Superintendencia de Servicios Financieros

Estándares Mínimos de Gestión para Intermediarios de Valores

Enero 2021

BANCO CENTRAL DEL URUGUAY

Estándares Mínimos de Gestión – Intermediarios de Valores [1]

Contenido

INTRODUCCIÓN

Los objetivos de la supervisión de las entidades que integran el sistema financiero son identificar en forma temprana las debilidades de las mismas promoviendo su efectiva resolución e identificar los riesgos y tendencias para el conjunto del sistema financiero, a efectos de que se pueda actuar oportunamente para minimizar tales riesgos.

A esos efectos, la Superintendencia de Servicios Financieros (SSF) ha diseñado una metodología que comprende diferentes componentes, entre los que se encuentran, los procedimientos de supervisión, las estrategias, los Estándares Mínimos de Gestión (EMG), etc. [2].Estos últimos, constituyen las expectativas del Supervisor sobre los elementos que deben estar presentes en la gestión de las entidades financieras, según el mercado que se trate.

Asimismo, en lo que respecta a la actuación de los corredores de bolsa y agentes de valores, se ha definido que el foco principal de atención es la protección del usuario de servicios financieros y la prevención de que las entidades sean utilizadas para el lavado de activos y financiamiento del terrorismo (LA/FT).

La supervisión por protección a los usuarios de servicios financieros busca garantizar que las entidades cumplan con las normas regulatorias y mejores prácticas en la materia, mientras que la prevención de ser utilizadas para el LA/FT busca promover que las mismas sean capaces de evitar ser utilizadas 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 cuando se pretenda el ocultamiento de activos provenientes de dichas actividades.

[1] Los términos del presente documento aplican a corredores de bolsa y agentes de valores. En el caso de empresas de intermediación financiera, en cuanto a su actividad como intermediario de valores, son de aplicación los estándares de Protección al inversor (P), además de los estándares mínimos de gestión específicos para dicho tipo de empresas.

[2] Para mayor información respecto del marco de actuación de la SSF ver "*Marco Operativo de la Superintendencia de Servicios Financieros*" (https://www.bcu.gub.uy/Servicios-Financieros-SSF/Paginas/Marco-Operativo.aspx).

En este marco, la SSF analizará:

- El Gobierno Corporativo, es decir, el sistema a través del cual las instituciones son dirigidas, monitoreadas y controladas.

- La forma en que las instituciones aseguran la protección del interés de los inversores.

- La capacidad de la institución de identificar, controlar, medir y monitorear los siguientes riesgos:

    - Riesgo Operacional y Cumplimiento
    - Riesgo de LA/FT
    - Riesgo de Reputación
    - Riesgo de Crédito, Contraparte y Custodia
    - Riesgo de Mercado

LOS ESTÁNDARES MÍNIMOS

Las instituciones adoptan diferentes esquemas y estructuras para desarrollar sus actividades y gestionar los riesgos que asumen. La SSF lleva adelante sus procedimientos de supervisión y evaluación teniendo en cuenta la naturaleza, tamaño y complejidad de las operaciones y su perfil de riesgos.. A los efectos de determinar el perfil de riesgos de la institución, se toman en cuenta factores tales como: la participación de mercado, la rotación de stock promedio de cartera administrada de clientes y la titularidad de las cuentas donde se radican las custodias.

Como se mencionó, los estándares constituyen prácticas de gestión que se espera encontrar en las entidades supervisadas y desde el punto de vista del Supervisor se entiende que el no cumplimiento de un estándar constituye una debilidad que debe ser tratada con atención prioritaria por la entidad.

La SSF formula su juicio global sobre la entidad en base a una combinación de procedimientos a distancia e in-situ, buscando evidencias de que los procesos y procedimientos, sean acordes a las características de cada entidad y a los riesgos que asumen. No obstante ello, la SSF no certifica la adherencia estricta a los puntos específicos contenidos en estos estándares.

ESTÁNDARES DE GOBIERNO CORPORATIVO (C)

El Gobierno Corporativo es el sistema a través del cual las instituciones son dirigidas, monitoreadas y controladas e incluye a la Dirección, la Alta Gerencia y a los distintos mecanismos de control.

Un Gobierno Corporativo eficaz se basa en los siguientes componentes fundamentales:

- Cultura corporativa apropiada con normas establecidas para un comportamiento responsable y ético.

- Gestión de riesgos acorde a las actividades que se realizan.

- Responsabilidades bien definidas y comunicadas a toda la organización para la gestión de riesgos y controles.

Atendiendo a las características actuales de la mayoría de los corredores de bolsa y agentes de valores existentes en nuestro mercado, con reducidas estructuras, los presentes estándares de Gobierno Corporativo no plantean una diferenciación de roles para la Dirección y la Alta Gerencia. No obstante, podrán realizarse mayores requerimientos a aquellas entidades que corresponda en función de su perfil de riesgos, tamaño y complejidad de sus operaciones.

Los estándares mínimos que deben cumplirse son los que se detallan a continuación:

1. Los miembros del Directorio[3] y la Alta Gerencia deben poseer los conocimientos y habilidades para dirigir, gestionar y supervisar los negocios bajo su responsabilidad.

Para ello, deben:

1.1 Tener un claro entendimiento de su rol dentro del Gobierno Corporativo y cumplir con el deber de lealtad y diligencia.

1.2 Tener acceso regular a capacitación para mantener y mejorar sus competencias en las áreas de su responsabilidad.

2. El Directorio y la Alta Gerencia deberán cumplir con determinados cometidos y responsabilidades.

Entre ellos se encuentran:

2.1 Aprobar, implementar y monitorear periódicamente el cumplimiento del Plan de Negocios que contemple los objetivos definidos, dentro de los cuales se considerarán las relaciones con partes vinculadas.

2.2 Asegurar la existencia de un sistema de información íntegro, confiable y oportuno que brinde información sobre la implementación de los planes, los controles internos y los resultados de la gestión a efectos de permitir la toma de decisiones efectivas.

2.3 Entender los riesgos que enfrenta la entidad así como definir el nivel de exposición a cada tipo de riesgo y promover una cultura de riesgos en la organización.

2.4 Mantener documentados los temas tratados, decisiones y análisis de información proveniente de los controles realizados, las evaluaciones y recomendaciones de la Auditoría Externa y del Supervisor (por ejemplo, actas de reuniones o resúmenes de temas tratados, recomendaciones emitidas, decisiones adoptadas y reportes utilizados para la toma de decisiones). Asimismo, periódicamente debe efectuar el seguimiento de las debilidades de control detectadas tanto de fuentes internas como externas.

3. La institución debe promover una cultura corporativa que exija y provea los incentivos adecuados para una conducta ética y que evite o administre los posibles conflictos de interés.

[3] Si bien se utiliza el término "Directorio", el concepto abarca a administradores cuando la institución no haya sido constituida como sociedad anónima. Debe entenderse como el órgano que ejerce la administración efectiva de la entidad.

Para ello, debe:

3.1 Establecer y comunicar los estándares éticos a través de un Código de Ética.

3.2 Definir una política sobre conflictos de interés otorgando absoluta prioridad al interés de los clientes y asegurar que existen políticas y procedimientos claramente definidos para el tratamiento de operaciones con partes relacionadas, de forma que todas las transacciones se realicen en condiciones de mercado evitando desventajas en perjuicio de los clientes.

3.3 Definir procedimientos de vinculación, formación y evaluación continua del personal para asegurar que la prestación de servicios se efectúa en forma honesta, imparcial y profesional, en el mejor interés de los clientes.

3.4 Asegurar que las políticas de remuneración y compensación son transparentes y consistentes con el plan de negocios de la institución y que existen mecanismos para verificar su cumplimiento. Se debe verificar que las políticas retributivas eviten que se asuman riesgos de forma imprudente e inadecuada respecto del perfil definido para los clientes.

4. La institución debe asumir un compromiso en materia de protección del interés de los inversores.

Para ello, debe:

4.1 Aprobar y asegurar que se adopten los principios y valores del Código de Buena Prácticas en el que se estipulen los principios y valores que rigen las relaciones que se establezcan con los clientes de la institución.

4.2 Comunicar a toda la organización dichos principios y en caso de incumplimiento de los mismos, verificar que se tomen las medidas correctivas adecuadas.

4.3 Diseñar los mecanismos que permitan velar por los intereses de sus clientes y tratarlos justamente, actuando con integridad, profesionalismo, cuidado y diligencia.

4.4 Establecer controles para asegurar la integridad, independencia y eficacia en el tratamiento de denuncias de irregularidades de la institución.

4.5 Contar con mecanismos para asegurar que los asesores cumplen con los requisitos de formación.

5. Debe promoverse la existencia de un ambiente de control confiable y adecuado.

Para ello, la institución debe:

5.1 Aprobar la estructura organizativa acorde al tamaño, complejidad, naturaleza y volumen de las operaciones y a su perfil de riesgos, asegurando una clara separación y equilibrio de las funciones comerciales y de cumplimiento, y, en general, una adecuada segregación de funciones.

5.2 Asegurar que existen mecanismos de control interno confiables, acorde a los riesgos y a la naturaleza y complejidad de las operaciones.

5.3 Realizar un seguimiento de los riesgos derivados de las actividades tercerizadas, evaluando su impacto en el ambiente de control.

5.4 Tomar las medidas necesarias para asegurar la objetividad e independencia de la Auditoría Externa dentro de la organización.

5.5 Corregir los problemas detectados en los controles internos por el Auditor Externo y por los Supervisores.

5.6 Facilitar el relacionamiento con el Supervisor y proveer los elementos necesarios para que éste pueda cumplir su rol.

6. La entidad debe gestionar adecuadamente los riesgos involucrando a todo el personal.

Para ello, debe:

6.1 Implementar los procedimientos que permitan identificar, medir, monitorear y controlar todos los riesgos que puedan afectar el cumplimiento de los objetivos de la institución.

6.2 Asegurar que cuenta con los recursos suficientes para un manejo adecuado de los riesgos y que el personal involucrado en los procesos tiene la capacidad técnica para comprender y analizar los riesgos asumidos.

6.3 Implementar un proceso para la aprobación y puesta en producción de nuevos productos que asegure un adecuado control y gestión de riesgos antes de su introducción o implementación.

7 La institución debe definir e implementar un sistema de información íntegro y oportuno.

El sistema de información debe:

7.1 Cubrir todas las actividades significativas de la institución y estar integrado por información financiera, operativa, de riesgos y de cumplimiento adecuada y completa.

7.2 Cumplir con las características de:

- Oportunidad – El sistema debe proveer información actualizada en forma oportuna a los usuarios apropiados, de forma de facilitar la toma de decisiones.
- Integridad – Los tomadores de decisiones deben contar con información completa y pertinente.
- Relevancia - Está directamente relacionado con las necesidades de la entidad.

7.3 La información suministrada al Supervisor debe ser confiable y oportuna y debe existir un responsable en la organización por su elaboración y presentación.

ESTÁNDARES DE PROTECCIÓN AL INVERSOR (P)

El intermediario debe promover la protección del interés de los inversores cumpliendo con las normas regulatorias y mejores prácticas en la materia en cada una de las etapas del proceso. Todos los integrantes de la organización deben demostrar compromiso con el cliente.

Dicha protección se basa en tres pilares: **trato justo y ético, transparencia, y efectiva resolución de reclamos**.

8. La institución debe contar con procedimientos que aseguren que toda relación comercial con el cliente se encuentra precedida por un contrato escrito que cumpla con los requisitos legales y reglamentarios establecidos.

8.1 El intermediario debe asegurarse que dicho contrato contemple, asimismo, los siguientes aspectos:

- Mención de los costos asociados a la prestación del servicio o lugar donde se encuentran disponibles para el cliente.
- Nombre del asesor, en caso que expresamente el cliente tenga designado uno.
- Definición del medio de envío del estado de cuenta y su periodicidad, la que debe ser al menos anual.

8.2 Asegurar que se notifica al cliente de la existencia del Código de Buenas Prácticas y del procedimiento de atención de reclamos.

9. La institución debe asegurarse que todos los clientes cuenten con un perfil y una estrategia de inversión, alineada al mismo.

9.1 La institución debe contar con procedimientos para definir el perfil de inversión de los clientes.

9.2 La definición del perfil debe quedar adecuadamente documentada, contemplando todos los aspectos dispuestos por la normativa, debiendo la entidad obtener todos los datos que estime conveniente para valorar si, en su opinión, el cliente tiene los conocimientos y experiencia necesarios para comprender la naturaleza y riesgos del servicio o producto ofrecido.

En el caso de personas jurídicas, a efectos de la definición del perfil, se debe considerar al representante de la empresa, para evaluar su experiencia previa y conocimientos financieros.

9.3 La entidad debe recabar toda la información necesaria y efectuar el análisis de los datos para poder formarse una opinión, aún cuando se utilicen cuestionarios, incluyendo la autoevaluación del cliente.

9.4 La institución debe determinar el mecanismo por el cual dicho perfil será notificado al cliente, recabando su conformidad por algún medio. Asimismo, debe verificar que se cumpla con una periodicidad mínima de revisión.

9.5 La institución debe contar con procedimientos que permitan asegurar que los productos ofrecidos son

acordes a los perfiles definidos, así como documentar adecuadamente la conformidad del cliente respecto a los apartamientos del perfil.

9.6 La institución debe contar con una estrategia de inversión definida para cada cliente que sea coherente con su perfil de inversión, estableciendo portafolios y límites a la realización de ciertas inversiones.

9.7 La estrategia debe ser notificada al cliente, debiéndose obtener la conformidad por los medios acordados. La institución debe contar con procedimientos que permitan asegurarse que los servicios prestados se corresponden con las estrategias de inversión establecidas. En caso de existir apartamientos de la estrategia debe recabarse la conformidad del cliente.

9.8 En caso de clientes que opten por gestión discrecional de portafolios, la estrategia debe comprender la definición del proceso de inversión, el que debe estar documentado y que debe ser conocido por el cliente.

10. La institución debe adoptar políticas y procedimientos de ejecución de órdenes a efectos de obtener el mejor resultado posible para el cliente.

Para ello, debe:

10.1 Contar con un manual de procedimientos y políticas de la Mesa de Operaciones, que sea documentado y difundido y conocido por los operadores de la mesa. Deberá contemplar, como mínimo, los siguientes aspectos: detalle de funciones y responsabilidades de los integrantes de la mesa; productos, monedas, contrapartes y operadores autorizados; definición de límites y atribuciones fijadas a los funcionarios; personas autorizadas a aprobar desvíos; y criterios para la aprobación de nuevos productos.

10.2 Procurar la mejor ejecución de las operaciones priorizando el interés de los clientes, debiendo poder demostrar la elección de la mejor cotización en beneficio de los mismos.

10.3 Realizar una adecuada priorización de las órdenes en beneficio de los clientes.

11. La institución debe proporcionar al cliente el estado de cuenta, con la periodicidad definida al inicio de la relación comercial, o cuando este lo solicite.

11.1 La institución debe contar con mecanismos que permitan verificar que el cliente recibe al menos anualmente el estado de cuenta.

11.2 El estado de cuenta debe proporcionar un detalle de todas las operaciones realizadas en el período, especificando todos los costos asociados, incluyendo los diferenciales de precios y las posiciones tanto en efectivo como en valores.

11.3 El estado de cuenta debe incluir información sobre la rentabilidad anual obtenida en el período determinado de envío.

12. La institución debe proporcionar al cliente información clara, suficiente, veraz y oportuna acerca de las características y riesgos de los productos y servicios solicitados por los clientes u ofrecidos a éstos, de modo que les permita tomar decisiones informadas.

Para ello, debe:

12.1 Asegurar que se realizan en tiempo y forma, las advertencias que correspondan a los clientes, en su propio interés, en especial en aquellas circunstancias en que el cliente insiste en asumir riesgos que exceden su perfil inversor.

12.2 Informar al cliente si su inversión se realiza en valores emitidos por una empresa vinculada y/o en valores en los que ha oficiado de estructurador de la emisión.

12.3 Detallar a los clientes las instituciones en que se custodian sus activos, especificando si se trata de una sociedad vinculada al intermediario. Esta información podrá estar incluida en los estados de cuenta que se proporcionan a los clientes, en la página web del intermediario de valores o en otros medios que se consideren adecuados.

13. La institución debe contar con un servicio de atención a los clientes que permita canalizar las consultas y los reclamos recibidos, velando por los derechos establecidos legalmente y en la normativa del Banco Central del Uruguay.

Para ello, debe:

13.1 Asegurar que existe un responsable del servicio de atención al cliente, el que debe ser llevado adelante con independencia y objetividad, por personas que cuentan con la experiencia y conocimientos adecuados para ejercer estas funciones.

13.2 Realizar una adecuada difusión del servicio de atención al cliente en las oficinas de la institución, en la documentación de las operaciones y en el sitio web de la entidad.

ESTÁNDARES DE GESTIÓN DE RIESGOS (R)

Una competencia clave de las instituciones es su capacidad de gestionar los riesgos que asumen, para sí y para sus clientes, en forma prudente y rentable.

Deben por lo tanto implementar un Sistema de Gestión de Riesgos, definido como el conjunto de políticas, procedimientos y mecanismos de control implementados por la Institución para propiciar una apropiada identificación, medición, control y monitoreo de los riesgos que asume.

RIESGO OPERACIONAL Y CUMPLIMIENTO

El riesgo operacional se define como la posibilidad de que el patrimonio de la entidad se vea afectado por pérdidas resultantes de procesos, personas o sistemas internos inadecuados o defectuosos, o por eventos externos. Incluye además el riesgo de cumplimiento, es decir, la posibilidad de que una entidad se vea afectada por violaciones a las leyes, regulaciones, estándares y prácticas de la industria o estándares éticos.

El riesgo operacional acompaña el desarrollo y la evolución de los servicios y los procesos transaccionales, está vinculado al desarrollo de los sistemas (en particular sistemas de computación) y guarda relación con la calidad del personal y el ambiente de control interno. Es un riesgo diferente a otros, como el riesgo de crédito o de mercado, ya que no sólo se asume riesgo operacional con el objetivo de obtener un retorno,

sino que surge de la actividad normal de la entidad.

14. La institución debe contar con procedimientos de identificación, medición y evaluación de las fuentes de riesgo operacional y cumplimiento y definir los mecanismos para mitigar dichos riesgos.

Para ello, debe:

14.1 Realizar un mapeo de los distintos procesos y revisarlo periódicamente.

14.2 Asegurar el cumplimiento de las leyes, normativas y estándares aplicables.

14.3 Asegurar que se cuenta con mecanismos de control de usuarios de plataformas, a efectos de evitar la utilización de usuarios genéricos o personas no pertenecientes a la institución.

15. La institución deberá establecer mecanismos de control que mitiguen la probabilidad de ocurrencia de eventos de fraude interno.

Para ello, debe:

15.1 Asegurar la independencia de las actividades de la mesa de operaciones y de los ejecutivos de cuenta, contando con una estructura de back office que permita una adecuada segregación de funciones.

15.2 Contar con procedimientos para proteger los fondos e instrumentos financieros de los clientes, asegurando la fiabilidad de los registros contables y custodias adecuadas.

15.3 Contar con evidencia de la realización de conciliaciones, identificando y justificando adecuadamente las partidas conciliatorias.

15.4 Identificar y prevenir prácticas indebidas, como por ejemplo, la rotación excesiva o compras y ventas que no tengan razonabilidad financiera, montos elevados de comisión por parte de los oficiales de cuenta o concentración de clientes en un activo o tipo de producto.

15.5 Contar con controles para asegurar la fiabilidad de la información contenida en los estados de cuenta, evitando su manipulación y asegurar que las comisiones cobradas a los clientes coinciden con las pactadas.

15.6 Contar con un procedimiento de monitoreo de cuentas de los empleados.

16. La institución debe contar con un plan de contingencia y de continuidad de los negocios que permita operar ante la ocurrencia de eventos externos severos.

Para ello, debe:

16.1 Contar con un Análisis de Impacto al Negocio en el cual se identifiquen las actividades críticas de la

institución.

16.2 Establecer planes que, ante distintos escenarios de desastre, aseguren la continuidad del negocio. Los mismos deben diseñarse para permitir la recuperación de las operaciones y para no interrumpir el servicio prestado por los centros de procesamiento de datos, redes, proveedores externos y en las áreas de trabajo.

16.3 Abarcar en sus planes la continuidad de los servicios tercerizados.

16.4 Establecer planes de respaldo de información que aseguren su recuperabilidad.

16.5 Revisar periódicamente la aplicabilidad de estos planes. Para esto, se debe realizar una prueba (paralela o completa) del plan por lo menos anualmente, debidamente documentada y analizada al culminarse.

17. La institución debe contar con una adecuada gestión de la seguridad de la información.

Para ello, debe:

17.1 Aprobar políticas de seguridad de la información adecuadas y asegurar que se implementen los procedimientos que la hacen aplicable.

17.2 Deberá implementar procedimientos de resguardo de datos y software, de tal forma que sea posible reconstruir las informaciones emitidas, los registros contables y cada uno de los movimientos que dan origen a los mismos.

17.3 Identificar y monitorear los riesgos asociados a la gestión de sus activos de información, de manera que se incluya un análisis sobre las amenazas y vulnerabilidades presentes.

17.4 Generar concientización y asegurar una adecuada capacitación al personal que permita involucrar a todos en la gestión de los riesgos asociados a los activos de información.

17.5 Asegurar el cumplimiento de las políticas de seguridad de la información en el caso de actividades tercerizadas, y velar por la seguridad de los datos procesados externamente.

18. La institución debe gestionar la Tecnología de Información (TI) para proporcionar los servicios en un ambiente seguro, garantizando el soporte y la capacitación a los usuarios.

Para ello, debe cumplir con los siguientes requerimientos:

18.1 Proporcionar un nivel de servicio que satisfaga las necesidades del negocio.

18.2 Establecer controles adecuados de los datos a nivel de la operación, entradas, proceso y salidas.

18.3 Asegurar la calidad de los procesos y/o los programas que monitorean la capacidad y el desempeño del

servicio de TI.

18.4 Asegurar la calidad de la seguridad física y lógica incluyendo la privacidad de la información.

18.5 Contar con una arquitectura adecuada y asegurar las conexiones con redes de comunicación.

En el caso de servicios prestados por terceros, debe asegurar que:

18.6 Se han documentado adecuadamente a través de contratos, las condiciones y niveles mínimos de servicio a ser obtenidos del proveedor.

18.7 Se han establecido controles adecuados sobre los proveedores externos y que la institución es capaz de monitorear los mismos.

18.8 El servicio a los requerimientos de los usuarios es adecuado.

18.9 El proveedor es capaz de proveer y mantener el desempeño de los niveles de servicios adecuado a las necesidades de los usuarios.

18.10 Se manejan adecuadamente los riesgos derivados del manejo de información confidencial o sensible por parte del proveedor.

RIESGO DE LAVADO DE ACTIVOS Y FINANCIAMIENTO DEL TERRORISMO (LA/FT)

El riesgo de Lavado de Activos y Financiamiento del Terrorismo refiere a la posibilidad de pérdida o daño que puede sufrir una entidad al 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 cuando se pretenda el ocultamiento de activos provenientes de dichas actividades.

Las instituciones deben instrumentar un sistema que abarque políticas, prácticas y procedimientos que le permitan identificar, evaluar, monitorear y mitigar el riesgo de ser utilizada como instrumento para el lavado o la canalización de fondos destinados al financiamiento del terrorismo. Para ello, las instituciones deben contar con políticas y procedimientos bien documentados y correctamente comunicados a todo el personal pertinente y estar integrados en la gestión integral de riesgos de la institución y deben ser aplicados de forma continuada y a todo el grupo financiero.

19. El Oficial de Cumplimiento es el responsable de la implantación, seguimiento y control del adecuado funcionamiento del sistema de prevención del riesgo de LA/FT.

Para ello, el Oficial de Cumplimiento debe:

19.1 Implementar las estrategias y políticas aprobadas por el Directorio y desarrollar procedimientos bien documentados que permitan identificar, medir y controlar el riesgo de LA/FT, los cuales deben aplicarse en toda la institución y en los servicios tercerizados.

19.2 Proponer la actualización de políticas y procedimientos en relación al riesgo de LA/FT y el uso de herramientas adecuadas a la complejidad y el nivel de actividad desarrollado.

19.3 Actuar con objetividad e independencia en la planificación y ejecución de sus actividades.

19.4 Asegurar que el personal esté en conocimiento y aplique los procedimientos internos, de forma que todas aquellas transacciones que puedan ser consideradas como sospechosas o inusuales lleguen a su conocimiento para dar inicio al mecanismo de análisis y reporte de operaciones a la UIAF.

19.5 Mantenerse actualizado, diseñar programas de capacitación del personal y detectar necesidades de capacitación en materia de prevención de LA/FT.

19.6 Participar en el desarrollo y actualización de nuevos productos y procesos a fin de asegurar controles adecuados en relación al riesgo LA/FT.

20. La institución debe desarrollar procedimientos de debida diligencia a ser aplicados a sus clientes y entidades o personas con las que se vincula y sus transacciones, que sean diferenciales en función de su nivel de riesgo y que cumplan con los requisitos dispuestos en la normativa vigente.

20.1 Aplicar procedimientos de debida diligencia a sus clientes en función de su categoría de riesgo, aplicando medidas intensificadas para los clientes de mayor riesgo.

20.2 En particular, en relación a las contrapartes con las que opere, la institución deberá:

(a) Recabar suficiente información sobre ellas para tener una comprensión plena de la naturaleza de su actividad, reputación de la institución, actividades principales y donde están localizadas, así como de la forma en que están reguladas y supervisados;

(b) Determinar el propósito de la transacción;

(c) Evaluar las políticas, procedimientos y controles de la institución a efectos de prevenirse de ser utilizada para el lavado de activos y financiamiento del terrorismo; y

(d) Obtener la aprobación de los principales niveles jerárquicos de la institución.

21. La institución debe desarrollar un sistema de monitoreo de las relaciones comerciales y de las transacciones acorde con su tamaño, complejidad y riesgo de sus actividades.

Para ello, debe:

21.1 Implementar procedimientos de monitoreo acorde con su tamaño, riesgos y complejidad de sus actividades que permitan detectar desvíos respecto de lo usual para el tipo de cliente, actividad o según el tipo de transacción.

El sistema de monitoreo debe:

- Ser continuo, oportuno y abarcar todas las actividades, productos, clientes y canales utilizados para realizar las transacciones, teniendo como base su evaluación de riesgo.

- Contar con un soporte informático acorde con la complejidad de sus actividades.

- Tener como base el perfil transaccional y la categoría de riesgo del cliente y los factores de riesgo propios de su actividad y las mejores prácticas internacionales respecto de éstos.

- Utilizar parámetros adecuados para reflejar situaciones de riesgo, operaciones inusuales o patrones de actividad sospechosos.

- Gestionar las alertas en forma oportuna, tomando como base la información disponible y requiriendo la información adicional que corresponda requerir.

- Comprender un control con listas de personas identificadas como terroristas confeccionadas en cumplimiento de la Resoluciones del Consejo de Seguridad de la Organización de Naciones Unidas o por resolución Judicial Firme, así como con listas de personas que puedan estar vinculadas con actividades de lavado de activos o financiamiento del terrorismo.

22. La institución debe contar con procedimientos para detectar las operaciones inusuales y/o sospechosas, a efectos de notificar al supervisor y atender en forma oportuna sus solicitudes.

Para ello, debe:

22.1 Definir claramente el proceso para identificar, investigar y notificar transacciones sospechosas al supervisor y comunicarse a todo el personal. Estas definiciones deben incluir los canales internos de reporte, los responsables por el análisis y las guías a considerar.

22.2 Asegurarse que los responsables por la decisión de reportar o no a la Unidad de Análisis e Información Financiera (UIAF) están claramente designados, como así también la forma en que se documenta la decisión.

22.3 Asegurarse que el procedimiento implementado garantiza la confidencialidad del reporte y de la información en él incluida.

22.4 Definir procedimientos o instructivos que permitan asegurar que los reportes de operaciones sospechosas se elaboran y notifican oportunamente y contienen la información mínima relevante y de acuerdo a los estándares.

22.5 Definir procedimientos para implementar la política definida por el Directorio sobre cómo proceder con los clientes respecto de los cuales se ha reportado una operación sospechosa a la UIAF. Para los casos en que se mantiene el vínculo con el cliente, los procedimientos deben contemplar el monitoreo intensificado para las transacciones cursadas por estos clientes.

22.6 Definir procedimientos que aseguren atender en forma oportuna y con información precisa las consultas o pedidos de información realizadas por la UIAF. Estos procedimientos deber establecer claramente los responsables y los procesos de búsqueda y consulta interna ante cada pedido y la forma en que se garantizará la confidencialidad de estas solicitudes.

RIESGO DE REPUTACION

El riesgo de reputación se define como el riesgo presente y futuro de que las ganancias o el patrimonio de la entidad se vean afectados por una opinión pública negativa. Afecta la capacidad de la institución de establecer nuevas relaciones o servicios, o continuar sirviendo a las relaciones ya existentes. Este riesgo puede exponer a la institución a juicios, pérdidas financieras o a una disminución en la base de clientes. La exposición al riesgo de reputación incluye la responsabilidad de tener amplia precaución al tratar con los clientes y la comunidad. El riesgo de reputación no es fácilmente cuantificable pero aparece en todas las relaciones con los clientes, en particular aquellas que aparejan asesoramiento y manejo de información confidencial de los mismos.

23. La institución debe conocer y gestionar cualquier aspecto que represente un riesgo de reputación significativo.

Para ello, debe:

23.1 Asegurar que se reporte al Directorio/Alta Gerencia en forma periódica aquellos eventos que afecten el riesgo de reputación, en particular en lo que refiere a los resultados de la gestión del servicio de atención al cliente.

RIESGO DE CRÉDITO, CONTRAPARTE Y CUSTODIA

El riesgo de crédito se define como la posibilidad de que la entidad vea afectado su patrimonio o se generen perjuicios para los clientes debido a la incapacidad de los emisores, contrapartes o custodios de cumplir con los términos originalmente pactados.

El riesgo de custodia es el riesgo de que una pérdida afecte a los valores o fondos mantenidos en custodia debido a la insolvencia, la negligencia, el fraude, la administración deficiente o el mantenimiento inadecuado de los registros de un custodio o un subcustodio.

24. La institución debe implementar un sistema para administrar los riesgos de crédito, contraparte y custodia, el cual debe ser consistente con el tamaño y el volumen de transacciones que realiza a Institución

Para ello, debe:

24.1 Contar con un sistema de identificación de las posibles fuentes de dichos riesgos que incorpore las exposiciones con las contrapartes y custodios y que capture toda fuente material de riesgo.

24.2 Desarrollar un sistema de información que permita:

- Suministrar información sobre todas las exposiciones con contrapartes y custodios
- Comparar la información sobre contrapartes y custodios con los límites de riesgo establecidos e informar sobre excepciones a los mismos de manera oportuna y adecuada.

24.3 Contar con adecuadas políticas de selección de contrapartes y custodios, que contemplen al menos los siguientes aspectos: reputación, costos, operativa, calificación y experiencia.

RIESGOS DE MERCADO Y LIQUIDEZ

Los riesgos de mercado son aquellos por los cuales el valor de las posiciones propias puede verse adversamente afectado, debido a movimientos en las variables de mercado - básicamente las tasas de interés y los tipos de cambio entre divisas- con el consiguiente impacto en las utilidades y el patrimonio del intermediario.

Por su parte, el riesgo de liquidez es la posibilidad de que la entidad no cuente con suficientes activos líquidos para hacer frente a las obligaciones asumidas.

25. La institución debe realizar una gestión adecuada de los riesgos de mercado y liquidez para su cartera propia.

Para ello, debe:

25.1 Contar con un sistema de medición de riesgo de mercado que capture toda fuente material de riesgo de tasa de interés, tipo de cambio, reajuste y liquidez y evaluar el impacto de los mismos sobre la institución. Los supuestos subyacentes en dichos sistemas deben ser comprendidos claramente por el Directorio y la Alta Gerencia.

25.2 Tener un sistema adecuado para el monitoreo y control de los riesgos de mercado y liquidez.

25.3 Establecer y realizar controles para asegurar que las excepciones en las políticas, los procedimientos y límites son identificadas y reportadas oportunamente al nivel jerárquico apropiado.
