1. OBJETIVO

Establecer los requisitos generales para la implementación de la metodología de gestión del riesgo que involucra la determinación del contexto, la identificación, análisis, medición, evaluación tratamiento, comunicación y monitoreo de los riesgos.

2. ALCANCE

Aplica a un amplio rango de actividades incluyendo estrategias, decisiones, operaciones, procesos, funciones, productos, proyectos y servicios aplica a riesgos de Lavado de activos, financiación al Terrorismo y financiación de la Proliferación de armas de destrucción masiva, según Circular Externa No. 100-000016 del 24 de diciembre de 2020 y NTC ISO 31000 Gestión del Riesgo

3. DEFINICIONES

Calificación del riesgo

Ejercicio en el cual se realiza la estimación de la probabilidad de ocurrencia de un riesgo y el impacto que puede causar la materialización del mismo.

Causas (factores internos o externos)

Son los medios, las circunstancias y agentes generadores que tienen la capacidad de originar un riesgo.

Contexto estratégico

Son las condiciones internas y externas de la compañía, que definen loseventos de oportunidad o amenaza que afectan positiva o negativamente el cumplimiento de la misión, visión y objetivos de la compañía.

Contraparte

Es cualquier persona natural o jurídica con la que la empresa tenga vínculos comerciales, de negocios, contractuales o jurídicos de cualquier orden. Entre otros, son contrapartes los accionistas, empleados, clientes, contratistas y proveedores de productos de la empresa.

Control

Medida que mantiene y/o modifica un riesgo

Expertos
Se refiere a los líderes de proceso o área que conocen a profundidad las operaciones y actividades de la empresa.

Gestión del riesgo
Comprende el conjunto de elementos de control y sus interrelaciones, para que la compañía evalúe e intervenga aquellos eventos, tanto internos como externos, que puedan afectar de manera positiva o negativa el logro de sus objetivos organizacionales.

Impacto
Resultado de un evento que afecta los objetivos. Un evento puede generar un rango de consecuencias, las cuales se pueden expresar cualitativa o cuantitativamente.

Matriz de riesgos
Herramienta que permite clasificar y visualizar los riesgos mediante la definición de categorías de consecuencias y su probabilidad de ocurrencia.

Oficial de Cumplimiento
Es la persona natural designada, que está encargada de promover, desarrollar y velar por el cumplimiento de los procedimientos específicos de prevención, actualización y mitigación del Riesgo LA/FT/FPADM.

Oportunidad
Circunstancia, momento o medio oportunos para realizar o conseguir algo, se pueden clasificar como oportunidades los riesgos positivos.

Probabilidad
Es la oportunidad de que algo suceda, medido o determinado de manera objetiva (basado en datos y hechos históricos) o subjetiva (bajo criterios de experiencia o experticia de quien analiza), utilizando términos generales o matemáticos (como la probabilidad numérica) o la frecuencia en un periodo de tiempo determinado.

Proceso
Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados.

Riesgo
Es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos organizacionales o del proceso. Se expresa en términos de probabilidad e impacto. Puede ser positivo o negativo, el riesgo positivo puede llamarse también oportunidad.

Riesgo Inherente
Riesgo al que se enfrenta una compañía en ausencia de acciones por parte de la dirección para modificar su probabilidad o impacto.

Riesgo LA/FT/FPADM
Es la posibilidad de pérdida o daño que puede sufrir la empresa por su propensión a ser utilizada directamente o a través de sus operaciones como instrumento para el Lavado de Activos y/o canalización de recursos hacia la realización de actividades terroristas o el Financiamiento de la Proliferación de Armas de Destrucción Masiva, o cuando se pretenda el ocultamiento de Activos provenientes de dichas actividades. Las contingencias inherentes al LA/FT/FPADM se materializan a través de riesgos tales como el Riesgo de Contagio, Riesgo Legal, Riesgo Operativo, Riesgo reputacional y los demás a los que se expone la empresa, con el consecuente efecto económico negativo que ello puede representar para su estabilidad financiera, cuando es utilizada para tales actividades.

Riesgo Residual
Nivel de riesgo que permanece luego de tomar medidas de tratamiento y controlde riesgo.

SAGRILAFT
Es el sistema de autocontrol y gestión del riesgo integral de LA/FT/FPADM establecido en la Circular Externa No. 100-000016 del 24 de diciembre de 2020 expedida por Superintendencia de Sociedades.

4. CONDICIONES GENERALES
N.A

5. CONTENIDO
- Para llevar a cabo la metodología de Gestión del Riesgo se deben tener en cuenta los elementos principales que son los siguientes:

    a. **Establecer el contexto:** Establecer el contexto estratégico, organizacional y de gestión del riesgo en el cual ocurrirá el resto del proceso. Es conveniente que se establezcan criterios contra los cuales va a de evaluar el riesgo, y se debe definir la estructura del análisis.

    b. **Identificar riesgos:** Identificar qué, por qué y cómo pueden surgir elementos como base para análisis posterior.

    c. **Analizar riesgos:** Determinar los controles existentes y analizar los riesgos en términos de consecuencia y posibilidad en el contexto de estos controles. El análisis debe considerar la gama de consecuencias potenciales y la posibilidad de que éstas ocurran. Se pueden combinar la consecuencia y la posibilidad para producir un nivel estimado de

riesgo.

d. **Evaluar los riesgos:** Comparar los niveles estimados de riesgo, contra los criterios preestablecidos. Esto posibilita que los riesgos sean clasificados de modo que se identifiquen prioridades de gestión. Si los niveles de riesgo establecido son bajos, entonces los riesgos pueden encajar en una categoría aceptable, y es posible que no se requiera tratamiento.

e. **Tratar los riesgos** : Aceptar y monitorear los riesgos de baja prioridad. Para los demás riesgos, desarrollar e implementar un plan de gestión específico que incluya considerar el suministro de recursos

f. **Monitorear y revisar**: Monitorear y revisar el desempeño del sistema de gestión del riesgo y los cambios que pudieran afectarlo.

g. **Comunicar y consultar**: Comunicar y consultar con las partes interesadas, internas y externas, según sea apropiado, en cada etapa del proceso de gestión del riesgo y con relación al proceso en conjunto.

- Para el establecimiento del contexto se debe realizar el siguiente análisis:

✓ **Determinación de los factores de riesgo LA/FT/FPADM**

Como análisis del contexto se determinan los factores de riesgo que deben ser objeto de autocontrol dado que cada empresa cuenta con sus distintos factores de riesgo, de acuerdo con la Circular Externa No. 16/2020 los factores de riesgo son los posibles elementos o causas generadoras del riesgo LA/FT/FPADM para cualquier empresa, se deberán identificar teniendo en cuenta: las contrapartes, los productos y servicios, los canales y las jurisdicciones.

Las contrapartes: se refiere a cualquier persona natural o jurídica con la que la empresa tenga vínculos comerciales, de negocios, contractuales o jurídicos de cualquier orden. Son contrapartes los clientes, proveedores/contratista, empleados y socios/accionistas de la empresa estos tienen clasificaciones según el factor de riesgo.

- **Clientes:** Se consideran como clientes para la identificación de los riesgos aquellas personas naturales o jurídicas que tengan una vinculación o relación contractual con la empresa y que entreguen a esta dinero, bienes o servicios como resultado del acuerdo establecido entre las partes.

- **Proveedores:** Es toda persona natural o jurídica con la cual la empresa establece y/o mantiene una relación contractual y/o comercial.

- **Accionistas**: Persona natural o jurídica que posee una o más acciones en la empresa por tanto, esa titularidad le otorgará la condición de propietario y socio. Los accionistas tienen el derecho a ejercer el voto, y serán responsables por hacer seguimiento a las decisiones adoptadas por los administradores de la empresa, siempre que las mismas sean ejercidas dentro del ámbito de sus funciones.

Clasificación para clientes, proveedores y accionistas:

- ✓ **Clasificación No. 1:** Corresponde al tipo de contraparte (clientes, proveedores/contratista, empleados y socios/accionistas)
- ✓ **Clasificación No. 2:** Se refiere al tipo de persona (natural, jurídica)
- ✓ **Clasificación No. 3:** Especifica el sector económico en el cual se desarrolla la contraparte.
- ✓ **Clasificación No. 4:** Se debe indicar si la contraparte pertenece al sector privado o público
- ✓ **Clasificación No. 5:** Muestra el medio de pago por el cual se realiza la transacción. (cheques, efectivo, transferencia bancaria)

- **Empleados**: Es la persona que brinda sus servicios a cambio de un salario por parte de un empleador. Así, los detalles de este vínculo son definidos en un contrato (verbal o escrito).

Clasificación para empleados:

- ✓ **Clasificación No. 1:** Corresponde al tipo de contraparte (clientes, proveedores/contratista, empleados y socios/accionistas)
- ✓ **Clasificación No. 2:** Indica el tipo de vinculación (directa o indirecta)
- ✓ **Clasificación No. 3:** Revela el área a la cual pertenece el empleado (administrativa, operativa)
- ✓ **Clasificación No. 4:** Enseña el tipo de contratación (fijo , indefinido)
- ✓ **Clasificación No. 5:** Muestra el medio de pago por el cual se remunera al empleado. (cheques, efectivo, transferencia bancaria)

Los productos y servicios: son los bienes y servicios que produce, comercializa, transforma u ofrece la empresa o adquiere de un tercero.

Clasificación para productos y/o servicios:

- ✓ **Clasificación No. 1:** Corresponde a los productos o servicios que ofrece la compañía
- ✓ **Clasificación No. 2:** Indica el tipo de productos o de servicios que se presta
- ✓ **Clasificación No. 3:** Enumerar de forma general los productos de venta

Los canales de distribución: es el medio por el cual se ofrece el producto o servicio.

Clasificación para canales de distribución:

- ✓ **Clasificación No. 1:** Se refiere al tipo de contratación con el servicio de transporte (directa – indirecta)
- ✓ **Clasificación No. 2:** Corresponde al producto o servicio que se transporta
- ✓ **Clasificación No. 3:** Es el tipo de canal de distribución ((**Directa**: Puntos de venta, Agentes Comerciales, E- commerce, Licitaciones, etc; **Indirecta**: Distribuidores, Agentes, Almacenes de cadena, Franquicias, Aliados Estratégicos, Intermediarios, Agentes Transportadores entre otros).

Las jurisdicciones: Son las regiones, zonas, áreas o países en los que opera la empresa o en donde se encuentra el cliente o contraparte.

Clasificación para jurisdicciones:

- ✓ **Clasificación No. 1:** Indica el tipo de relación comercial (ventas – compras)
- ✓ **Clasificación No. 2:** Revela el lugar donde se realiza la relación comercial (nacional – internacional)
- ✓ **Clasificación No. 3:** Indica el país en el cual se lleva a cabo la negociación
- ✓ **Clasificación No. 4:** Indica la ciudad en el cual se lleva a cabo la negociación
- ✓ **Clasificación No. 5:** Se establece el nivel de riesgo de acuerdo con la jurisdicción

Estos factores de riesgo se identifican en la matriz de riesgo en la pestaña ***Factores de riesgo,*** el proceso de identificación de factores se realiza con los lideres de proceso; según las clasificaciones anteriores, la finalidad de esta determinación de factores de riesgo es conocer el contexto externo de la empresa e identificar los riesgos inherentes de acuerdo con sus actividades

- **Identificación de los riesgos**

Esta etapa busca identificar los riesgos de LA/FT/FPADM que se pueden presentar en las actividades que realiza la empresa es decir en los diferentes procesos previstos en la empresa para el adecuado desempeño de su objeto social. La empresa debe aplicar herramientas y técnicas para la identificación del riesgo que sean adecuadas a sus objetivos, expectativas y a los riesgos que se enfrenta en cuanto al LA/FT/FPADM. En la identificación del riesgo se deben involucrar las personas asignadas para tal fin con un conocimiento apropiado.

La etapa de identificación de los riesgos debe realizarse previamente cuando exista una modificación de los factores de riesgo, como podría ser el caso del lanzamiento de un nuevo tipo de producto, la modificación de sus características, la incursión en un nuevo mercado, la apertura de operaciones en nuevas jurisdicciones, y/o el lanzamiento o modificación de los canales de distribución.

Para identificar los eventos de riesgo de LA/FT/FPADM y sus riesgos asociados se revisará cada una de las actividades que conforman los procesos en los cuales se ha identificado la posibilidad de ocurrencia de eventos de riesgos de LA/FT/FPADM para conformar la matriz de riesgos. Empleando así mismo las siguientes fuentes de información:

✓ **Entrevistas con líderes de procesos:** En la identificación del riesgo se deben involucrar las personas asignadas para tal fin con un conocimiento apropiado.

✓ **Señales de alerta:** Señales de alerta y/o operaciones Inusuales identificadas por los empleados de la empresa.

✓ **Cartillas:** Documentos de tipologías y señales de alerta publicados por la UIAF-Colombia y/o por cualquier entidad especializada.

✓ **Otras fuentes**

- OCDE: Organización para la Cooperación y Desarrollo Económico
- GAFI: Grupo de Acción Financiera Internacional
- GAFILAT: Grupo de Acción Financiera Latinoamericana (Antes GAFISUD)
- OEA: Organización de los Estados Americanos
- Comité de Basilea

- **Responsables de la identificación de riesgos**

El Oficial de Cumplimiento junto con los líderes de los procesos son los responsables de la identificación de riesgos de LA/FT/FPADM y sus riesgos asociados, definidos en un monitoreo anual para su estudio y reconocimiento o cuando sea necesario. Para la identificación de los riesgos se efectúan reuniones con los líderes de los procesos basándose en su conocimiento de la operación de la empresa, se identifican los riesgos LA/FT/FPADM relacionados con los factores de riesgo. El insumo básico de este proceso será la conformación de grupos de trabajo integrados por personas conocedoras de las actividades que desarrolla la empresa la experiencia y la capacitación en temas relacionados con la prevención y control de

LA/FT/FPADM.

- **Registro de Riesgos**

Una vez identificados los riesgos inherentes en cada uno de los factores, estos se deben registrar en la matriz de riesgos en la pestaña ***Expertos***; en la casilla código se procede a enumerar los posibles eventos de riesgo identificados; teniendo claro los grupos de interés con los que tiene relación la empresa, en la columna riesgo se debe describir de forma precisa y clara como considera que puede presentarse el riesgo. Posteriormente a la identificación del riesgo, se procede a vincular el factor de riesgo que puede ser la causa generadora del riesgo.

- **Análisis de los riesgos**

Los riesgos identificados y codificados en la pestaña de expertos con su respectiva medición se deben vincular al proceso y al factor de riesgo correspondiente en la pestaña ***Elaboración – Mapa de riesgos***. El análisis de riesgo incluye considerar las causas, las consecuencias y la posibilidad de que estas consecuencias ocurran.

La causa del riesgo hace referencia a los factores o condiciones que contribuyen al surgimiento o materialización de un riesgo específico relacionado con el LA/FT/FPADM. Estas causas pueden incluir una variedad de elementos, como deficiencias en los controles internos, falta de capacitación del personal, cambios en la regulación, presencia de clientes de alto riesgo, entre otros. Para efectos de identificar las causas sobre cada riesgo, se utilizan las siguientes palabras claves como: *Falta de, inadecuado, ausencia de, fallas en, exceso de,* etc.

Las consecuencias representan las pérdidas que la ocurrencia del riesgo le acarrea a la empresa que se detallan en la parametrización de la tabla de impacto.

- **Medición del riesgo inherente por expertos**

Partiendo del objetivo principal que corresponde a la medición acertada del riesgo inherente en términos de probabilidad e impacto, en la matriz se han creado espacios para que el experto o líder del proceso califique cada riesgo identificado y los riesgos asociados de acuerdo con su conocimiento y experiencia en el desarrollo de las actividades de la empresa.

El impacto se determina con base en el nivel de pérdida o daño que podría resultar en el caso de materializarse el riesgo y su consecuencia en los objetivos del Sistema SAGRILAFT y en los riesgos asociados.

Con el fin de establecer un estándar de medición los criterios pueden ser subjetivos, esto depende de la particularidad del riesgo, los antecedentes en cada uno de los procesos y los equipos de gestión. Para fines de estandarización se califica la probabilidad y el impacto según las siguientes tablas:

Escala de medición probabilidad

		Posibilidad	Frecuencia
Probabilidad	Muy baja (20%)	Insignificante posibilidad de que el evento ocurra.	Cada 5 años
	Baja (40%)	Alguna posibilidad de que el evento ocurra.	Anual
	Media (60%)	Posiblemente ocurra varias veces.	Semestral
	Alta (80%)	Que ocurra la mayoría de veces.	Mensual
	Muy alta (100%)	Que ocurra todas las veces.	Diario

Al seleccionar el tipo de riesgo asociado con el cual se relaciona el riesgo de LA/FT/FPADM identificado, estos riesgos tienen efectos negativos que pueden ser representativos para la estabilidad financiera y comercial de la empresa, a su vez pueden afectar el buen nombre de la empresa, su productividad, competitividad y perdurabilidad. Los riesgos asociados se clasifican en:

Riesgo Reputacional: Relaciona la afectación del buen nombre de una empresa al ser expuesta a situaciones o procesos que impliquen una mala imagen donde se vea afectada mediante publicidad negativa en redes sociales, escándalos en medios de comunicación sobre sus prácticas operaciones, sea verídica o no que causen pérdida de clientes o disminución en los activos, incluso procesos judiciales a raíz de estos desprestigios en los que la empresa se encuentra implicada.

Riesgo Legal: Hace referencia a la posibilidad de ser sancionados o estar obligados por la ley a indemnizar daños como consecuencia del incumplimiento de las normas establecidas, regulaciones acordadas o cláusulas rotas en obligaciones contractuales. Surge como consecuencia de faltas, fallas o incumplimiento derivados de malintencionadas, negligencias o actos involuntarios en el marco normativo exigido, sea en la contratación o a nivel transaccional con las contrapartes. Ejemplos de estos riesgos podrían ser procesos penales, demandas civiles, multas y sanciones.

Riesgo Operativo: Se define como la posibilidad de que ocurran pérdidas financieras en la compañía al ejecutar sus operaciones diarias. Este puede ser causado por fallas humanas, fraude externo o interno, fallas tecnológicas o presencia de eventos imprevistos. Las consecuencias pueden ser tales como el cierre temporal de la empresa, embargos por proceso penal, ocupaciones con fines de extinción de dominio, entre otras.

Riesgo de Contagio: Está relacionado con el impacto reputacional, legal o económico que puede sufrir una empresa cuando se relaciona con las acciones o experiencias de los actores con quien la

que la empresa tenga vínculos de negocios, comerciales, jurídicos de cualquier orden o contractuales ya sea un cliente o proveedor se encuentra implicado en un proceso o experiencia que estén relacionadas con los delitos LA/FT/FPADM. Como por ejemplo la extensión de problemas económicos a empresas controladas o controladoras.

Escala de medición impacto

Impacto	TABLA DE IMPACTO Legal
Leve (20%)	Requerimiento
Menor (40%)	Amonestación
Medio (60%)	Suspensión, inhabilitación de administradores, oficial de cumplimiento y otros funcionarios
Mayor (80%)	Suspensión o cierre parcial de operaciones, actividades o remoción de administradores del negocio por decisión de los reguladores
Catastrófico (100%)	Cancelación de la matrícula / cierre permanente de operaciones y actividades de negocio por decisión de los reguladores

Impacto	TABLA DE IMPACTO Contagio
Leve (20%)	No produce efecto contagio
Menor (40%)	Puede producir efecto entre línea(s) de servicio(s) relacionadas con la Compañía.
Medio (60%)	Puede producir efecto contagio entre empresas o entidades relacionadas con la Compañía.
Mayor (80%)	Puede producir efecto contagio significativo entre empresas o entidades relacionadas con la Compañía.
Catastrófico (100%)	Puede producir efecto contagio catastrófico entre empresas o entidades relacionadas con la Compañía.

Impacto	TABLA DE IMPACTO Operacional
Leve (20%)	No produce afectación.
Menor (40%)	Afectación de un proceso específico, recurso, infraestructura o tecnología para continuar con la operación.
Medio (60%)	Afectación parcial de algunos procesos, recursos, infraestructura o tecnología para continuar con la operación.
Mayor (80%)	Afectación temporal de procesos, recursos, infraestructura o tecnología para continuar con la operación.
Catastrófico (100%)	Imposibilidad de contar con procesos, recursos, infraestructura o tecnología para continuar con la operación.

Impacto	TABLA DE IMPACTO Reputacional
Leve (20%)	El riesgo afecta la imagen de algún área de la entidad
Menor (40%)	El riesgo afecta la imagen de la entidad internamente; de conocimiento general a nivel interno, accionistas y/o de proveedores
Medio (60%)	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia, frente al logro de los objetivos.
Mayor (80%)	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental y/o municipal.
Catastrófico (100%)	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

La calificación del riesgo dada por los expertos proporciona el resultado de la severidad del riesgo que es otra métrica clave en el análisis cuantitativo del riesgo y permite ubicar cada riesgo en el mapa térmico (Probabilidad x impacto= Severidad del riesgo); y se clasifican según la siguiente tabla

RIESGO EXTREMO

Riesgo Extremo: se refiere a aquellos riesgos que tienen el potencial de causar un daño significativo o de gran magnitud a la empresa en términos de LA/FT/FPADM. Estos riesgos suelen ser identificados como los más críticos y urgentes de abordar, requiriendo medidas de mitigación inmediatas y efectivas.

RIESGO ALTO

Riesgo Alto: Se refiere a riesgos que tienen el potencial de causar un daño significativo a la empresa en términos de LA/FT/FPADM, aunque no tan crítico como el riesgo extremo. Estos riesgos requieren medidas de mitigación sólidas y periódicas para reducir su impacto.

RIESGO MODERADO

Riesgo Moderado: Son riesgos que tienen el potencial de causar un daño moderado a la empresa en términos de LA/FT/FPADM. Requieren medidas de mitigación adecuadas y regulares para controlar su impacto y prevenir posibles consecuencias **negativas.**

RIESGO BAJO

Riesgo Bajo: Se refiere a riesgos que tienen un impacto limitado en la empresa en términos de LA/FT/FPADM. Aunque estos riesgos son menos críticos, aun así requieren medidas de mitigación básicas para garantizar el cumplimiento normativo y la integridad de la empresa.

	SEVERIDAD DEL RIESGO			
Resultado	RIESGO BAJO	Son los riesgos que son menos críticos, aún así requieren medidas de mitigación básicas para garantizar el cumplimiento normativo y la integridad de la empresa.	10	40
	RIESGO MODERADO	Son los riesgos que requieren medidas de mitigación adecuadas y regulares para controlar su impacto y prevenir posibles consecuencias negativas.	50	100
	RIESGO ALTO	Son los riesgos que requieren medidas de mitigación sólidas y periódicas para reducir su impacto.	110	190
	RIESGO EXTREMO	Son los riesgos más críticos y urgentes de abordar, requiriendo medidas de mitigación inmediatas y efectivas.	200	+

- **Perfil del riesgo**

Son criterios definidos por la empresa para decidir el nivel de aceptación sobre la materialización de los riesgos que han sido identificados previamente. Estos criterios incluyen estimación sobre la probabilidad de ocurrencia y el impacto potencial en los objetivos de la empresa. Así mismo, el perfil de riesgo permite comprender la naturaleza y la magnitud de los riesgos a los que está expuesta la empresa, lo que facilita tomar decisiones acertadas sobre el manejo de los riesgos de una manera efectiva.

Perfil de riesgo aceptado: Se refiere al nivel de riesgo que la empresa está dispuesta a aceptar o tolerar basada en la implicación o posibles afectaciones en el cumplimiento de sus objetivos

estratégicos. Una vez que se establece el perfil de riesgo aceptado, la empresa debe tomar decisiones sobre cómo gestionar los riesgos, priorizando acciones para mitigar los riesgos más significativos, ajustando sus estrategias y operaciones en consecuencia a los resultados obtenidos. El perfil de riesgo se obtiene promediando las calificaciones de la severidad del riesgo, tanto en el mapa térmico inherente como en el residual. El perfil de riesgo en el mapa inherente indica el nivel de exposición frente a riesgos LA/FT/FPADM, que puede fluctuar en el máximo resultado considerando que es un perfil sin controles; no obstante, el resultado obtenido en el mapa residual únicamente puede variar entre bajo y moderado, teniendo en cuenta que los controles establecidos deben ser eficaces y/o efectivos disminuyendo así la severidad del riesgo.

Es importante destacar que el perfil de riesgo aceptado no es estático y puede cambiar con el tiempo a medida que cambian las circunstancias internas y externas de la empresa. Por lo tanto, la gestión de riesgos debe ser un proceso continuo que requiere de monitoreo constante y ajustes oportunos según sea necesario para garantizar que la empresa opere dentro de los límites aceptables de riesgo.

Criterios de medición del perfil de riesgo:

- **Perfil de riesgo aceptado BAJO:** Nivel mínimo de exposición, los controles son eficaces y efectivos.

- **Perfil de riesgo aceptado MODERADO**: Nivel aceptable, siempre y cuando todos los riesgos en el mapa residual se encuentren en "Riesgo Bajo" y/o "Riesgo Moderado". Los controles son adecuados.

- **Perfil de riesgo aceptado ALTO:** Este nivel solo se acepta en el mapa de riesgo inherente, si en algún caso se refleja este nivel en el mapa residual, indica que los controles no son suficientes, es decir se deben revisar los atributos del control.

	PERFIL DEL RIESGO			
Resultado	BAJO	Nivel mínimo de exposición, los controles son eficaces y efectivos.	0	1
	MODERADO	Nivel aceptable, siempre y cuando todos los riesgos en el mapa residual se encuentren en "Riesgo Bajo" y/o "Riesgo Moderado". Los controles son adecuados.	1,1	2
	ALTO	Este nivel solo se acepta en el mapa de riesgo inherente, si en algún caso se refleja este nivel en el mapa residual, indica que los controles no son suficientes, es decir se deben revisar los atributos del control.	2,1	+

- **Tratamiento del riesgo**

El propósito del tratamiento del riesgo es seleccionar e implementar opciones para abordar los riesgos. La selección de las opciones más apropiadas para el tratamiento de los riesgos implica hacer un balance entre los beneficios potenciales, derivado del logro de los objetivos contra costos.

Las siguientes son las estrategias que se pueden considerar según el tratamiento del riesgo:

Reducir: Implica implementar controles y procedimientos para disminuir la probabilidad o el impacto de que ocurra el lavado de activos, financiamiento del terrorismo o financiamiento de la proliferación de armas de destrucción masiva. Esto puede incluir la debida diligencia en las transacciones, la vigilancia de actividades sospechosas y la capacitación del personal para detectar y prevenir estas actividades.

Transferir: Esta estrategia implica trasladar la responsabilidad del riesgo a otra parte, como instituciones financieras, aseguradoras o autoridades reguladoras. Esto puede incluir el uso de servicios de cumplimiento externo o la participación en esquemas de intercambio de información para detectar y mitigar el lavado de activos, financiamiento del terrorismo o financiamiento de la proliferación de armas de destrucción masiva.

Aceptar: Significa reconocer que existe el riesgo de lavado de activos, financiamiento del terrorismo o financiamiento de la proliferación de armas de destrucción masiva y decidir conscientemente no tomar medidas adicionales para mitigarlo. Esto puede suceder cuando el costo o la complejidad de mitigar el riesgo superan los beneficios potenciales, y la organización está dispuesta a aceptar las posibles consecuencias negativas si el riesgo se materializa.

Evitar: Implica tomar medidas para eliminar completamente la posibilidad de que ocurra el lavado de activos, financiamiento del terrorismo o financiamiento de la proliferación de armas de destrucción masiva. Esto puede implicar abstenerse de realizar ciertos tipos de transacciones o negocios que presenten un alto riesgo de ser utilizados para actividades ilícitas.

- **Control de los riesgos**

En esta etapa, la empresa podrá determinar y adoptar los controles o medidas conducentes a controlar el riesgo inherente. Para estos efectos, se definen las metodologías para determinar los controles y su aplicación y se definen los procedimientos para la detección de operaciones inusuales y sospechosas.

Los controles son las políticas, actividades y procedimientos que se desarrollan a través de toda la empresa, para eliminar o mitigar los riesgos adversos, y garantizan que las directrices asumidas por la empresa se lleven a cabo y los riesgos se administren, de tal manera que se cumplan los objetivos.

El control se debe traducir en una disminución de la posibilidad de ocurrencia y/o del impacto del riesgo de LA/FT/FPADM en caso de materializarse. Debe reiterarse que siempre los controles se deben aplicar en todas las etapas de los procesos identificados.

- **Definición y calificación de los atributos de los controles**

El control debe tener un propósito que indique para qué se realiza el control, y que ese propósito conlleve a prevenir las causas que generan el riesgo, podemos tener como propósito las siguientes acciones: verificar, validar, conciliar, comparar, revisar, cotejar. El solo hecho de establecer un procedimiento o contar con una política por sí sola, no va a prevenir o detectar la materialización del riesgo o una de sus causas.

a. Tipo de control: Por la naturaleza de los riesgos a gestionar, los tipos de controles que se sugiere aplicar, son los siguientes:

- ✓ **Controles preventivos**: son la primera barrera de seguridad, y corresponde a aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización.
- ✓ **Controles detectivos**: corresponden a la segunda barrera de seguridad. Es una alarma que se acciona cuando se descubre una situación.
- ✓ **Controles correctivos:** acciones y procedimientos rectificatorios en recurrencia. Comprenden documentación y reportes, sobre supervisión a los asuntos, hasta su reformulación o solución.

b. Implementación de controles: El control debe indicar el cómo se realiza, de tal forma que se pueda evaluar si la forma de ejecutar el control es confiable para la mitigación del riesgo.

- ✓ **Manual:** Actividades de control ejecutadas por una persona.
- ✓ **Automático:** Actividad de control desarrollada de forma totalmente automática donde no interviene el juicio de una persona.

c. Documentación de controles: La documentación de procesos consiste en llevar un registro o paso a paso de las actividades que permiten cumplir el proceso. El objetivo es aprender de la implementación para adaptar la estrategia y mejorar el procedimiento.

- ✓ **Documentado y divulgado:** El control se encuentra documentado y se ha divulgado a los responsables.
- ✓ **Documentado:** Se encuentra definido y documentado en los procedimientos y o Manuales del sistema SAGRILAFT.
- ✓ **No documentado:** El control no se encuentra documentado en manuales y políticas.

d. Frecuencia de los controles: El control debe tener una periodicidad específica de su realización, se puede establecer un control diario, mensual, trimestral, anual, etc. Y su ejecución debe ser consistente y oportuna para la mitigación del riesgo. Una vez definido el responsable del Control, debe identificarse si la periodicidad de su ejecución es adecuada o inadecuada.

- ✓ **Adecuada:** Se refiere a que la frecuencia con la que se realizan los controles es suficiente

y apropiada para detectar y mitigar los riesgos. Los controles se llevan a cabo con la frecuencia necesaria para mantener la efectividad y la actualización del sistema de prevención.

- ✓ **Inadecuada:** Indica que la frecuencia de los controles no es suficiente para identificar de manera oportuna los riesgos. Los controles se realizan con una frecuencia insuficiente, lo que puede resultar en la falta de detección temprana de actividades sospechosas o vulnerabilidades en el sistema.

e. Responsable de los controles: Persona asignada de ejecutar el control, debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso y sus responsabilidades deben ser adecuadamente segregadas o redistribuidas entre diferentes individuos para reducir así el riesgo de error o de actuaciones irregulares o fraudulentas. Si el responsable quisiera hacer algo indebido, por sí solo, no lo podría realizar. Si la respuesta es que se cumple con esto, quiere decir que el control está bien diseñado, si la respuesta es que no cumple tenemos que identificar la situación y mejorar el diseño del control con relación a la persona responsable de la ejecución del control.

- ✓ **Idóneo:** Hace referencia a la persona que posee las habilidades y conocimientos necesarios para desempeñar eficazmente las funciones asignadas en el control y llevar a cabo las actividades acordes a este.
- ✓ **No Idóneo:** Hace referencia a una persona que carece de las habilidades, conocimientos o experiencia necesarios para cumplir adecuadamente con las responsabilidades asignadas al control. Este individuo puede no estar debidamente capacitado o no estar acorde con el proceso que refleja el control.

f. Evidencia del control: Se debe dejar evidencia de la ejecución del control. Esta evidencia ayuda a que se puedan verificar la misma información por parte de un tercero y llegue a la misma conclusión de quien ejecutó el control, y se pueda evaluar que el control realmente fue ejecutado de acuerdo con los parámetros establecidos y descritos anteriormente.

- ✓ **Evidenciado:** Control que cuenta con un soporte documental adecuado que respalda su funcionamiento. Este soporte documental puede incluir registros, procedimientos escritos, evidencia de seguimiento, informes de auditoría u otra documentación que demuestre claramente que el control ha sido aplicado según lo previsto.
- ✓ **No evidenciado:** Control para el cual no existe un soporte documental adecuado que respalde su funcionamiento.

- **Calificación de los controles**

Concepto	Criterio	Puntuación
Tipo de Control	Preventivo	15
	Detectivo	10
	Correctivo	5
Implementación	Automatico	15
	Manual	10
Soporte Documental	Documentado y Divulgado	20
	Documentado	15
	No documentado	0
Frecuencia / Periodicidad	Adecuada	15
	No adecuada	5
Responsable(s)	Idoneo	15
	No idoneo	5
Evidencia	Evidenciado	20
	No evidenciado	0

Valoración de los controles: La valoración final, resultante del análisis de la efectividad y el estado de implementación de los controles en la empresa, será la siguiente:

- ✓ **Fuerte**: Los controles son adecuados y operan correctamente
- ✓ **Moderado**: Existen debilidades con respecto a su diseño y/o implementación y se requieren modificaciones – oportunidades de mejoramiento.
- ✓ **Débil**: Los Controles no son de nivel aceptable.

	MEDICION DEL CONTROL			
Control	FUERTE	Los controes son adecuados y operan correctamente	76	100
	INTERMEDIO	Existen debilidades con respecto a su diseño y/o implementación y se requieren modificaciones – oportunidades de mejoramiento.	51	75
	DEBIL	Los Controles no son de nivel aceptable.	0	50

Como resultado de la aplicación de los controles sobre los riesgos, se obtiene una nueva valoración de la severidad del riesgo y de esta forma el Perfil de Riesgo inherente se convierte en riesgo Residual.

- **Comunicación y consulta**

La comunicación interna y externa de la empresa debe ser eficaz; es importante asegurar que los responsables del procedimiento de gestión del riesgo y grupos de interés entiendan la base sobre la cual se toman decisiones y porque se requieren acciones particulares.
Los registros y reportes de las actividades referentes al Sistema SAGRILAFT pretende:

- ✓ Comunicar las actividades de la gestión de riesgos y los resultados obtenidos en la empresa.
- ✓ Ofrecer información para la toma de decisiones.
- ✓ Mejorar las actividades de la gestión de riesgos.

Para ello, cabe mencionar que los controles establecidos se deben divulgar a los líderes de proceso y responsables de la aplicación por medio de comunicación directa bien sea virtual y/o presencial; En la pestaña "Divulgación de Controles" se relaciona la siguiente información:

a. Riesgo identificado
b. Factor de riesgo evidenciado
c. Controles definidos
d. Registro y/o soporte de la aplicación de los controles establecidos
e. Fecha de divulgación y/o transmisión de la información a los responsables de la ejecución de los mismos.
f. Responsable asignado para la ejecución del control
g. Cargo del responsable asignado
h. Firma del responsable en aceptación de conocimiento del control.

Una vez diligenciados todos los campos se debe entregar el formato para su correspondiente firma a cada responsable, a fin de que cada persona conozca y entienda su actividad dentro de los procesos.

- **Monitoreo del control**

Esta etapa tiene como principal objetivo hacer seguimiento general al Sistema, al igual que desarrollar un Programa de seguimiento efectivo que facilite la rápida detección y corrección de las deficiencias encontradas y asegurar que los controles sean comprensivos de todos los riesgos y que los mismos estén funcionando en forma oportuna y efectiva.
La principal herramienta del Monitoreo o Seguimiento es la autoevaluación de riesgos y controles, con el fin de establecer un enfoque que examine y evalúe la efectividad del Sistema SAGRILAFT.
La revisión anual está en responsabilidad del oficial de cumplimiento y los líderes de procesos, se ejecuta a través de alternativas de seguimiento adicionales, como inspecciones documentales, evaluaciones o auditorias, con el fin de asegurar el mantenimiento de los planes y/o necesidad de cambio de éstos, la metodología de seguimiento se realiza a través de auditoría; ésta debe asegurar que el alcance considere la validación de la efectividad de los controles establecidos.

Los ajustes de la matriz ameritan un cambio de versión en el momento que se presenten las

siguientes situaciones :

- ✓ Identificación de nuevos riesgos
- ✓ Lanzamiento de nuevas líneas de negocio,
- ✓ Desarrollo de actividades comerciales en jurisdicciones distintas a las identificadas en la segmentación de factores de riesgo
- ✓ Cambios en la actividad económica de la compañía

Los demás cambios de la matriz SAGRILAFT realizados durante el proceso de revisión anual se deben relacionar en la pestaña ***control de cambios*** con la misma versión y describir el cambio en el campo de observaciones.

6. REFERENCIAS Y ANEXOS

Anexo 5 Matriz de riesgos Sagrilaft

7. REGISTROS DE CALIDAD

CÓDIGO	TITULO	ALMACENAMIENTO	RETENCIÓN	DISPONIBILIDAD
Anexo 5	Matriz de Riesgos Sagrilaft	https://cferretera.sharepoint.com/sites/Calidad/Documentos%20compartidos/Forms/AllItems.aspx?id=%2Fsites%2FCalidad%2FDocumentos%20compartidos%2FCALIDAD/DZZ\SAGRILAFT Y PTEE	Mientras este vigente	Conservar

8. MODIFICACIONES