONES SOSPECHOSAS

El Reporte de Operaciones Sospechosa (ROS) es la base sobre la cual se construyen los datos de inteligencia financiera, por lo que la comunicación oportuna y con prontitud es esencial en el ámbito preventivo.

Conforme a las reglamentaciones vigentes, cada SO posee un plazo para analizar una operación que haya sido considerada como una alerta, de manera a calificarla como inusual.

Una vez individualizada de esta forma la operación, se inicia el cómputo de otro plazo para que el Oficial de Cumplimiento, el Comité y el Directorio, o los responsables que cada reglamento indique, analicen la operación y decidan calificarla como sospechosa, remitiendo posteriormente un ROS.

Teniendo en cuenta que las comunicaciones relativas a operaciones sospechosas son comunicadas por medio del sistema implementado por la SEPRELAD, cada normativa ha establecido un plazo de 24 (veinticuatro) horas para la remisión.

Atendiendo al desglose de los plazos que rigen para cada uno de los procesos, el periodo entre la formulación de la alerta y la remisión del ROS se distribuye de la siguiente manera:

Generación de la alerta	X días
Calificación de la operación como inusual	30 días
Certificación de que la operación es sospechosa	90 días
Plazo para la remisión del ROS	24 horas

Obs.: Los plazos son computados en días corridos.

8. PAUTAS FINALES

La UIF- SEPRELAD ha elaborado este documento con la finalidad de otorgar herramientas orientativas que permitan desarrollar con mayor certeza los deberes que le han sido encomendados en el rol como SO respecto a conductas u operaciones presuntamente vinculadas con los delitos de LA/FT, aplicando un enfoque basado en riesgos.

Las directrices descritas resultan aplicables a todos los SO y su contenido debe ser implementado atendiendo a los preceptos del Reglamento de prevención emitido en forma específica para cada sector, además de las guías oficiales emitidas por el Grupo de Acción Financiera (GAFI) y aquellas que se consideren pertinentes en un futuro.

La SEPRELAD, eventualmente, podrá emitir guías de aplicación complementarias atinentes a los diferentes puntos desarrollados en la presente, actualizar los mismos y, en su caso, emitir nuevas pautas a ser implementadas en base a los parámetros y preceptos de las disposiciones legales nacionales, las 40 recomendaciones, sus notas interpretativas y los parámetros de la metodología de evaluación del GAFI.

Elaborado por: Dirección General de Asesoría Jurídica- SEPRELAD

Aprobado por: Carlos Arregui Romero, Ministro- Secretario Ejecutivo