



# SISTEMA DE AUTOCONTROL Y GESTIÓN DEL RIESGO INTEGRAL LA/FT/FPADM “SAGRILAFT”

Circular Externa 100-000016 del 24 de diciembre de 2020 –  
Superintendencia de Sociedades



# ¿QUÉ ES SAGRILAFT?

Es un sistema para autocontrolar y gestionar los riesgos Lavado de Activos (LA), Financiación del Terrorismo (FT) y el Financiamiento de la Proliferación de Armas de Destrucción Masiva (FPADM).

Este sistema incluye las directrices, procedimientos y controles necesarios para prevenir que las organizaciones criminales puedan tratar de usar o involucrar a PERSONAL SOFT en sus actividades ilegales.

# ¿POR QUÉ DEBEMOS IMPLEMENTAR EL SAGRILAFT EN PERSONAL DSOFT?

Al ser una empresa vigilada por la Superintendencia de Sociedades y al cumplir con los requisitos que pide la circular Personal Soft tiene que implementar dicho sistema y aplicarlo dentro de todas las operaciones y con todas las contrapartes de la sociedad.

Se entiende por contrapartes de Personal Soft a sus empleados, clientes, proveedores, miembros de junta directiva y accionistas, y en general a cualquier persona, sea natural o jurídica que sostenga una relación laboral o comercial con esta.

# DEFINICIONES CLAVE

## LAVADO DE ACTIVOS

Es el proceso de hacer que dinero sucio parezca limpio, haciendo que las organizaciones criminales puedan hacer uso de dichos recursos y en algunos casos obtener ganancias sobre los mismos.

DELITOS RELACIONADOS CON EL LA: secuestro, narcotráfico, trata de personas, extorsión, rebelión, corrupción, tráfico de armas, trata de personas, etc.

## FINANCIACIÓN DEL TERRORISMO - FPADM

Relacionada con los fondos, bienes o recursos a los que acceden las organizaciones terroristas o los terroristas para poder costear sus actividades.

# DEFINICIONES CLAVE

## FINANCIAMIENTO DE LA PROLIFERACION DE ARMAS DE DESTRUCCION MASIVA

Todo acto que provea fondos o utilice servicios financieros, en todo o en parte, para la fabricación, adquisición, posesión, desarrollo, exportación, trasiego de material, fraccionamiento, transporte, transferencia, depósito o uso de armas nucleares, químicas o biológicas, sus medios de lanzamiento y otros materiales relacionados en contravención de las leyes nacionales o internacionales.

# ELEMENTOS DEL SAGRILAFT

1. Manual de procedimientos (incluye: políticas, controles y funciones)
2. Matriz de riesgos (identificación /calificación de riesgos por impacto y probabilidad)
3. Herramientas tecnológicas: (buscador / segmentación)
4. Debida Diligencia: Formatos de vinculación / actualización
5. Cláusulas de contratos y declaraciones
6. Oficial de cumplimiento
7. Divulgación y Capacitación
8. Monitoreo

# POLÍTICAS PARA LA PREVENCIÓN, LA GESTIÓN Y AUTOCONTROL DEL RIESGO DE LA/FT/FPADM

Dentro del manual de Procedimientos encontrarán las siguientes políticas

## POLÍTICAS GENERALES

Los empleados de La Empresa se obligan igualmente a seguir los lineamientos internos y a adoptar comportamientos que revelen el estricto cumplimiento de la ley y en especial aquellas que hacen referencia a la prevención del riesgo LA/FT/FPADM.

## POLÍTICAS ESPECÍFICAS

- Política de conocimiento clientes
- Política de conocimiento de proveedores
- Política de conocimiento de empleados y personal en proceso de selección
- Política de conocimiento de Accionistas
- Políticas adicionales para operaciones generales en PERSONAL SOFT

# PROTÉJASE

**DUDE**  
de “negocios  
fáciles”

**NUNCA**  
preste su nombre

**NUNCA**  
preste sus  
productos  
financieros





# PROTÉJASE



## SIEMPRE

pregunte el origen  
de los bienes y el  
dinero

## VERIFIQUE

con quién va a  
hacer el negocio

## SIEMPRE

documente las  
transacciones que  
realice

# ETAPAS DEL SAGRILAFT

RIESGO OPERATIVO

Comunicación y Monitoreo

Contextualización

RIESGO REPUTACIONAL

Tratamiento

Identificación

RIESGO LEGAL

Análisis y Medición

RIESGO DE CONTAGIO

Riesgo es cualquier **situación** que en caso de suceder puede desviar el cumplimiento de los **objetivos**.

# ETAPAS DE LA IMPLEMENTACIÓN DEL CONTROL DE RIESGO

**1. IDENTIFICAR EL RIESGO LA/FT/FPADM:** Implementar los mecanismos que le permitan un adecuado conocimiento, identificación e individualización de los Factores de Riesgo LA/FT/FPADM.

**2. EVALUAR EL RIESGO:** Una vez identificado el Riesgo, se debe medir la probabilidad de ocurrencia del Riesgo Inherente frente a cada uno de los Factores de Riesgo LA/FT/FPADM, así como el impacto en caso de materializarse.



# ETAPAS DE LA IMPLEMENTACIÓN DEL CONTROL DE RIESGO

**3. CONTROLAR EL RIESGO:** Tomar las Medidas Razonables para el control del Riesgo Inherente al que se vean expuestas.

**4. MONITOREAR EL RIESGO:** Ejercer vigilancia respecto del perfil de riesgo y, en general, estar en condiciones de detectar Operaciones Inusuales y Operaciones Sospechosas.



# LOS RIESGOS

**RIESGO DE CONTAGIO:** posibilidad de pérdida que una Empresa puede sufrir, directa o indirectamente, por una acción o experiencia de una Contraparte.

**RIESGO LEGAL:** posibilidad de pérdida de una Empresa al ser sancionada u obligada a indemnizar daños como resultado del incumplimiento de normas y obligaciones contractuales.

**RIESGO OPERATIVO:** posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

**RIESGO REPUTACIONAL:** posibilidad de pérdida de una Empresa por desprestigio, mala imagen, publicidad negativa, respecto de la organización y sus prácticas de negocios, que cause pérdida de clientes, disminución de ingresos o procesos judiciales.

# MEDIDAS DE DEBIDA DILIGENCIA

• Uno de los principales instrumentos para prevenir y controlar los Riesgos LA/FT/FPADM a los que se encuentra expuesta una Empresa Obligada, es la aplicación de medidas de Debida Diligencia.

¿Qué es la debida diligencia?

Consiste en poder conocer e identificar plenamente a las CONTRAPARTES (accionistas, clientes, empleados, proveedores) con las que se relaciona PERSONAL SOFT.

En las personas jurídicas la debida diligencia se extiende hasta llegar a los beneficiarios finales con 5% de participación accionaria o control de la sociedad.

- Se realiza a través del diligenciamiento de formatos de vinculación y solicitud de documentación anexa.
- Chequeo en listas de control y medios públicos
- Segmentación de los factores de riesgo para identificar señales de alerta
- Actualización de esta debida diligencia es cada 2 años.

# DEBIDA DILIGENCIA INTENSIFICADA

¿Qué es la debida diligencia Intensificada? Consiste en tomar medidas adicionales y con mayor intensidad para el conocimiento de la contraparte, su negocio, operaciones y productos.

La debida diligencia intensificada se debe realizar en tres casos:

- Contrapartes u operaciones que en el interior de PERSONAL SOFT se califiquen como de mayor riesgo.
- PEP: (Persona expuesta Políticamente) hasta segundo grado de afinidad, segundo de consanguinidad , primero civil y asociados cercanos.
- Contrapartes ubicadas en países no cooperantes y jurisdicciones de alto riesgo.

La actualización de información de contrapartes con DDI se hace cada año.

# PEP: PERSONAS EXPUESAS POLÍTICAMENTE

## ¿Quiénes son PEP?

Son los servidores públicos de cualquier sistema de nomenclatura y clasificación de empleos de la administración pública nacional y territorial, cuando tengan asignadas o delegadas funciones de expedición de normas o regulaciones, dirección general, formulación de políticas institucionales y de adopción de planes, programas y proyectos, manejo directo de bienes, dineros o valores del Estado, administración de justicia o facultades administrativo sancionatorias, y los particulares que tengan a su cargo la dirección o manejo de recursos en los movimientos o partidos políticos.

Estas funciones podrán ser ejercidas a través de ordenación de gasto, contratación pública, gerencia de proyectos de inversión, pagos, liquidaciones, administración de bienes muebles e inmuebles.

- Son considerados PEP las personas que de manera enunciativa se encuentran en el Artículo 2 del Decreto 830 del 26 de julio de 2021.
- Los PEP informarán su cargo, fecha de vinculación y fecha de desvinculación durante la debida diligencia realizada en los procesos de vinculación, monitoreo y actualización de los datos del cliente.
- Los PEP mantendrán esta marcación, hasta después de 2 años de dejar el cargo.
- Se les realizará en todos los casos DDI extendida a sus familiares y asociados cercanos.



# LISTAS DE CONTROL

Las **listas vinculantes** para Colombia son las siguientes:

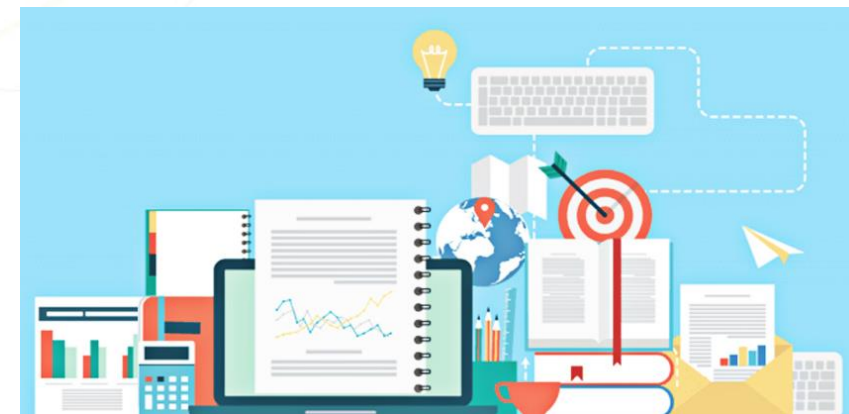
- Lista del consejo de Seguridad de las Naciones Unidas.
- Listas de terroristas de los Estados Unidos de América.
- La lista de la Unión Europea de Organizaciones Terroristas y de Personas Catalogadas como Terroristas.

Las **listas restrictivas** son las listas públicas que relacionan a personas, organizaciones o países que de acuerdo con el organismo que las publica, pueden estar vinculadas con actividades de lavado de activos, financiación del terrorismo u otros delitos, faltas administrativas o de responsabilidad fiscal.

# DOCUMENTAR TODO

Las actividades adoptadas por PERSONAL SOFT S.A.S., en desarrollo de la implementación y ejecución del sistema SAGRILAFT, deben reposar en documentos y registros que garanticen la integridad, oportunidad, confiabilidad, reserva y disponibilidad de la información.

**NOTA:** el desarrollo e implementación del SAGRILAFT por parte de PERSONAL SOFT S.A.S. deberá respetar las disposiciones legales en materia de protección de datos personales contenidas en las Leyes 1266 de 2008, 1581 de 2012, y demás normas aplicables.



# LOS REPORTES

Se deben establecer herramientas y aplicativos, preferiblemente tecnológicos, que permitan identificar Operaciones Inusuales y Operaciones Sospechosas.

Una vez identificada y analizada una Operación Inusual o una Operación Sospechosa, deberán conservarse los soportes que dieron lugar a calificarla en una u otra categoría.

## ¿ANTE QUIÉN SE HACE EL REPORTE?

Las empresa deberán reportarle a la UIAF todas las Operaciones Sospechosas que detecten en el giro ordinario de sus negocios o actividades.

El reporte deberá hacerse de manera inmediata y con naturaleza de ROS, a través de la plataforma denominada SIREL de la UIAF .

# LOS REPORTES

Se deben establecer herramientas y aplicativos, preferiblemente tecnológicos, que permitan identificar Operaciones Inusuales y Operaciones Sospechosas.

Se entiende por **Operación Inusual** todas aquellas operaciones, comportamientos o transacciones que se salgan de la normalidad o habitualidad en el comportamiento de una contraparte.

**Operación Sospechosa** Se entiende por todas aquellas operaciones inusuales que no puedan ser completamente justificadas.

Una vez identificada y analizada una Operación Inusual o una Operación Sospechosa, deberán conservarse los soportes que dieron lugar a calificarla en una u otra categoría.

## ¿ANTE QUIÉN SE HACE EL REPORTE?

Las empresa deberán reportarle a la UIAF ( Unidad de investigación y análisis financiero) todas las Operaciones Sospechosas que detecten en el giro ordinario de sus negocios o actividades.

El reporte deberá hacerse de manera inmediata y con naturaleza de ROS (Reporte de Operación Sospechosa), a través de la plataforma denominada SIREL de la UIAF .

# EL OFICIAL DE CUMPLIMIENTO

El Oficial de Cumplimiento debe participar activamente en los procedimientos de diseño, dirección, implementación, auditoría, verificación del cumplimiento y monitoreo del SAGRILAFT, y estar en capacidad de tomar decisiones frente a la gestión del Riesgo LA/FT/FPADM.

- ✓ Verificar el cumplimiento de los procedimientos de Debida Diligencia
- ✓ Diseñar las metodologías de segmentación, identificación, medición y control del riesgo de LA/FT que formarán parte del Sistema
- ✓ Velar por el adecuado archivo de los soportes documentales y demás información relativa a la gestión y prevención del riesgo LA/FT.
- ✓ Rendir informes a la Asamblea , por lo menos una vez al año.
- ✓ Realizar el reporte de las Operaciones Sospechosas (ROS), Reporte de Ausencia de Operaciones Sospechosas (AROS), I a la UIAF y cualquier otro reporte o informe, en los términos del capítulo X.
- ✓ Contar con el apoyo de un equipo de trabajo humano y técnico.
- ✓ No pertenecer a la administración o a los órganos sociales, ni de auditoría o control interno o externo.
- ✓ No fungir como Oficial de Cumplimiento en más de 10 empresas obligadas (en caso de tercerización). Se deberá verificar que el OC no actúa como tal en empresas que compiten entre sí.

# ASAMBLEA GENERAL DE ACCIONISTAS

- ✓ Establecer y aprobar para PERSONAL SOFT una política LA/FT/FPADM.
- ✓ Aprobar el SAGRILAFT y sus actualizaciones, presentadas por el Representante Legal.
- ✓ Aprobar el manual de procedimientos SAGRILAFT y sus actualizaciones.
- ✓ Designar al Oficial de Cumplimiento y su respectivo suplente si es procedente.
- ✓ Ordenar y garantizar los recursos técnicos, logísticos y humanos necesarios para implementar y mantener en funcionamiento el SAGRILAFT, según los requerimientos del Oficial de Cumplimiento.
- ✓ Establecer los criterios para aprobar la vinculación de contraparte cuando esta sea un PEP o delegarlo en el oficial de cumplimiento o representante legal.
- ✓ Establecer pautas y determinar los responsables de realizar auditorías sobre el cumplimiento y efectividad del SAGRILAFT en caso de que así se determine.
- ✓ Verificar la capacidad y disponibilidad del Oficial de Cumplimiento.

# REPRESENTANTE LEGAL

- ✓ Presentar con el oficial de cumplimiento, para aprobación de la asamblea de accionistas la propuesta del SAGRILAFT y sus actualizaciones, así como su respectivo manual de procedimientos.
- ✓ Estudiar los resultados de la evaluación del Riesgo LA/FT/FPADM efectuada por el oficial de cumplimiento y establecer los planes de acción que correspondan.
- ✓ Asignar de manera eficiente los recursos técnicos y humanos, determinados por la asamblea, necesarios para implementar el SAGRILAFT.
- ✓ Verificar que el oficial de cumplimiento cuente con la disponibilidad y capacidad necesaria para desarrollar sus funciones.
- ✓ Prestar efectivo, eficiente y oportuno apoyo al oficial de cumplimiento en el diseño, dirección, supervisión y monitoreo del SAGRILAFT.
- ✓ Presentar a la asamblea los reportes, solicitudes y alertas que considere que deban ser tratados por dichos órganos y que estén relacionados con el SAGRILAFT.
- ✓ Asegurarse de que las actividades que resulten del desarrollo del SAGRILAFT se encuentran debidamente documentadas, de modo que se permita que la información responda a unos criterios de integridad, confiabilidad, disponibilidad, cumplimiento, efectividad, eficiencia y confidencialidad.
- ✓ Certificar ante la Superintendencia de Sociedades el cumplimiento de lo previsto en el Capítulo X de la Circular Básica Jurídica de la Superintendencia de Sociedades.

# CAPACITACIONES

PERSONAL SOFT, tendrá como principal instrumento de comunicación del SAGRILAFT un plan de capacitación, el cual cumplirá con las siguientes condiciones:

- Tendrá una periodicidad anual
- Será ejecutado en los procesos de inducción de nuevos empleados y terceros que desarrollen actividades con impacto y riesgo alto para la empresa.
- Se dejará registro de los asistentes
- Podrá tener mecanismos de evaluación de los resultados obtenidos, con el fin de determinar la eficacia de los programas y el entendimiento de los objetivos propuestos.



# SANCIONES

## 1. ADMINISTRATIVAS

El incumplimiento por parte de PERSONAL SOFT y/o sus administradores del SAGRILAFT dará lugar a la imposición de las siguientes sanciones y multas por parte de la Superintendencia de Sociedades, el numeral 3 del artículo 86 de la Ley 222 de 1995 señala que “La Superintendencia de Sociedades está facultada para imponer sanciones o multas, sucesivas o no, hasta de doscientos salarios mínimos legales mensuales, cualquiera sea el caso, a quienes incumplan sus órdenes, la ley o los estatutos”.

## 2. PENALES

- Por lavado de activos: prisión entre 10 - 30 años y multa entre 500 - 50.000 SMMLV
- Por financiación del terrorismo: prisión entre 13 – 22 años y multa entre 1.300 a 15.000 SMMLV
- Por omisión de denuncia: prisión entre 3 y 8 años.

