BCU
SUPERINTENDENCIA
DE SERVICIOS FINANCIEROS

ESTÁNDARES MÍNIMOS DE GESTIÓN PARA INSTITUCIONES DE INTERMEDIACIÓN FINANCIERA

Vigencia: 1 de Julio de 2017

BANCO CENTRAL DEL URUGUAY

Estándares Mínimos de Gestión IIF

Tabla de contenido

INTRODUCCIÓN

Se hace saber a las Instituciones de intermediación financiera que, en el marco de las facultades y cometidos asignados por las normas legales correspondientes, la Superintendencia de Servicios Financieros ha definido que el proceso de supervisión debe estar orientado a ser integral, proactivo, enfocado a los riesgos y sobre una base consolidada. Una de las herramientas con que cuenta la supervisión para cumplir con sus cometidos es la Evaluación Integral, trabajo llevado a cabo in-situ en la institución. El propósito de la Evaluación Integral es evaluar la calidad de la gestión de las entidades, y en caso de detectar debilidades, evaluar su impacto sobre la capacidad de la entidad de mantener niveles prudenciales de solvencia a corto, mediano y largo plazo. Asimismo y a efectos de contar con un mecanismo que permita resumir los resultados de la evaluación, se ha definido una metodología de calificación denominada CERT. El objetivo del CERT es sintetizar la evaluación, por componente y en forma general, de tres aspectos:

- si existe alguna debilidad en uno de los componentes que requiera atención prioritaria por parte de la institución
- en qué etapa de resolución se encuentra dicha debilidad
- el impacto potencial de la debilidad encontrada sobre la capacidad de la institución de mantener niveles de solvencia prudenciales en el corto plazo.

METODOLOGÍA DE CALIFICACIÓN CERT

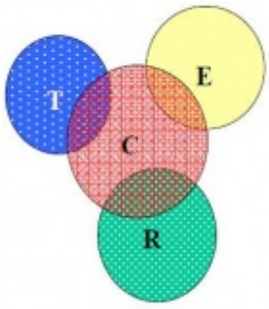
Para aplicar la metodología CERT a una entidad, los Supervisores analizarán los siguientes componentes:

- C –Gobierno Corporativo, es el sistema a través del cual las instituciones son dirigidas, monitoreadas y controladas.
- E – Evaluación económico-financiera – La situación Económico-Financiera se analiza haciendo hincapié en el nivel y calidad del patrimonio de la institución y su capacidad de respaldar los riesgos asumidos y proveer protección a los acreedores.
- R – Riesgos – El Sistema de Gestión de Riesgos de la institución y la capacidad de la institución de identificar, controlar, medir y monitorear los siguientes riesgos en forma integral:
  - Riesgo de Crédito[1]
  - Riesgo de Mercado[2]
  - Riesgo de Liquidez [3]
  - Riesgo Operacional[4]
  - Riesgo de Lavado de Activos y Financiamiento de Terrorismo
  - Riesgo Estratégico
  - Riesgo Reputación
- T – Tecnología – Refiere a la gestión de los Riesgos Tecnológicos y a la confiabilidad y eficacia de los sistemas de información como herramientas de la gestión.

Interrelación entre los distintos componentes del CERT

Desde el punto de vista metodológico, debe visualizarse al Gobierno Corporativo como el núcleo central del análisis, con el cual se interrelacionan los otros componentes del sistema. Gráficamente, podemos verlo de la siguiente manera:

[1] Incluye el riesgo país en la dimensión activa
[2] Incluye riesgo tipo de cambio y tasa de interés
[3] Incluye el riesgo país en la dimensión pasiva,
[4] Incluye el Riesgo de cumplimiento



En aras de una mayor transparencia sobre la aplicación del sistema y con la idea de proveer orientación a las instituciones sobre qué se espera de ellas, se ha elaborado una serie de estándares mínimos de gestión asociados a los componentes de la metodología CERT. 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.

LOS ESTÁNDARES MÍNIMOS

Las instituciones adoptan diferentes esquemas y estructuras para llevar adelante su gestión, tomando en cuenta la naturaleza, tamaño y complejidad de sus operaciones y su perfil de riesgos.

El supervisor lleva adelante sus procedimientos de supervisión y evaluación teniendo en cuenta estos elementos. Los estándares constituyen prácticas de gestión que el supervisor espera encontrar en las entidades supervisadas. El supervisor formula su juicio global sobre la entidad en base a procedimientos a distancia y a una serie de procedimientos in-situ (según la metodología CERT).

Se buscan evidencias de que los procesos y procedimientos, en general, son adecuados dadas las características de cada entidad y que las distintas estructuras de Gobierno Corporativo cumplen con sus roles y responsabilidades en forma adecuada.

Los hallazgos permiten a posteriori definir si existen o no apartamientos a los estándares que se definen seguidamente. El supervisor no certifica la adherencia estricta a los puntos específicos contenidos en estos estándares.

El caso de los Conglomerados Financieros o Grupos Financieros

Las prácticas de gestión deben aplicarse tanto a las entidades individualmente consideradas como al grupo financiero que integran. El hecho de pertenecer a un grupo genera una serie de riesgos (contagio, concentraciones, riesgos derivados de operaciones y exposiciones intra-grupo, múltiple uso del capital, etc.), por lo cual deben considerarse estas características en el marco de una gestión integrada.

En el marco de este documento se estará refiriendo a este tipo de estructuras como “conglomerados financieros” o “grupos financieros” en forma indistinta.

En el caso del sistema financiero uruguayo, las estructuras de conglomerados financieros que se han identificado, se pueden asimilar a alguno de los siguientes dos tipos:

- Estructuras entidad controlante - subsidiaria: Donde una entidad que opera en el sistema cumple el rol de Entidad Controlante en relación a otras empresas vinculadas.
- Estructuras horizontales: Donde varias entidades son controladas por un accionista común (en el país o en el exterior), y ninguna de las entidades locales opera como controlante de las otras.

En el primer caso, la Dirección de la Entidad Controlante tendrá responsabilidades sobre la gestión de todo el conglomerado financiero en base consolidada, tanto en lo que refiere al funcionamiento del Gobierno Corporativo como en relación a la Gestión de Riesgos.

En el caso de las estructuras horizontales, la Dirección de cada una de las entidades locales a nivel individual deberá gestionar los eventuales impactos que puedan provenir de las entidades vinculadas locales.

Los Estándares Mínimos se aplicarán teniendo en cuenta las particularidades de la estructura adoptada por cada conglomerado financiero.

Definiciones

Marco de gestión de riesgos: incluye las políticas, procesos, controles y sistemas a través de las cuales se establece, comunica y monitorea el apetito de riesgo. Incluye además la declaración del apetito de riesgo, los límites de riesgo y un resumen de los roles y responsabilidades de los que supervisan la implementación y el monitoreo el apetito de riesgo. El marco debe tomar en cuenta los principales riesgos que enfrenta la institución y estar alineado con su estrategia y su plan de negocios.

Apetito de riesgo: El apetito de riesgo es el nivel y el tipo riesgo que una institución está dispuesta a asumir en sus exposiciones y actividades de negocio, teniendo en cuenta los objetivos definidos y las obligaciones con los accionistas y otras partes interesadas. El apetito de riesgo es generalmente expresado en términos cuantitativos y cualitativos y deben considerarse para definirlo la posibilidad de ocurrencia de condiciones y eventos extremos. El apetito de riesgo debe reflejar el potencial impacto en los resultados, el nivel de capital, el nivel de fondeo y la liquidez de la institución.

Declaración del apetito de riesgo: es el documento en el cual se establece el apetito de riesgo.

Límites de riesgo: Es la cantidad de riesgo aceptable relacionado a ciertos riesgos específicos o unidades específicas del negocio. Un sistema de límites debe incluir los límites de riesgo que no deben ser superados, de acuerdo con las políticas y los indicadores de alerta definidos.

Perfil de riesgo – valoración en un momento dado de las exposiciones al riesgo brutas de la institución o si procede exposiciones al riesgo netas.

Deber de diligencia - Deber de los miembros del Directorio de decidir y actuar con conocimiento de causa y prudencia en los asuntos de la institución. Suele interpretarse como la obligación de los directores de tratar los asuntos de la entidad como lo haría una «persona prudente» con sus asuntos personales.

Deber de lealtad - Deber de los directores de actuar de buena fe en el interés de la institución. El deber de lealtad debe impedir que cada director actúe en interés propio, o en el interés de otro individuo o grupo, a expensas de la institución sus accionistas y partes interesadas.

Conglomerado Financiero: conjunto o grupo formado por dos o más entidades interconectadas bajo un control común, o influencia significativa, de forma directa o indirecta, donde al menos alguna de ellas opera en algún sector regulado por la Superintendencia de Servicios Financieros.

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 como son la Auditoría Interna, la Auditoría Externa y Comité de Auditoría.

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

- Cultura corporativa apropiada con normas establecidas para un comportamiento responsable y ético.
- Marco de apetito de riesgo
- Responsabilidades bien definidas y comunicadas a toda la organización para la gestión de riesgos y controles, lo que se conoce como «las tres líneas de defensa»:
    - la línea de negocio;
    - una función de gestión del riesgo y de cumplimiento independientes de la primera línea de defensa; y
    - una función de auditoría interna independiente

La línea de negocio – primera línea de defensa - es donde se generan primordialmente los riesgos y es responsable de su gestión continua,

La Gestión del riesgo, -segunda línea de defensa-, es responsable de identificar, medir, controlar y monitorear el riesgo, en forma independiente de la primera línea de defensa. La función de cumplimiento es también parte de esta segunda línea; es responsable de realizar el seguimiento continuo del cumplimiento de la legislación, normas de gobierno corporativo, regulaciones, códigos y políticas a las que esté sujeta la institución.

La función de Auditoría Interna es la tercera línea de defensa. La misma debe realizar auditorías y revisiones independientes de las dos líneas anteriores, para garantizar al Directorio que el marco de gobierno general, incluido el marco de gestión de riesgos, es eficaz y que existen y se aplican consistentemente las políticas y procesos definidos.

- Debe existir una clara definición de roles y responsabilidades dentro de la organización y una estructura que permita establecer sus objetivos, determinando los medios para alcanzarlos y cómo supervisar su cumplimiento. La estructura organizacional debe permitir a la Dirección implementar una estrategia eficiente y efectiva para asegurar al mismo tiempo un fuerte control interno y un buen sistema de administración de riesgos a través de sistemas de información que garanticen su integridad, confiabilidad, oportunidad y accesibilidad. El Directorio y la Alta Gerencia de la institución deben ser integrados por personas con los conocimientos, experiencia y competencias necesarias para cumplir con sus respectivos roles. Deben planificar y dirigir la gestión comercial y de riesgos y manejar eficazmente la solvencia de la entidad.
- Debe promoverse una cultura de riesgo adecuada en relación al volumen y complejidad de las operaciones y al perfil de riesgo de la institución. Se considerarán en este capítulo los estándares mínimos que deben cumplir el Directorio, la Alta Gerencia, el Comité de Auditoría, la Auditoría Interna y la Auditoría Externa para asegurar un adecuado funcionamiento del Gobierno Corporativo.

DIRECTORIO

En adelante, cuando se hace referencia al Directorio debe entenderse como el órgano que ejerce la administración efectiva de la entidad. En las instituciones de intermediación financiera organizadas como sociedades anónimas será el Directorio estatutario, en las organizadas como cooperativas, será el Consejo Directivo o Mesa Directiva según definición estatutaria y en el caso de las sucursales de personas jurídicas extranjeras será el Directorio de la Casa Matriz o el órgano de control al que la Casa Matriz le haya asignado en forma expresa sus atribuciones respecto a la sucursal en el país.

El Directorio es el responsable último de definir la estrategia de negocios y controlar su implementación, vigilar la solvencia de la institución, tomar las decisiones sobre el personal clave, la organización interna y las prácticas de gobierno, fijar el apetito de riesgo y controlar la gestión del riesgo y el cumplimiento de las obligaciones legales y regulatorias. También es responsable de asegurar la implementación de un sistema de remuneración con los incentivos adecuados.

El cuidado, diligencia, habilidad y prudencia con la cual los integrantes del Directorio cumplen sus roles tiene una influencia crítica sobre la viabilidad, seguridad y solidez de la institución, sobre su capacidad de ejecutar la estrategia de negocio y cumplir los objetivos y sobre su capacidad de generar confianza a los depositantes, inversores, supervisores, calificadores y otros actores.

Los estándares mínimos que el Directorio debe cumplir son los que se detallan a continuación:

1 - El Directorio debe mantener una estructura apropiada que permita una visión independiente de la influencia de la Alta Gerencia, de influencias políticas y/o de otros intereses externos.

Para ello:

1.1 El Directorio debe incluir personas con un buen balance de habilidades, experiencia y conocimientos, que de forma colectiva posean las aptitudes necesarias conforme al tamaño, complejidad y perfil de riesgo de la institución y del conglomerado cuando corresponda.

1.2 El Directorio debe comprender un número suficiente de directores independientes[5].

1.3 Los Directores No Ejecutivos[6] no deben tener injerencia en las decisiones diarias de la gestión.

1.4 Los Directores Ejecutivos no deben ejercer una influencia dominante en el conjunto del Directorio.

1.5 Los integrantes del Directorio deben tener un claro entendimiento de su rol dentro del Gobierno Corporativo y deben cumplir con el deber de lealtad y diligencia.

1.6 El Directorio debe poseer la capacidad de ejercer un juicio independiente sobre los asuntos de la institución financiera. Ello no obsta a que el Directorio pueda participar en el proceso de aprobación de algunas operaciones o en algunas decisiones operativas de significativa magnitud para la entidad.

1.7 El Directorio debe implementar una estructura de Comités de Dirección acorde con el volumen, complejidad de las actividades y perfil de riesgos de la entidad para asegurar la participación de los distintos sectores involucrados en las decisiones relevantes.

1.8 El Directorio y sus comités deben mantener documentadas sus deliberaciones y decisiones (por ejemplo, actas de reuniones o resúmenes de temas tratados, recomendaciones emitidas decisiones adoptadas y reportes utilizados para la toma de decisiones).

1.9 Los bancos de importancia sistémica deberán contar con un Comité de Riesgos a nivel de Directorio.

El Comité de Riesgos debe:

- contar con un Presidente que sea director independiente
- incluir una mayoría de miembros no ejecutivos
- incluir miembros con experiencia en temas y prácticas de gestión de riesgos;
- analizar las estrategias de riesgo a nivel agregado y por tipo de riesgo y emitir las correspondientes recomendaciones al Directorio, así como sobre el apetito de riego;
- revisar periódicamente las políticas de riesgo y el apetito de riesgo de la institución y sus subsidiarias cuando corresponda
- vigilar la aplicación por la Alta Gerencia de la declaración de apetito por el riesgo
- vigilar las estrategias de gestión de capital y liquidez, así como de todos los riesgos relevantes para garantizar que son coherentes con el apetito de riesgo aprobado.

2. El Directorio debe asegurar un adecuado relacionamiento con el accionista o con la entidad controlante.

Para ello el Directorio debe asegurar que:

2.1 Existe una adecuada coordinación e integración entre las distintas estructuras de Gobierno Corporativo de la entidad y su controlante.

[5] **Director independiente**: miembro no ejecutivo del Directorio (ver Definición Director no ejecutivo – Pie de página # 6) sin responsabilidades de gestión en la institución y que no se encuentra sometido a ninguna influencia interna o externa, política o de propiedad, que le pudiera condicionar su opinión sobre los asuntos en los que debe intervenir. Será de aplicación a bancos privados sin perjuicio de que en el futuro se pueda evaluar su aplicación a otras entidades.

[6] **Director no ejecutivo:** Si bien no existe desde el punto de vista jurídico el concepto de Director No Ejecutivo, debe entenderse por tal a aquellos Directores que no cumplen ninguna función ejecutiva, aunque mantienen sus responsabilidades en tanto Directores.

2.2 Existe un adecuado control y monitoreo sobre las actividades tercerizadas, cuando sean realizadas por empresas relacionadas.

2.3 Sus roles y responsabilidades y los de su controlante se encuentran claramente establecidos y delimitados.

2.4 Su independencia es respetada por parte de su controlante en lo que refiere a las responsabilidades que debe asumir el Directorio.

3. El Directorio debe aprobar los objetivos estratégicos de la institución y supervisar su implementación, tanto a nivel individual como en base consolidada, cuando corresponda.

Para ello, el Directorio debe:

3.1 Aprobar un marco estratégico que defina claramente el o los negocios objetivo y los retornos esperados y que éstos sean consistentes con el nivel de riesgo definido. Este marco debe ser claramente plasmado en políticas escritas y comunicado a toda la institución.

3.2 Aprobar el Plan de Negocios que contemple los objetivos estratégicos definidos, dentro de los cuales se contemplarán los negocios de las distintas entidades que componen el Conglomerado.

3.3 Evaluar regularmente los resultados comparándolos contra el presupuesto aprobado.

3.4 Revisar por lo menos anualmente los objetivos estratégicos, los planes, el apetito de riesgo y los límites de riesgo para asegurar que siguen siendo válidos.

3.5 Asegurar la existencia de un sistema de información íntegro, confiable y oportuno que permita tomar sus decisiones y que asegure la efectividad de las mismas.

3.6 Aprobar una estrategia y políticas de Tecnología de la Información (TI) adecuadas a la estrategia general de la institución y asegurar que la Alta Gerencia implemente los procedimientos que las hace aplicables: Para lo cual debe asegurar que:

- Cuenta con una organización y con personal capacitado para una adecuada gestión de TI y de los riesgos asociados.
- El soporte de TI permite dar cumplimiento a los requerimientos legales, regulatorios, contractuales y operativos para el manejo de riesgos.

3.7 Aprobar una estrategia y políticas de Seguridad de la información adecuadas a la estrategia general de la institución y asegurar que la Alta Gerencia implemente los procedimientos que las hacen aplicables.

4. En un Conglomerado Financiero, el Directorio de la entidad controlante debe asegurar el establecimiento y funcionamiento de un marco de gobierno corporativo claro y adecuado para la estructura, negocio y riesgos del Conglomerado y sus entidades. El Directorio debe conocer y comprender la estructura organizativa del Conglomerado y los riesgos que asume.

A fin de cumplir sus responsabilidades, el Directorio de la entidad controlante debe:

4.1 Establecer un marco de gobierno corporativo con funciones y responsabilidades claramente definidas.

4.2 Ser consciente de los riesgos sustanciales que puedan afectar tanto a la entidad controlante como a sus subsidiarias, incluyendo tanto a entidades locales como del exterior, reguladas y o no reguladas.

4.3 Ejercer una vigilancia adecuada de las subsidiarias, al tiempo que respeta la independencia de las responsabilidades jurídicas y de gobierno que puedan corresponder a los Directorios de las mismas.

4.4 Asegurar que la estructura del Conglomerado:

- Sea clara y transparente, evitando la existencia de estructuras opacas, carentes de sustancia económica o fines empresariales. En este sentido, la realidad jurídica debe ser consistente con la realidad económica.
- Deje de manifiesto la unidad quién ejerce el control final del Conglomerado.
- Resulte adecuada al perfil de riesgos y modelo de negocio del Conglomerado.
- Permita al supervisor ejercer una supervisión efectiva sobre las actividades del Conglomerado.

4.5 Incluir en el marco de gobierno corporativo del Conglomerado políticas y procedimientos para identificar y tratar potenciales conflictos de intereses intragrupo,

4.6 Asegurar que existen políticas y procedimientos claramente definidos en relación a las operaciones entre empresas del Conglomerado, para:

- Evaluar su riesgo,
- Ser sometidas a límites apropiados
- Ser pactadas en condiciones de mercado de forma de evitar desventajas en perjuicio de alguna entidad del grupo o sus clientes.

4.7 Asegurar que existan sistemas eficaces para intercambiar información, y gestionar los riesgos de las distintas entidades del Conglomerado, y de éste en su conjunto.

4.8 Comunicar oportunamente al supervisor cualquier cambio de estructura, de la situación económica financiera o de cualquier otro hecho relevante del Conglomerado.

5. El Directorio debe seleccionar, monitorear y si es necesario reemplazar a la Alta Gerencia.

Para ello, el Directorio debe:

5.1 Aprobar los roles y responsabilidades de la Alta Gerencia.

5.2 Evaluar si el conocimiento, integridad y experiencia de la Alta Gerencia siguen siendo apropiados dada la naturaleza del negocio y el perfil de riesgo del banco.

5.3 Evaluar regularmente la efectividad y prudencia de la Alta Gerencia en la gestión de las operaciones y de los riesgos, así como de los Directorios de las empresas subsidiarias, cuando corresponda y establecer las posibles consecuencias si dichas acciones no se alinean con las expectativas de desempeño del Directorio. Esto incluye respetar los valores de la institución, su cultura y apetito de riesgo en todas las circunstancias.

5.4 Asegurar que las actuaciones de la Alta Gerencia son coherentes con la estrategia y políticas aprobadas por el Directorio, incluido el apetito de riesgo.

5.5 Cuestionar y revisar de forma crítica las explicaciones e información facilitada por la Alta Gerencia.

5.6 Aprobar los planes de sucesión del Gerente General y de la Alta Gerencia.

6. El Directorio debe aprobar el marco de gestión de riesgos que contenga la declaración de apetito de riesgo consistente con los objetivos estratégicos, los límites de riesgo y políticas asociadas que permitan ~~y~~ el control de todos los riesgos que puedan afectar el cumplimiento de los objetivos de la entidad, tanto a nivel individual como en base consolidada.

Para ello el Directorio debe:

6.1 Entender los riesgos que enfrenta la entidad y el Conglomerado de manera integral, incluyendo aquellos riesgos provenientes de entidades no reguladas establecidas en el país o en el

exterior, así como también vehículos de propósito especial y definir el nivel de exposición a cada tipo de riesgo en forma individual.

6.2 Promover una cultura de riesgos en la organización y en todas las entidades del Conglomerado.

6.3 Aprobar el marco de gestión de riesgos que incluya la declaración del apetito de riesgo , los roles y responsabilidades asociados y los mecanismos de medición y seguimiento...

La declaración del apetito de riesgo debe:

- Ser consistente con la estrategia general, y el Plan de Negocios definidos.
- Contemplar los riesgos propios de la naturaleza del Conglomerado cuando corresponda
- Estar claramente definida por escrito y cumplir con los requisitos regulatorios y ser adecuada para la índole y complejidad de las actividades de la institución.
- Fijar niveles deseados de riesgo tanto cuantitativos como cualitativos

6.4 Asegurar que la Alta Gerencia implemente un sistema de gestión integral de riesgos que contemple el apetito de riesgo definido por el Directorio, y que involucra a todo el personal.

6.5 Asegurar que cuenta con los recursos requeridos para gestionar los riesgos dentro del marco establecido y tomando en cuenta las presiones externas de precio, tiempo y/o estructura que puedan sobrevenir.

6.6 Asegurar que existan políticas y procedimientos escritos que constituyan una guía efectiva para asumir y gestionar los riesgos y que dichos procedimientos estén implementados previo a la realización de nuevas actividades o al lanzamiento de nuevos productos.

6.7 Asegurar que se cuenta con programas de pruebas de tensión prospectivas, acordes con el perfil de riesgo como parte integral del proceso de gestión del riesgo.

6.8 Asegurar que existe una gestión de la seguridad de la información cuyos objetivos se encuentran alineados con los del negocio.

6.9 Asegurar que existe un sistema de Evaluación de Riesgos que garantiza el logro de los objetivos de TI y de seguridad de la información y que permita a la institución responder a las amenazas que pueden afectar estos servicios.

6.10 Asegurar que los procesos de TI se monitorean y son auditados regularmente por personas independientes.

6.11 Asegurar que la institución cuenta con un plan de continuidad del negocio adecuado al volumen, naturaleza y complejidad de sus operaciones y que, en particular, incluya un plan de contingencia de TI.

7. El Directorio 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.

Para ello el Directorio debe:

7.1 Establecer y comunicar los estándares éticos (a través de un Código de Ética) que guíen el accionar de la institución financiera, así como del Conglomerado.

7.2 Definir una política sobre conflictos de intereses y un procedimiento de cumplimiento para su aplicación.

7.3 Actuar como ejemplo del cumplimiento de los estándares éticos.

7.4 Asegurar que la Alta Gerencia implementa políticas y procedimientos adecuados para evitar o administrar los posibles conflictos de interés y confirmar que los empleados y la Alta Gerencia son conscientes de que se tomarán medidas disciplinarias u otras medidas apropiadas ante comportamientos inaceptables o infracciones.

7.5 Asegurar que existen políticas y procedimientos claramente definidos para el tratamiento de operaciones con el personal superior o con empresas vinculadas a éste o al accionista. Estas políticas deben incluir la aprobación por parte del Directorio de las operaciones más significativas (excluyendo a los Directores que pueden tener conflictos de interés).

7.6 Asegurar que existen políticas y procedimientos claramente definidos en relación a las operaciones entre empresas del conglomerado, de forma de evaluar sus riesgos y asegurar que sean pactadas en condiciones de mercado evitando desventajas en perjuicio de alguna entidad del grupo o sus clientes.

7.7 Asegurar que las políticas de compensación son transparentes y consistentes con la estrategia global de largo plazo la cultura y apetito de riesgo a largo plazo de la institución y que existen mecanismos para verificar su cumplimiento. El sistema de remuneración debe crear los incentivos necesarios para gestionar en forma adecuada el riesgo, el capital y la liquidez.

7.8 Vigilar la integridad, independencia y eficacia de las políticas y procedimientos de denuncia de irregularidades de la institución.

8. El Directorio debe promover una cultura de control en la institución y a nivel del Conglomerado cuando corresponda, verificando que la Alta Gerencia implementa las políticas y procedimientos necesarios para que todos entiendan su rol en el control interno y la gestión de riesgos.

Para ello, el Directorio debe:

8.1 Promover una cultura de riesgo y transmitir que todos los empleados son responsables de ayudar a la institución a operar dentro del grado de apetito de riesgo y las delimitaciones del riesgo establecidas.

8.2 Aprobar la estructura organizativa acorde al tamaño, complejidad, naturaleza y volumen de las operaciones y al perfil de riesgos de la institución y asegurar que la misma es conocida por toda la organización. Esta estructura debe asegurar:

- Una clara separación y equilibrio de las funciones comerciales y de toma de riesgos de las funciones de monitoreo y control.
- Que existan sendas funciones de riesgo y de cumplimiento claramente definidas e independientes de la gestión, contando con la suficiente autoridad, relevancia, recursos y acceso al Directorio.
- Que existe una adecuada segregación de funciones que facilite los controles cruzados.
- Que exista una función de Auditoría Interna, independiente de la gestión, que cuente con la suficiente autoridad, relevancia, recursos y acceso al Directorio

8.3 Asegurar que existen mecanismos de control interno efectivos, acorde a la naturaleza y complejidad de las operaciones.

8.4 Asegurar que existe una clara definición de deberes y responsabilidades que sea consistente con la estrategia definida y que permita una clara asignación de autoridad.

8.5 Asegurar que la estructura organizativa definida permite un monitoreo de la subsidiarias y que sus actividades se incluyen dentro de los controles y auditorías regulares.

8.6 Controlar a la Alta Gerencia en la implementación de las estrategias y el cumplimiento de las políticas establecidas.

8.7 Asegurar que el nivel de control se mantiene aún en el caso de tareas tercerizadas.

8.8 . Asegurar que el Comité de Auditoría y/o la Auditoría Interna brinden garantías sobre el Sistema de información Gerencial de modo que el mismo sea oportuno, íntegro y confiable.

9. El Directorio debe asegurar que el Comité de Auditoría cumple su cometido.

Para ello, el Directorio debe:

9.1 Aprobar un estatuto o misión que establezca el propósito del Comité, sus objetivos, organización, autoridad y responsabilidad, así como las características que debe tener el Registro de Control Interno.

9.2 Asegurar que la integración de este Comité de Dirección es acorde con la naturaleza, complejidad y volumen de las operaciones de la institución y que permite cumplir su cometido con independencia. Para ello, la mayoría de los miembros no deben estar involucrados con la gestión diaria de la entidad.

9.3 Asegurar que la experiencia de todos sus miembros es compatible con sus obligaciones.

9.4 Proveer al Comité de Auditoría de apoyo y recursos para que pueda desempeñar sus funciones en forma independiente.

9.5 Asegurar que la periodicidad de las reuniones es suficiente para monitorear y evaluar el adecuado funcionamiento de los mecanismos de control interno.

9.6 Tener comunicación regular con el Comité de Auditoría promoviendo la rápida resolución de debilidades encontradas.

9.7 En caso de corresponder, asegurar que el Comité de Auditoría considere el impacto de estar integrando un Conglomerado.

10. El Directorio debe asegurar que la función de Auditoría Interna cumple su cometido.

Para ello el Directorio debe:

10.1 Asegurar que la Auditoría Interna es independiente de las actividades auditadas y que cuenta con la suficiente autoridad y jerarquía para poder actuar con objetividad e imparcialidad.

10.2 Asegurar que la línea de reporte es a sí mismo o al Comité de Auditoría. En el caso de las sucursales, deberá reportar además a la Auditoría Interna corporativa y debe tener independencia presupuestal respecto a las operaciones locales.

10.3 Asegurar que la función de Auditoría Interna es llevada a cabo por personal independiente, competente y capacitado y que existen recursos suficientes para cumplir con los objetivos establecidos y el plan anual.

10.4 Asegurar, en forma directa o a través del Comité de Auditoría que el Auditor Interno cumple con sus cometidos con eficacia y eficiencia.

10.5 Asegurar el acceso de la Auditoría Interna a la información necesaria para ejercer su función con eficacia.

10.6 Asegurar que la Alta Gerencia actúa para resolver deficiencias o debilidades encontradas por la Auditoría Interna.

11. El Directorio debe asegurar que la Auditoría Externa cumple su cometido.

Para ello, el Directorio debe:

11.1 Reconocer y comunicar la importancia de la función de Auditoría Externa dentro de la organización.

11.2 Tomar las medidas necesarias para asegurar la independencia de la Auditoría Externa dentro de la organización.

11.3 Asegurar que la Alta Gerencia toma las medidas necesarias para corregir los problemas detectados oportunamente.

12. El Directorio debe implementar un proceso para evaluar la suficiencia del capital en función del perfil de riesgo de la institución y contar con una estrategia eficaz para mantener en el corto y mediano plazo un nivel y una composición adecuados para respaldar los riesgos asumidos y proveer seguridad a los depositantes y otros acreedores, tanto a nivel individual como del conglomerado financiero cuando corresponda.

Para ello el Directorio debe:

12.1 Implementar un proceso sistemático e integral para determinar el nivel y calidad de capital tanto en forma individual como en base consolidada tomando en cuenta una serie de factores:

- La estrategia de negocios actual y futura.
- El perfil de riesgos y apetito de riesgo
- La capacidad del capital de absorber pérdidas por eventos no anticipados e incertidumbre en los propios sistemas de medición.

A efectos de la estimación del capital a nivel del conglomerado financiero en forma consolidada se deberá considerar especialmente:

- Las potenciales situaciones de doble o múltiple apalancamiento, así como situaciones de endeudamiento excesivo o de inversiones recíprocas entre entidades del conglomerado.
- Las limitaciones a las transferencias de capital inter empresa, las cuales podrían limitar la capacidad de considerar los excesos de capital de una entidad en la evaluación del capital global.
- Estimaciones de capital necesario para los riesgos asumidos por entidades no reguladas.
- Los riesgos a nivel agregado del Conglomerado Financiero.

ALTA GERENCIA

Las responsabilidades de la Alta Gerencia se centran en la implementación de las políticas, procedimientos, procesos y controles necesarios para gestionar las operaciones y riesgos en forma prudente para cumplir con los objetivos estratégicos y el apetito de riesgo fijados por el Directorio y en asegurar que éste recibe información relevante, íntegra y oportuna que le permita evaluar la gestión y analizar si las responsabilidades delegadas a la Alta Gerencia se están cumpliendo efectivamente.

En general, debe entenderse como Alta Gerencia al equipo formado por la Gerencia General o similar y las líneas de reporte relevantes, quienes en su conjunto son los responsables de la ejecución de la estrategia de la institución

Los estándares mínimos que la Alta Gerencia debe cumplir son los que se detallan a continuación:

13. La Alta Gerencia como equipo y cada uno de sus integrantes deben poseer los conocimientos y habilidades para gestionar y supervisar la actividad de conformidad con la estrategia del negocio, el apetito de riesgo y otras políticas aprobadas por el Directorio.

Para ello, la Alta Gerencia debe:

13.1 Estar integrada por personas con capacidad, experiencia e integridad necesarias para gestionar las actividades y el personal bajo su supervisión.

13.2 Trabajar como equipo respetando los roles de los distintos integrantes y asegurar el cumplimiento de las directivas establecidas por el Directorio.

13.3 Ejercer una adecuada vigilancia de sus subordinados y garantizar que las actividades de la institución son coherentes con la estrategia de negocio, apetito de riesgo y políticas aprobadas por el Directorio.

13.4 Tener acceso regular a capacitación para mantener y mejorar sus competencias y mantenerse al tanto de los desarrollos relevantes para sus áreas de responsabilidad.

14. La Alta Gerencia debe establecer y seguir un proceso continuo y adecuado para la gestión estratégica de la entidad en función de los lineamientos del Directorio y rendir cuentas a éste de lo actuado.

Para ello, la Alta Gerencia debe:

14.1 Desarrollar y presentar al Directorio para su aprobación:

- El plan de negocios en base a los lineamientos estratégicos y a la declaración de apetito de riesgo definidos por el Directorio, que considere las características del entorno económico y de negocios, la situación financiera y patrimonial de la institución y los riesgos en los cuales tiene o tendrá exposiciones.
- El presupuesto anual.
- El plan de continuidad del negocio

14.2 Implementar la estrategia y el plan de negocios aprobado.

14.3 Asegurar que la estructura organizacional es consistente con los objetivos estratégicos y políticas aprobadas por el Directorio.

14.4 Monitorear periódicamente el cumplimiento con respecto al presupuesto y al plan de negocios y analizar los desvíos.

14.5 Proveer al Directorio de información completa, relevante, oportuna y periódica al menos sobre los siguientes temas:

- implementación de la estrategia y de los planes,
- cambios en la estrategia del negocio, en la estrategia de riesgo o apetito de riesgo
- los resultados y condición financiera de la institución
- excepciones a los límites del riesgo y/o infracciones a las normas de cumplimiento
- deficiencias en los controles internos;
- inquietudes jurídicas o reguladoras;
- denuncia de irregularidades
- resultados de las pruebas del plan de continuidad

14.6 Poner en práctica las políticas de compensación fijadas por el Directorio.

15. La Alta Gerencia debe implementar un sistema de gestión integral de riesgos que contemple el apetito de riesgo, involucre a todo el personal y sea proactivo.

Para ello, la Alta Gerencia debe:

15.1 Implementar la estrategia de riesgos aprobada por el Directorio.

15.2 Asegurar que existe un responsable del manejo de cada uno de los riesgos y un sistema que permita obtener una visión integral de los riesgos que asume la entidad.

15.3 Desarrollar, poner en práctica y hacer cumplir los procesos y procedimientos que permitan identificar, medir, monitorear y controlar todos los riesgos que puedan afectar el cumplimiento de los objetivos de la institución. Estos procedimientos deben considerar el riesgo en todas las actividades de la institución, dentro y fuera de balance, y a nivel de cartera, línea de negocio y de grupo.

15.4 Asegurar que cuenta con los recursos suficientes para un manejo adecuado de acuerdo al marco de riesgos determinado por la Dirección.

15.5 Asegurar que el personal involucrado en el proceso de Gestión de Riesgos tiene la capacidad técnica para comprender y analizar los riesgos asumidos. La descripción de funciones, cargos y responsabilidades del personal involucrado deberá incluir explícitamente el rol en el sistema de gestión integral de riesgos.

15.6 Implementar procedimientos sobre las políticas de seguridad de la información aprobadas por el Directorio.

15.7 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.

15.8 Evaluar y revisar periódicamente los riesgos a los que se enfrenta la institución y su perfil general de riesgo reportándolo oportunamente al Directorio.

16. La Alta Gerencia debe promover una cultura de control en toda la organización.

Para ello, la Alta Gerencia debe:

16.1 Diseñar y mantener una estructura organizacional de acuerdo a los lineamientos aprobados por el Directorio, que asegure un adecuado sistema de control.

16.2 Diseñar un sistema de comunicación que asegure que todo el personal de la institución entiende y cumple su rol en el control interno.

16.3 Asegurar que existen comités y delegaciones de responsabilidades que aseguren la coordinación y comunicación de actividades entre distintas áreas y que promuevan la transparencia y rendición de cuentas.

16.4 Asegurar que los comités mantengan adecuadamente documentadas sus deliberaciones y decisiones (por ejemplo, actas de reuniones o resúmenes de temas tratados, recomendaciones emitidas y decisiones adoptadas).

16.5 Demostrar en su actuación diaria un claro compromiso con el control.

16.6 Mantener un seguimiento estricto de los riesgos derivados de las actividades tercerizadas, evaluando su impacto en la calidad del sistema de control.

16.7 Tomar las medidas necesarias para corregir los problemas detectados por el Auditor Interno o Auditor Externo y Supervisores.

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

16.9 Proporcionar al Directorio la información que necesite para efectuar sus funciones de supervisión de la Alta Gerencia y evaluar la calidad de su desempeño.

17. La Alta Gerencia debe implementar las políticas aprobadas por el Directorio para evitar o administrar posibles conflictos de interés y establecer los procedimientos de control necesarios.

Para ello, la Alta Gerencia debe:

17.1 Implementar las políticas y procedimientos para identificar, evitar o administrar y explicitar adecuadamente los conflictos de intereses, en particular, en lo vinculado a las operaciones con entidades relacionadas.

17.2 Asegurar, en caso de concederse préstamos a los empleados, que existen procedimientos que regulen la operativa y su efectivo cumplimiento. Estas operaciones deben estar sujetas a revisión de los Auditores Internos y Externos.

17.3 Implementar procedimientos que aseguren que la entidad cumple efectivamente con lo dispuesto por la ley en relación a la concesión de créditos o avales al personal superior, así como a empresas o a instituciones de cualquier naturaleza en las que el personal superior actúe en forma rentada u honoraria.

18. La Alta Gerencia debe implementar un proceso íntegro de gestión de la Tecnología de Información (TI) consistente con la estrategia.

Para ello se debe cumplir que:

18.1 Los roles del responsable del área de TI se encuentran claramente definidos.

18.2 Existen políticas de medición y mitigación de los riesgos en los procesos.

18.3 Se entiende y se comunica la necesidad de cumplir con los requerimientos del organismo supervisor.

18.4 El Área de TI esté ubicada dentro de la estructura general de la organización de modo de garantizar la competencia técnica e independencia respecto de las áreas usuarias, para garantizar soluciones de tecnología de la información útiles para la organización.

18.5 El área de TI tenga la habilidad de desarrollar, adquirir, instalar y mantener soluciones apropiadas y acordes a las necesidades de la entidad, en forma prudente y dentro de un ambiente controlado.

18.6 Existan procedimientos de control de la gestión del área de TI. Los servicios a ser prestados por el área de TI deben ser monitoreados (indicadores clave del desempeño y/o factores críticos de éxito) por la Alta Gerencia y comparados con los niveles mínimos establecidos. La evaluación del desempeño del área de TI debe llevarse a cabo en forma continua.

18.7 Se mida, a intervalos regulares, la satisfacción del cliente sobre los servicios prestados por el área de TI para identificar el déficit en los niveles de servicio y establecer objetivos de mejoras.

18.8 Los procesos que no alcancen las metas mínimas de desempeño establecidas, se seleccionan para ser incluidos en procesos de mejoras.

19. La Alta Gerencia debe definir e implementar un sistema de información adecuado para cuantificar, evaluar e indicar el volumen, composición y calidad de las exposiciones de los riesgos que asume la entidad. La información debe ser confiable, oportuna, fácilmente accesible y provista en un formato adecuado.

El sistema de información debe:

19.1 Cubrir todas las actividades significativas de la institución.

19.2 Captar la información relevante de todas las entidades que conforman el Conglomerado cuando corresponde, recogiendo especialmente la información de operaciones y exposiciones intra-grupo y concentraciones de exposiciones con terceros.

19.3 Estar integrado por información financiera, operativa, de riesgos y de cumplimiento adecuada y completa. Se deberá explicitar el sistema de reportes de forma que incluya tanto los reportes utilizados internamente como los que se emiten para terceras partes.

19.4 Incluir información sobre eventos externos y condiciones relevantes a la toma de decisiones.

19.5 El proceso de generación de información debe ser seguro, estar independientemente monitoreado y respaldado con planes de contingencia adecuados.

19.6 El sistema de información debe 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.
- Precisión – El sistema de controles sobre el procesamiento de información debe ser efectivo.
- Consistencia – La información debe ser procesada y compilada en forma consistente y uniforme. Los cambios en los sistemas deben estar adecuadamente documentados y claramente comunicados a los usuarios de la información.
- Integridad – Los tomadores de decisiones deben contar con información completa y pertinente en forma sintetizada.
- Relevancia - Está directamente relacionado con las necesidades de la Gerencia y la Dirección para el desarrollo de su trabajo.

19.7 Los informes remitidos al organismo supervisor y al Directorio deben proveer datos confiables, para lo cual se deben verificar previamente.

COMITÉ DE AUDITORÍA

20. El Comité de Auditoría debe asegurar que el sistema de gestión integral de riesgos de la institución es adecuado y que se toman las medidas necesarias para su mantenimiento en forma continua.

Para ello, el Comité de Auditoría debe:

20.1 Estar conformado adecuadamente de forma de asegurar el cumplimiento de los objetivos fijados para esta estructura de control.

20.2 Tomar medidas para que la Alta Gerencia lleve a cabo las acciones correctivas necesarias para subsanar las observaciones de la Auditoría Interna, Externa y del Supervisor de manera oportuna y monitorear su implementación. Para ello se debe tener en cuenta los informes de la entidad individual como del resto de las entidades del conglomerado. También se deben considerar la resolución de los hallazgos de las distintas entidades pertenecientes al Conglomerado cuando corresponda.

20.3 Proveer información al Directorio que le permita evaluar el desempeño del Comité de Auditoría y sus preocupaciones.

20.4 Asegurar que la Alta Gerencia establece y mantiene un adecuado y efectivo sistema de gestión integral de riesgos

20.5 Implementar un proceso orientado a identificar áreas de riesgo donde se debe profundizar las tareas de Auditoría y documentar sus resultados por lo menos anualmente.

20.6 Aprobar el Estatuto del Auditor Interno en donde se establece el propósito de la Auditoría Interna, sus objetivos, su autoridad y responsabilidades.

20.7 Analizar y aprobar el plan y cronograma anual de Auditoría Interna y monitorear su funcionamiento y desempeño en el cumplimiento de los planes de Auditoría oportunamente aprobados.

20.8 Asegurar que la Auditoría Interna revise los riesgos derivados de pertenecer a un conglomerado financiero (Ej. operaciones intra-grupo).

20.9 Contar con un proceso para aprobar —o bien para recomendar que se apruebe— la designación, reelección, sustitución y remuneración del Auditor Externo e informar al Directorio. Esta contratación también puede ser realizada por el propio Directorio.

20.10 Validar el plan de trabajo de la Auditoría Externa y efectuar un seguimiento de la independencia y eficacia del Auditor Externo, asegurando que otras tareas adicionales (por ejemplo, consultorías) son compatibles y no impactan negativamente su independencia.

20.11 Revisar los informes de la Auditoría Externa y de la Auditoría Interna tanto de la entidad individual, como del resto de las entidades del Conglomerado, cuando corresponda.

20.12 Establecer una comunicación eficaz con el Auditor Externo y exigirle que le informe sobre todos los asuntos pertinentes de forma que permita a dicho comité desempeñar sus responsabilidades de vigilancia y mejorar la calidad de la auditoría.

20.13 Acceder a los resultados obtenidos por el Síndico o la Comisión Fiscal en la realización de sus tareas, según surja de sus respectivos informes.

20.14 Mantener comunicación periódica con la Superintendencia de Servicios Financieros a fin de conocer sus inquietudes, los problemas detectados en la supervisión de la institución, así como el seguimiento llevado a cabo para su solución.

20.15 Revisar las políticas establecidas en la institución relativas al cumplimiento de leyes y regulaciones, normas de ética, conflictos de intereses e investigaciones por faltas disciplinarias y fraude.

AUDITORÍA INTERNA

21. La función de Auditoría Interna debe proporcionar fiabilidad al Directorio y al Comité de Auditoría sobre la calidad y eficacia de los sistemas y procesos de control interno, sobre los procesos de gestión del riesgo, cumplimiento y gobierno corporativo de la institución, ayudando con ello al Directorio y al Comité de Auditoría a proteger su organización y reputación.

Para el cumplimiento el Auditor Interno debe:

21.1 Tener un mandato claro, rendir cuentas al Directorio y al Comité de Auditoría ser independiente de las actividades auditadas. Debe contar con suficiente prestigio, destrezas, recursos y autoridad en la institución para desempeñar sus funciones de forma eficaz y objetiva.

21.2 Elaborar y someter a la aprobación del Comité de Auditoría un Estatuto de Auditoría Interna en el cual se establezcan los objetivos, funciones, autoridad, responsabilidades, políticas de la Auditoría Interna y en el caso de ser aplicable para la tercerización de tareas de Auditoría interna.

21.3 Contar con los conocimientos y experiencia adecuados en forma individual y colectiva.

21.4 Cumplir con los estándares y prácticas internacionales de auditoría interna y con el código de ética pertinente.

21.5 Implementar procesos que aseguren que las pruebas, hallazgos y acciones correctivas son documentados adecuadamente y realizar un seguimiento proactivo de las debilidades encontradas.

21.6 Desarrollar y presentar al Comité de Auditoría un plan anual de Auditoría basado en riesgos. El plan anual debe contener el alcance, los ciclos a auditar con su valoración de riesgo, , cronogramas, recursos humanos necesarios, sistema de reportes y de ser aplicable, el presupuesto financiero requerido.

21.7 El alcance debe ser determinado en base a riesgos y debe cubrir todas las actividades (incluso las tercerizadas) de la entidad y tomar en cuenta los riesgos derivados de pertenecer a un conglomerado financiero.

21.8 Deberá evaluar la efectividad y eficiencia, al menos de:

- La aplicación de las técnicas de gestión del riesgo y de los métodos de evaluación del riesgo
- El sistema de información gerencial y sus procesos.
- los procesos de TI y de gestión de seguridad de la información.
- los controles internos
- la precisión y confiabilidad de los registros contables y los informes financieros y de gestión;
- los métodos para custodiar activos de forma segura;
- el sistema de cálculo del nivel de capital de la institución en relación con sus estimaciones de riesgo
- los sistemas diseñados para asegurar el cumplimiento de los requisitos legales, normativos y contractuales, así como del código de ética.
- la comprobación de las transacciones, de la puesta en práctica de políticas, procedimientos y límites adecuados y del funcionamiento de los mecanismos de control;
- la comprobación de la fiabilidad y oportunidad de los informes exigidos por el supervisor
- Cuando la institución utilice modelos para medir los riesgos se debe realizar validaciones periódicas e independientes de los mismos.
- El seguimiento de las recomendaciones realizadas.

21.9 Implementar el plan aprobado e informar al Comité de Auditoría sobre la existencia de desvíos significativos y el impacto de dichos desvíos sobre el cumplimiento de los objetivos establecidos.

21.10 Presentar sus informes de actuación con sus conclusiones y recomendaciones al Comité de Auditoría para su información y acción.

21.11 Mantener estrecha coordinación con otras estructuras de control (Síndico, Comisión Fiscal, etc.) que aseguren la cobertura de todas las actividades de la entidad.

AUDITORÍA EXTERNA

22. La Auditoría Externa debe aportar una seguridad razonable de que los estados financieros en su conjunto están libres de incorrección material, debido a fraude o error, que permita al auditor expresar una opinión sobre si los estados financieros están preparados, en todos los aspectos materiales, de conformidad con un marco de información financiera aplicable.

Para ello, la institución debe asegurar que el auditor externo:

22.1 Designa un equipo de Auditoría que cuenta con un número adecuado de personas competentes para la función y con conocimiento del negocio

22.2 Comprende su responsabilidad hacia la institución y todas las partes interesadas.

22.3 Actúa con objetividad e independencia en la planificación de las actividades y en la ejecución de la auditoría.

22.4 Reporta todos los hallazgos significativos y conclusiones de su trabajo tanto a la Dirección como al supervisor.

ESTÁNDARES DE GESTIÓN DE RIESGOS (R)

EL SISTEMA DE GESTIÓN INTEGRAL DE RIESGOS

El negocio de una institución financiera implica asumir riesgos para generar ganancias. Como consecuencia, una competencia clave de cualquier institución financiera es su capacidad de gestionar los riesgos que asume en forma prudente y rentable. La institución debe implementar un Sistema de Gestión Integral de Riesgos, definido como el conjunto de políticas, procedimientos y mecanismos de control implementados por la entidad para propiciar una apropiada identificación, medición, control y monitoreo de los riesgos a los que se encuentra expuesto y evaluar la suficiencia de su capital y liquidez en relación con su perfil de riesgo y la situación macroeconómica y de los mercados.

Las prácticas de gestión de riesgos deberán aplicarse tanto a nivel individual como en base consolidada, cuando corresponda.

Para el caso de aquellas entidades controlantes de un conglomerado financiero, la gestión de riesgos deberá ser ejercida tanto en forma individual, como en base consolidada, considerando todos los riesgos relevantes de las entidades subsidiarias.

Para aquellas entidades que formen parte de un conglomerado, no siendo estas la entidad controlante, dentro de su gestión de riesgos deberán considerar el potencial impacto del vínculo con otras entidades del grupo, especialmente aquel proveniente de operaciones y exposiciones intra- grupo, contagios, y problemas reputacionales entre otros.

RIESGO DE CRÉDITO

El riesgo de crédito se define como la posibilidad de que la entidad vea afectadas sus ganancias o su patrimonio debido a la incapacidad del deudor de cumplir con los términos del contrato firmado con la institución o de actuar según lo pactado. El riesgo crediticio puede encontrarse en todas las actividades donde el éxito depende del cumplimiento del deudor o contraparte. El riesgo crediticio se encuentra cada vez que la institución extiende o compromete fondos, coloca en custodia, invierte o se expone en otra forma a través de un acuerdo existente o implícito que puede reflejarse o no en sus estados contables.

Dentro del riesgo de crédito también se incluye el riesgo de sufrir pérdidas en los activos causadas por hechos económicos, sociales o políticos acaecidos en un país extranjero.

La institución debe de disponer de una visión integral de las exposiciones al riesgo de crédito en el conjunto del banco y del conglomerado.

A - MARCO DE RIESGOS, POLÍTICAS Y PROCEDIMIENTOS

23. El Directorio debe aprobar la estrategia de negocios y las políticas para la gestión del riesgo de crédito en base individual y consolidada y revisarlas periódicamente. La estrategia debe contemplar el apetito de riesgo, el perfil de riesgos de la institución y entidades controladas y la situación macroeconómica y de los mercados. El Directorio debe revisar regularmente las exposiciones al riesgo de crédito y asegurar que los niveles de riesgos se encuentran dentro del marco establecido.

Para ello el Directorio debe:

23.1 Aprobar la estrategia de negocios y políticas de gestión del riesgo de crédito y revisarlas periódicamente. Estas políticas deben ser consistentes con el apetito de riesgo definido y deben ser aplicadas a nivel de las entidades individuales y en forma consolidada y cuando corresponda y ser divulgadas eficazmente a toda la institución.

Las mismas deben:

- Contemplar el ciclo de vida completo del crédito, incluida la concesión el análisis del crédito, la gestión continua del portafolio de crédito y la recuperación (incluidas las cuentas fuera de balance).
- Incluir tipos, niveles y límites de riesgos aceptables acordes con el apetito de riesgo y perfil de riesgo de la institución.
- Identificar los mercados objetivo.
- Prever mecanismos de identificación y notificación de excepciones a las mismas.

23.2 Evaluar periódicamente los resultados de la institución y en función de los mismos evaluar cambios en las políticas de riesgo..

23.3 Revisar las estrategias, políticas y apetito de riesgo en función de los resultados de la pruebas de estrés. y sus mediciones de riesgos.

23.4 Asegurar que la institución cuenta con una estructura organizacional adecuada para la gestión del riesgo de crédito.

23.5 Promover que exista un equilibrio razonable entre las áreas comerciales y de riesgos. Esta última debe disponer de recursos suficientes, independencia, autoridad y acceso al Directorio de forma de poder desempeñar eficazmente sus tareas.

23.6 Establecer claramente las funciones, responsabilidades y atribuciones en materia de identificación, aprobación, medición y control del riesgo de crédito. Identificar líneas de responsabilidad y autoridad en la gestión del riesgo de crédito.

23.7 Contar con información suficiente, detallada y oportuna sobre el riesgo de crédito de forma que le permita comprender los riesgos asumidos y evaluar el desempeño de la Alta Gerencia en el monitoreo y control de dicho riesgo.

23.8 Asegurar la realización de revisiones independientes para que en forma periódica se validen los procesos, las políticas, los procedimientos. Asegurar que se instrumenten las acciones apropiadas ante las debilidades o fallas significativas detectadas por el auditor interno, externo, supervisor o profesional independiente.

23.9 Asegurar que la Alta Gerencia implemente las políticas y los procesos necesarios para que los riesgos asumidos sean consistentes con las estrategias y políticas aprobadas.

24. La Alta Gerencia debe implementar la estrategia y las políticas aprobadas por el Directorio para la gestión del riesgo de crédito y desarrollar procedimientos para su identificación, medición, monitoreo y control. Estas políticas y procedimientos deben considerar el riesgo de crédito tanto a nivel de riesgos crediticios individuales como del total de la cartera.

Para ello, la Alta Gerencia debe:

24.1 Implementar las políticas y desarrollar procedimientos para gestionar el riesgo de crédito de forma consistente con la estrategia y las políticas definidas.

24.2 Asignar claramente las funciones, responsabilidades y atribuciones en materia de identificación, aprobación, medición y control del riesgo de crédito

24.3 Asignar los recursos necesarios en cantidad, calidad a efectos de un buen manejo del riesgo de crédito.

24.4 Asegurar que las personas involucradas en el proceso de crédito cuenten con las competencias, conocimiento técnico y experiencia necesarios para cumplir con sus responsabilidades.

24.5 Asegurar que existan mecanismos efectivos de control y de corresponder, asegurar controles eficaces sobre los modelos utilizados para identificar y cuantificar el riesgo de crédito.

24.6 Implementar un sistema de control de límites que asegure que las exposiciones a los riesgos se mantienen dentro de las políticas aprobadas por el Directorio. El sistema de límites debe incorporar parámetros que permitan controlar impactos adversos en el riesgo de crédito de la institución derivados de cambios en condiciones, hechos económicos, sociales y políticos.

24.7 Implementar un proceso de monitoreo periódico de la composición y calidad de las exposiciones del portafolio (considerando las operaciones dentro y fuera de balance) frente a los límites fijados y contar con procedimientos para incrementar el monitoreo y tomar medidas adecuadas si las exposiciones se acercan a los límites.

24.8 Implementar procesos adecuados que permitan la pronta identificación y gestión de créditos con problemas potenciales y efectivamente problemáticos así como el seguimiento y gestión de recupero de operaciones vencidas.

24.9 Asegurar que exista un proceso adecuado de evaluación y aprobación de nuevos productos, asegurando que se cuenta con procedimientos y controles suficientes antes de la entrada en vigencia de los mismos. Asegurar que en el proceso de creación de nuevos productos se considera el riesgo de crédito en forma explícita

24.10 Definir un sistema de clasificación de créditos y asegurar que las previsiones son adecuadas en relación al nivel de riesgos asumidos

24.11 Definir procedimientos y criterios claros sobre la aceptación y valuación de garantías

24.12 Evaluar los resultados de las pruebas de tensión periódicamente y tomar acciones oportunas y adecuadas cuando los resultados son superiores a las tolerancias definidas.

24.13 Revisar periódicamente las políticas y procedimientos para asegurar que siguen siendo adecuados y prudentes.

24.14 Desarrollar un sistema de información que permita una oportuna y correcta agregación y notificación al Directorio de las exposiciones al riesgo de crédito así como que permita evaluar la efectividad de gestión del riesgo.

25. La Alta Gerencia debe asegurar que el otorgamiento de créditos se realiza en forma transparente sin estar sujetos a conflictos de interés. Particularmente, los créditos a compañías e individuos relacionados a la institución y al conglomerado financiero tienen que ser monitoreados en forma cercana.

Para ello la Alta Gerencia debe:

25.1 Establecer criterios que las operaciones con partes vinculadas se realicen con total imparcialidad y transparencia

25.2 Asegurar que los términos y condiciones de estos créditos no sean más favorables que el crédito otorgado a deudores no relacionados bajo circunstancias similares e imponiendo límites estrictos sobre estos créditos.

25.3 Asegurar que los criterios generales de la institución para otorgar crédito no deben ser modificados en función de las características de las operaciones o de las empresas y/o individuos relacionados.

25.4 Adoptar medidas adecuadas para monitorear, controlar o mitigar este tipo de créditos.

26. La institución debe establecer criterios prudentes y bien definidos para aprobar nuevas exposiciones al riesgo, así como para renovar, refinanciar, reestructurar y recuperar créditos. (Manual de créditos)

Para ello, la institución debe:

26.1 Contar con criterios bien definidos para aprobar, renovar, refinanciar y reestructurar créditos de una forma prudente y segura.

26.2 Incorporar en el proceso de aprobación de riesgos crediticios el caso de las inversiones en valores no líquidos.

26.3 Establecer pautas claras para manejar los riesgos derivados de la concesión de créditos en una moneda diferente a la de los ingresos principales del prestatario (descalce de monedas del deudor).

26.4 Definir criterios para evaluar la relación riesgo/retorno a nivel de cada operación, deudor y portafolio. Los precios y las condiciones de los créditos (garantías, restricciones, etc.) se deben fijar de forma que cubran todos los costos implícitos y compensen a la institución por los riesgos incurridos.

26.5 Definir criterios sobre la documentación necesaria para aprobar créditos nuevos, renovar, reestructurar o refinanciar créditos existentes y/o cambiar los términos y las condiciones de los créditos aprobados con anterioridad así como la gestión posterior de dicha información.

26.6 Disponer de la documentación adecuada que sustente la clasificación asignada y el nivel de previsiones del deudor.

26.7 Definir criterios y procedimientos de análisis de la capacidad de pago del deudor en función del riesgo a asumir. Según corresponda, se tendrá en cuenta como mínimo:

- El destino del crédito, fuente de repago y nivel de ingresos
- Integridad y reputación de la contraparte
- Capacidad legal del prestatario o contraparte
- Posición del deudor en la institución y en el sistema financiero
- Análisis de la experiencia de pago
- Conocimiento del negocio, del sector económico y de la situación económica financiera de la empresa,

- Análisis de la situación financiera y patrimonial actual, prospectiva y bajo condiciones de estrés

26.8 En caso de contar con sistemas de calificación cualitativos, tener definidos y documentados los criterios, parámetros y la metodología utilizada.

B - MEDICIÓN, CONTROL Y MONITOREO DEL RIESGO DE CRÉDITO

27. La institución debe contar con procesos adecuados para identificar, cuantificar, informar y controlar las concentraciones de riesgo en el momento oportuno.

Para ello la institución debe:

27.1 Fijar límites de concentraciones aceptables de riesgos de acuerdo a su apetito de riesgo y el perfil de riesgos. Estas concentraciones de crédito resultan de exposiciones frente a: contrapartes individuales o grupos de contrapartes conectadas tanto de forma directa como indirecta, contrapartes en la misma industria, sector económico o región geográfica y contrapartes cuyos resultados financieros dependen de la misma actividad o materia prima, así como de exposiciones fuera de balance.

27.2 Identificar situaciones en las que es apropiado clasificar un grupo de deudores como contrapartes relacionadas entre sí (conjunto económico) y por ende, como un solo riesgo.

27.3 Comunicar a la Alta Gerencia sobre los excesos en los límites de concentración establecidos.

27.4 Disponer de adecuados sistemas de información que le permita y gestionar en forma activa las posiciones de generadoras de concentraciones de riesgos y frente a contrapartes individuales o grupos de contrapartes relacionadas (conjuntos económicos).

28. La institución debe contar con procesos eficaces para la gestión del riesgo de crédito.

Para ello, la institución debe:

28.1 Cumplir con los procesos de aprobación y recupero de créditos de acuerdo con las pautas establecidas por la Dirección y Alta Gerencia.

28.2 Contar con mecanismos claros que documenten que se ha cumplido con el proceso de aprobación, evaluación y recupero y que identifican al (a los) individuo(s) y/o comité(s) que se han involucrado en las decisiones.

28.3 Cumplir con los criterios definidos respecto a la información del deudor y documentación del crédito.

29. La institución debe contar con un sistema de clasificación coherente con la naturaleza, el tamaño y la complejidad de las actividades de la institución.

29.1 El sistema de clasificación de riesgos debe:

- Segmentar la cartera de créditos en forma efectiva y consistente.
- Tomar en cuenta la situación financiera del deudor y su capacidad de pago, el tipo de exposición y/o garantías que podrían afectar las perspectivas de cobro de capital e intereses.
- Ser revisado y probado en forma periódica
- Permitir a la Alta Gerencia verificar las características actuales de la cartera de crédito
- Permitir identificar créditos donde existe deterioro potencial o actual y tomar acciones correctivas
- Ser aplicado en forma consistente a lo largo de la institución y de acuerdo con políticas y procedimientos establecidos.

29.2 En el caso de utilizar un sistema de calificación cuantitativo, la institución debe contar con un proceso documentado que incluya:

- La metodología estadística utilizada para definir y comprobar el sistema de scoring. Las condiciones de los productos (monto máximo, condiciones y plan de repago).
- Documentar los supuestos utilizados para las clasificaciones establecidas mediante modelos cuantitativos
- Controles que aseguren la veracidad de la información recabada sobre los solicitantes y el cumplimiento con los lineamientos de la aprobación.
- Procedimientos de revisión periódica de la metodología utilizada y de los resultados del modelo.

30. La institución debe definir procedimientos para asegurar que las previsiones constituidas a nivel individual y colectivo son suficientes para absorber las pérdidas crediticias esperadas y son consistentes con el nivel de riesgo de crédito asumido.

La institución debe:

30.1 Asegurar que las previsiones se reconocen contablemente en forma oportuna y reflejan expectativas realistas de reembolso y recuperación, teniendo en cuenta la situación del deudor, macroeconómica y de los mercados.

30.2 Asegurar que las previsiones toman en cuenta las posiciones fuera de balance.

30.3 De corresponder, contar con procedimientos de validación de los modelos utilizados en el cálculo de las pérdidas crediticias esperadas.

31. La institución debe tener un sistema para monitorear la condición de créditos individuales.

Para ello, la institución debe:

31.1 Proveer de información para monitorear la condición de créditos en las diferentes carteras de la institución.

31.2 Contar con medidas para:

- Actualizar la información sobre la condición financiera relevante del deudor, asegurando que se incluya la identificación de todas las fuentes de riesgo posibles.
- Asegurar que todos los créditos cumplen con los contratos existentes.
- Controlar el uso que los clientes hacen de las líneas de crédito aprobadas.
- Identificar problemas de repago.

31.3 Medir en forma regular el riesgo de descalce a nivel individual y determinar los controles y mitigantes de este riesgo.

31.4 Asegurar que la carpeta de crédito del deudor contenga toda la información necesaria para verificar la situación del deudor en forma permanente.

31.5 Valorar periódicamente y monitorear las coberturas de riesgo, incluidos avales, derivados crediticios y garantías.

31.6 Verificar la ejecutabilidad de las garantías durante la vigencia del crédito.

32. La institución debe tener procesos y procedimientos y sistemas de información adecuados para identificar, gestionar y monitorear administrar los créditos potencial o efectivamente problemáticos.

Para ello, la institución debe:

32.1 Realizar una pronta identificación de activos con problemas potenciales o efectivamente problemáticos.

32.2 Realizar una vigilancia continua de los activos problemáticos.

32.3 Definir responsables en la identificación temprana y resolución de problemas de créditos con problemas potenciales o problemáticos.

32.4 Contar con criterios claros y bien definidos para el pasaje de un crédito problemático o con problemas potenciales a un sector especializado de resolución.

32.5 Contar con procedimientos tendientes a maximizar la recuperación de créditos.

32.6 Contar con criterios de cobranza, reestructuración de operaciones y castigo de los créditos.

32.7 Contar con reportes para monitorear los créditos con síntomas de deterioro que sean revisados regularmente por la Alta Gerencia.

33. La institución debe tener un sistema para monitorear la composición y calidad general de la cartera de crédito.

Para ello, la institución debe:

33.1 Monitorear:

- la calidad y composición de la cartera de crédito incluidas las operaciones fuera de balance.
- las exposiciones en relación a los límites de concentración fijados y tomar medidas cuando se acerquen o superen los límites.
- el riesgo de descalce del portafolio en su conjunto
- las concentraciones de créditos directos o indirectos a:
    - Una sola contraparte:
    - Un grupo de contrapartes relacionadas.
    - Un sector industrial o económico particular.
    - Un país extranjero individual
    - Un producto de crédito.
    - Un tipo de garantía.
- la diversificación del portafolio en relación a los mercados objetivos y la estrategia de crédito de la institución.

33.2 Definir estrategias y alternativas para reducir o minimizar las concentraciones, tales como fijar precios para el riesgo adicional, exigir tenencias crecientes de capital para compensar los riesgos adicionales y utilizar participaciones en préstamos para reducir la dependencia de sectores específicos de la economía o grupos de deudores relacionados.

33.3 Definir procedimientos para identificar el riesgo de monedas, medirlo en forma regular y determinar los controles y mitigantes.

34. La institución debe evaluar la exposición al riesgo de crédito del portafolio teniendo en cuenta los cambios futuros posibles en las condiciones económicas y en condiciones de estrés.

Para ello debe:

34.1 Tener un sistema de pruebas de estrés para identificar posibles eventos o cambios en las condiciones económicas que podrían tener efectos adversos en las exposiciones de crédito de la institución y evaluar su capacidad para hacer frente a estos cambios.

34.2 Establecer escenarios acordes con su perfil de riesgo los cuales tendrán que captar fuentes de riesgo significativas.

34.3 Documentar los supuestos y la metodología utilizada para la elaboración de los diferentes escenarios de estrés.

34.4 Incluir planes de contingencia respecto al conjunto de acciones que la Alta Gerencia puede tomar en ciertas circunstancias.

34.5 Las pruebas de estrés deben ser oportunas e integradas a la gestión y ser realizadas con una periodicidad definida y comunicados sus resultados a los comités involucrados y al Directorio.

35. La institución debe 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.

Para ello, la institución debe:

35.1 Contar con mecanismos de control interno que aseguren que la gestión del riesgo de crédito se realiza de acuerdo con las políticas y procedimientos definidos por el Directorio y Alta Gerencia.

35.2 Establecer procedimientos de identificación, monitoreo, documentación y notificación de excepciones a las políticas y límites establecidos.

35.3 Asegurar que las posiciones que exceden niveles predefinidos reciban la atención de la Alta Gerencia en forma oportuna.

36. La institución debe contar con un sistema de información gerencial que suministre información adecuada sobre la composición de la cartera de crédito.

Para ello, el sistema debe:

36.1 Permitir al Directorio y a todos los niveles gerenciales cumplir con sus roles respectivos de supervisión, incluyendo la determinación del nivel de patrimonio adecuado que la institución debe mantener.

36.2 Proveer una visión sobre la composición y calidad de los distintos portafolios, incluyendo el consolidado, que permita a la Gerencia evaluar exactamente el nivel del riesgo de crédito derivado de las actividades de la institución y determinar si ésta se encuadra en la estrategia definida para el riesgo de crédito y las regulaciones vigentes.

36.3 Emitir reportes en forma regular, Incluir todas las exposiciones y medirlas contra los límites de riesgo establecidos.

36.4 Proveer información que permita a la Gerencia identificar concentraciones de riesgo en la cartera de crédito.

36.5 Informar sobre las excepciones en los límites del riesgo de crédito de manera oportuna y adecuada y proveer señales oportunas a la Alta Gerencia de las exposiciones que se están acercando a los límites de riesgo.

36.6 Permitir análisis adicionales de la cartera de crédito, incluyendo las pruebas de estrés.

C – REVISIÓN DEL SISTEMA

37. La institución debe establecer mecanismos de revisión independiente y periódica del proceso de gestión de créditos. Los resultados de las revisiones deben ser reportados directamente al Directorio y a la Alta Gerencia.

La revisión independiente debe incluir la evaluación de:

37.1 El sistema en su conjunto y su eficacia en el cumplimiento de los objetivos.

37.2 El cumplimiento efectivo de las políticas y procedimientos y la adecuada documentación de los procesos y las decisiones adoptadas.

37.3 La organización y la suficiencia de los recursos humanos en cuanto a número y competencia técnica para gestionar en forma correcta el riesgo.

37.4 El equilibrio existente entre las áreas comerciales y de control de riesgos.

37.5 El desempeño de los oficiales y el estado actual de la cartera de crédito.

37.6 La capacidad y eficacia del sistema para e capturar todos los elementos materiales de riesgo.

37.7 La exactitud de las clasificaciones de riesgo y de las previsiones constituidas.

37.8 La confiabilidad y corrección en el procesamiento, agregación y cotejo de los datos.

37.9 Los supuestos utilizados en la formulación de los modelos y si están correctamente documentados.

37.10 Los cambios significativos que puedan afectar la efectividad de los controles, como cambios en los mercados, recursos humanos, tecnología o estructuras de cumplimiento.

RIESGOS DE MERCADO

Los riesgos de mercado son aquellos por los cuales el valor de las posiciones dentro y fuera de balance 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 de la institución financiera. A estos efectos se identifican como riesgos de mercado:

- **Riesgo de tasa de interés**
- **Riesgo de tipo de cambio**
- **Riesgo de reajuste**
- **Otros riesgos de mercado**

a) RIESGO DE TASA DE INTERES

El **riesgo tasa de interés** está integrado por los siguientes riesgos:

- **Riesgo de tasa de interés de la Cartera de Valores** – Es el riesgo asociado a las eventuales pérdidas en el valor de mercado de la cartera de Valores originadas por movimientos adversos en las tasas de interés.

  Este riesgo tiene dos componentes:

- Riesgo Específico: Deriva de movimientos adversos en el valor de mercado dela cartera de valores originados en factores relacionados con los emisores de los instrumentos.
- Riesgo General: Proviene de movimientos adversos de precios originados por variaciones en las tasas de interés de mercado libres de riesgo. Este riesgo general tiene, a su vez, tres componentes básicos: el riesgo direccional, que mide la sensibilidad del precio de cada una de las posiciones, el riesgo de base, que contempla posibles compensaciones provenientes de posiciones con signos opuestos en una misma banda temporal y el riesgo de movimientos no paralelos en la curva, que mide las posibles compensaciones entre posiciones situadas con distintos horizontes temporales.

- **Riesgo de tasa de interés estructural** – Este riesgo abarca a todo el balance del banco, incluyendo las posiciones fuera de balance. Es el riesgo potencial de que los resultados (perspectiva contable) o el patrimonio de la entidad (perspectiva económica) se vean afectados como consecuencia de movimientos en las tasas de interés. Este riesgo surge por la diferencia que existe entre el momento en que se recalculan las tasas activas y las pasivas de la entidad. También en este caso, se pueden distinguir tres componentes: el riesgo direccional, el riesgo de base y el riesgo de movimientos no paralelos en la curva de tasas de interés.

b) RIESGO DE TIPO DE CAMBIO

El riesgo tipo de cambio se define como la posibilidad de que los resultados o el ratio de capital sobre activos se vea adversamente afectado por movimientos desfavorables en las tasas de cambio entre divisas para posiciones dentro y fuera de balance.

c) RIESGO DE REAJUSTE

El riesgo de reajuste es el riesgo de que el patrimonio se vea adversamente afectado por movimientos en los tipos de cambio de las unidades de cuenta en moneda nacional en un horizonte de largo plazo.

d) OTROS RIESGOS DE MERCADO

Los otros riesgos de mercado se definen como la posibilidad de que el patrimonio se vea afectado por movimientos adversos en el precio de acciones y/o precio de mercancías.

A - MARCO DE RIESGOS, POLÍTICAS Y PROCEDIMIENTOS

38. El Directorio debe aprobar la estrategia y las políticas para la gestión de los riesgos de mercado en base individual y consolidada y revisarlas periódicamente. La estrategia debe reflejar el apetito de riesgo, el perfil de riesgos de la institución y entidades controladas y la situación macroeconómica y de los mercados.
El Directorio debe revisar regularmente las exposiciones a los distintos riesgos de mercado y asegurar que los niveles de riesgos se encuentran dentro del marco establecido.

Para ello el Directorio debe:

38.1 Aprobar la estrategia y las políticas de gestión del riesgo de mercado y revisarlas periódicamente. Estas políticas deben ser consistentes con el apetito de riesgo definido y deben ser aplicadas en forma consolidada y a nivel de las entidades individuales cuando corresponda.

Las mismas deben:

- Incluir tipos, niveles y límites de riesgos aceptables acordes con el apetito de riesgo y perfil de riesgo de la institución.
- Prever mecanismos de identificación y notificación de excepciones a las mismas.

38.2 Revisar la estrategia, políticas y apetito al riesgo en función de los resultados de las pruebas de tensión y sus mediciones de riesgos.

38.3 Evaluar periódicamente las políticas de riesgos de mercado y el impacto de las estrategias comerciales sobre los riesgos asumidos.

38.4 Asegurar que la institución cuenta con una estructura organizacional adecuada para la gestión del riesgo de mercado.

38.5 Promover que exista un equilibrio razonable entre las áreas comerciales y de riesgos. Esta última debe disponer de recursos suficientes, independencia, autoridad y acceso al Directorio de forma de poder desempeñar eficazmente sus tareas.

38.6 Identificar líneas de responsabilidad y autoridad en la gestión del riesgo de mercado.

38.7 Contar con información suficiente, detallada y oportuna sobre los riesgos de mercado, de forma que permita comprender los riesgos asumidos y evaluar el desempeño de la Alta Gerencia en el monitoreo y control de dichos riesgos.

38.8 Asegurar la realización de revisiones independientes para que en forma periódica se validen los procesos, las políticas, los procedimientos. Asegurar que se instrumenten las acciones apropiadas ante las debilidades o fallas significativas detectadas por el auditor interno, externo, supervisor o profesional independiente.

38.9 Asegurar que la Alta Gerencia implemente las políticas y procesos necesarios para que los riesgos asumidos sean consistentes con las estrategias y políticas aprobadas.

39. La Alta Gerencia debe implementar la estrategia y las políticas aprobadas por el Directorio para la gestión del riesgo de mercado y desarrollar procedimientos para su identificación, medición, monitoreo y control.

Para ello, la Alta Gerencia debe:

39.1 Implementar las políticas y desarrollar procedimientos para gestionar los riesgos de mercado en el corto, mediano y largo plazo de forma consistente con la estrategia y las políticas definidas.

39.2 Asignar claramente las funciones, responsabilidades y atribuciones en materia de identificación, aprobación, medición y control del riesgo de mercado.

39.3 Asignar los recursos necesarios en cantidad, calidad y competencia a efectos de un buen manejo del riesgo de mercado.

39.4 Asegurar que existan mecanismos efectivos de control y de corresponder, asegurar controles eficaces sobre los modelos utilizados para identificar y cuantificar los riesgos de mercado.

39.5 Implementar un sistema de límites que asegure que las exposiciones a los riesgos se mantienen dentro de las políticas aprobadas por el Directorio.

39.6 Implementar un sistema para asegurar la medición correcta de los riesgos.

39.7 Definir una metodología para valuar posiciones y medir el desempeño.

39.8 Asegurar que en el proceso de creación de nuevos productos se considera el riesgo mercado en forma explícita

39.9 Revisar periódicamente las políticas y procedimientos para asegurar que siguen siendo adecuados y prudentes.

39.10 Desarrollar un sistema de información que permita una oportuna y correcta agregación y notificación al Directorio de las exposiciones al riesgo de mercado así como que permita evaluar la efectividad de gestión del riesgo.

40. La Alta Gerencia debe asegurar que hay una adecuada separación de responsabilidades entre las áreas clave del proceso de gestión de riesgos para evitar potenciales conflictos de interés.

Para ello, la Alta Gerencia debe:

40.1 Definir claramente los responsables del desarrollo de estrategias, tácticas, medición y reportes de los riesgos de mercado.

40.2 Asegurar que existe un responsable de la administración de los riesgos financieros en forma integral, con la formación y experiencia suficiente de acuerdo a la complejidad y naturaleza de las operaciones.

40.3 Asegurar que existen suficientes resguardos para minimizar la influencia inadecuada de los que asumen posiciones de riesgos sobre las funciones de control, elaboración de reportes u otras áreas administrativas.

B - MEDICIÓN, CONTROL Y MONITOREO DEL RIESGO DE MERCADO

41. La institución debe tener un sistema de medición de riesgo de mercado que capture toda fuente material de riesgo tasa de interés, tipo de cambio, reajuste y otros riesgos de mercado 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.

El sistema debe:

41.1 Incorporar las exposiciones que provienen de todas las actividades de la institución.

41.2 Evaluar el impacto de los cambios en los resultados, el valor económico y el ratio de capital/activos.

41.3 Identificar excesos en límites establecidos.

41.4 Asegurar que los supuestos están claramente documentados y que pueden ser comprendidos por la Alta Gerencia. Dichos supuestos deben ser revisados por lo menos anualmente.

41.5 Prestar especial atención en las siguientes áreas:

- Instrumentos complejos o con vencimientos inciertos.
- Posiciones cuyo comportamiento difiere del vencimiento contractual.
- Posiciones denominadas en diferentes monedas.

41.6 Utilizar conceptos financieros y técnicas de medición de riesgos de mercado generalmente aceptados.

En particular, el sistema de medición de riesgo tipo de cambio debe considerar no solamente el impacto de las variaciones en las tasas de cambio entre divisas sobre las utilidades de la institución, sino también sobre el ratio de capital/activos. Es decir, debe considerarse la probabilidad de que, ante movimientos de las tasas de cambio entre divisas, los mayores/menores requerimientos de capital en moneda nacional necesarios para mantener el ratio capital/activos constante, no se compensen con las ganancias/pérdidas por diferencias de cambio medidas en moneda nacional, generadas por las posiciones en divisas dentro y fuera de balance.

Por su parte, el sistema de medición de riesgo tasa de interés debe:

41.7 Incluir todas las fuentes materiales de riesgo incluyendo los riesgos de:

- cambios en los valores de las tasas al vencimiento de las operaciones.
- los cambios en la relación de tasas entre diferentes curvas de interés (riesgo base).
- los cambios en la relación entre las tasas a lo largo de los diferentes vencimientos dentro de la curva (cambios no paralelos).
- la concentración de posiciones.
- Instrumentos con opciones implícitas o explicitas..

41.8 Tener un grado de detalle y complejidad que sea consistente con la complejidad y nivel de riesgo asumido.

42. La institución debe medir su vulnerabilidad a pérdidas bajo condiciones de estrés y considerar dichos resultados cuando se defina o se revise el apetito de riesgo.

Para ello, el sistema de medición en condiciones de estrés debe:

42.1 Proveer información sobre las condiciones bajo las cuales las estrategias o posiciones son más vulnerables.

42.2 Establecer escenarios en base a diversas técnicas disponibles como ser: análisis de sensibilidad, o de variación de varios parámetros simultáneamente, ya sea histórico o hipotético, considerando sus interrelaciones.

42.3 Las pruebas de estrés deben ser oportunas e integradas a la gestión. Realizadas con una periodicidad definida y comunicados sus resultados a los comités involucrados y al Directorio.

43. La institución debe tener un sistema adecuado para el monitoreo y control de los riesgos de mercado.

43.1 Para ello el sistema de monitoreo y control debe:

- Controlar los límites y métricas aprobadas
- Incluir procedimientos y metodologías de control claramente establecidas y definidas.
- Capturar todos los elementos materiales de riesgo de mercado dentro y fuera del balance.

Asimismo se deberá:

43.2 Evaluar los supuestos utilizados y revisar si están adecuadamente documentados.

43.3 Verificar que los datos utilizados son procesados correctamente y la agregación de los datos es correcta y confiable.

43.4 Asegurar que las posiciones que exceden los niveles predefinidos reciben la atención de la Alta Gerencia en forma oportuna. Las excepciones a los límites deben ser reportadas rápidamente a la Alta Gerencia.

44. La institución debe 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.

Para ello, la institución debe:

44.1 Contar con mecanismos de control interno que aseguren que la gestión del riesgo de mercado se realiza de acuerdo con las políticas y procedimientos definidos por el Directorio y Alta Gerencia.

44.2 Establecer procedimientos de identificación, monitoreo, documentación y notificación de excepciones a las políticas y límites establecidos.

44.3 Asegurar que las posiciones que exceden niveles predefinidos reciban la atención de la Alta Gerencia en forma oportuna.

45. La institución debe contar con un sistema de información gerencial que suministre información adecuada y oportuna sobre las exposiciones a los riesgos de mercado al Directorio y la Alta Gerencia y los Gerentes de línea.

Un sistema informativo, fiel y oportuno es esencial para gestionar las exposiciones de riesgos de mercado y asegurar el cumplimiento con las políticas establecidas por el Directorio.

Para ello, el sistema debe:

45.1 Emitir reportes en forma regular y comparar las exposiciones con los límites establecidos.

45.2 Incluir una comparación de las proyecciones con los resultados reales para permitir la identificación de limitaciones o errores en los modelos.

45.3 Incluir como mínimo un resumen de las exposiciones agregadas con:

- el cumplimiento con las distintas políticas y los límites aprobados.
- los supuestos clave incluyendo el comportamiento de depósitos sin vencimiento establecido y prepago.
- los resultados de las pruebas de estrés, incluyendo las fallas en los supuestos y los parámetros clave.
- un resumen de los hallazgos de revisiones internas y externas de políticas, procedimientos y sistemas.

C – REVISIÓN DEL SISTEMA

46. La institución debe establecer mecanismos de revisión independiente y periódica del proceso de gestión del riesgo de mercado. Los resultados de las revisiones deben ser reportados directamente al Directorio y a la Alta Gerencia.

La revisión independiente debe incluir la evaluación de:

46.1 El sistema en su conjunto y su eficacia en el cumplimiento de los objetivos.

46.2 El cumplimiento efectivo de las políticas y procedimientos y la adecuada documentación de los procesos y las decisiones adoptadas.

46.3 La organización y la suficiencia de los recursos humanos en cuanto a número y competencia técnica para gestionar en forma correcta el riesgo.

46.4 El equilibrio existente entre las áreas comerciales y de control de riesgos.

46.5 La capacidad y eficacia del sistema para capturar todos los elementos materiales de riesgo.

46.6 La confiabilidad y corrección en el procesamiento, agregación y cotejo de los datos.

46.7 Los supuestos utilizados en la formulación de los modelos y si están correctamente documentados.

46.8 Los cambios significativos que puedan afectar la efectividad de los controles, como cambios en los mercados, recursos humanos, tecnología o estructuras de cumplimiento.

RIESGO DE LIQUIDEZ

El **riesgo de liquidez** depende de dos dimensiones definidas como el riesgo de liquidez de fondeo (Pasiva) y el riesgo de liquidez de mercado (Activa) y de la correlación existente entre las mismas.

- **Riesgo de liquidez de fondeo** - Incluye la incapacidad de la institución de gestionar bajas o cambios inesperados en las fuentes de financiamiento tanto locales como internacionales. A menudo esto puede causar la liquidación prematura de parte de sus activos.
- **Riesgo de liquidez de mercado** - Proviene de las dificultades derivadas de los cambios en las condiciones de mercado que afecten la rápida liquidación de los activos con una mínima pérdida de valor.

A - MARCO DE RIESGOS, POLÍTICAS Y PROCEDIMIENTOS

47. El Directorio debe aprobar la estrategia y las políticas para la gestión del riesgo de liquidez de la institución en base individual y consolidada y revisarlas periódicamente. La estrategia debe reflejar el apetito de riesgo, el perfil de riesgos de la institución y entidades controladas y la situación macroeconómica y de los mercados. El Directorio debe revisar regularmente las exposiciones a los distintos riesgos de liquidez y asegurar que los niveles de riesgos se encuentran dentro del marco establecido.

Para ello, el Directorio debe:

47.1 Aprobar la estrategia y las políticas de gestión del riesgo de liquidez y revisarlas periódicamente a la luz de la experiencia y de las tendencias de liquidez de la empresa y del mercado. Estas políticas deben ser consistentes con el apetito de riesgo definido y deben ser aplicadas en forma consolidada y a nivel de las entidades individuales cuando corresponda.

Las mismas deben:

- Incluir límites a las exposiciones al riesgo de liquidez.
- Prever mecanismos de identificación y notificación de excepciones a las mismas.

47.2 Revisar la estrategia, políticas y el apetito al riesgo en función de los resultados de las pruebas de tensión

47.3 Aprobar y revisar los planes de contingencia para enfrentar eventuales problemas de liquidez.

47.4 Monitorear la relación de rentabilidad y riesgo de liquidez de la Institución.

47.5 Asegurar que la institución cuenta con una estructura organizacional adecuada para la gestión del riesgo de liquidez.

47.6 Identificar líneas de responsabilidad y autoridad en la gestión del riesgo de liquidez.

47.7 Promover que exista un equilibrio razonable entre las áreas comerciales y de riesgos. Esta última debe disponer de recursos suficientes, independencia, autoridad y acceso al Directorio de forma de poder desempeñar eficazmente sus tareas.

47.8 Contar con información suficiente, detallada y oportuna sobre el riesgo de liquidez de forma que permita comprender los riesgos asumidos y evaluar el desempeño de la Alta Gerencia en el monitoreo y control de dicho riesgo.

47.9 Asegurar la realización de revisiones independientes para que en forma periódica se validen los procesos, las políticas, los procedimientos. Asegurar que se instrumenten las acciones apropiadas ante las debilidades o fallas significativas detectadas por el auditor interno, externo, supervisor o profesional independiente.

47.10 Asegurar que la Alta Gerencia implemente las políticas y los procedimientos necesarios para que los riesgos asumidos sean consistentes con las estrategias y políticas aprobadas.

48. La Alta Gerencia debe implementar la estrategia y las políticas aprobadas por Directorio para la gestión del riesgo de la liquidez y desarrollar procedimientos para su identificación, medición, monitoreo y control.

Para ello, la Alta Gerencia debe:

48.1 Implementar las políticas y Desarrollar procedimientos específicos para la gestión de liquidez que incluyan lineamientos sobre la composición de activos y pasivos, la administración de liquidez en diferentes monedas, de los activos y pasivos radicados en diferentes países y el uso de los distintos instrumentos financieros.

48.2 Definir los responsables de la administración del riesgo de liquidez y el mecanismo a través del cual se implementa la política de liquidez y se revisan las decisiones tomadas sobre la posición de liquidez.

48.3 Asignar los recursos necesarios en cantidad, calidad y competencia a efectos de un buen manejo del riesgo de liquidez.

48.4 Asegurar que existan mecanismos efectivos de control y de corresponder, asegurar controles eficaces sobre los modelos utilizados para identificar y cuantificar el riesgo de liquidez.

48.5 Implementar un sistema de límites que asegure que la liquidez se mantiene dentro de las políticas aprobadas por el Directorio.

48.6 Desarrollar procedimientos para la gestión de riesgos de liquidez que incluya la medición de costos, beneficios y riesgos de liquidez en los procesos de formación interna de precios, medición de resultados y aprobación de nuevos productos.

48.7 Desarrollar procedimientos de control que expliciten los procesos de aprobación, límites, revisiones y otros mecanismos apropiados designados para proporcionar una seguridad razonable de que se logren los objetivos del manejo del riesgo de liquidez de la institución.

48.8 Evaluar cómo otros riesgos, incluyendo los riesgos de crédito, de mercado y de operación, pueden impactar sobre la estrategia global de liquidez de la institución.

48.9 Asegurar que en el proceso de creación de nuevos productos se considera el riesgo de liquidez en forma explícita.

48.10 Implementar un proceso continuo de evaluación sobre el posible impacto de diferentes escenarios sobre su posición de liquidez.

48.11 Revisar periódicamente las políticas y procedimientos para asegurar que siguen siendo adecuados y prudentes.

48.12 Desarrollar e implementar el Plan de Contingencia de Liquidez aprobado por el Directorio.

48.13 Desarrollar planes para enfrentar la potencial falta de liquidez tanto transitoria como a largo plazo.

48.14 Desarrollar un sistema de información que permita una oportuna y correcta agregación y notificación al Directorio de las exposiciones al riesgo de liquidez, así como que permita evaluar la efectividad de gestión del riesgo.

B - MEDICIÓN, CONTROL Y MONITOREO DEL RIESGO DE LIQUIDEZ

49. La institución debe establecer un sistema de medición y monitoreo continuo de los requerimientos netos de fondos, considerando sus posiciones de liquidez en las principales monedas con las que trabaja.

Para ello el sistema debe:

49.1 Tener la capacidad de calcular las posiciones de liquidez en plazos cortos y en distintos periodos específicos (incluyendo períodos más lejanos en el tiempo, por moneda y en forma agregada Las posiciones de liquidez deberán ser calculadas en una situación estática y/o dinámica.

49.2 Ser lo suficientemente flexible como para enfrentar variadas contingencias que puedan surgir.

49.3 Contar con un sistema de información que le permita comparar los ingresos y egresos de efectivo en forma diaria o para distintos periodos especificados y. los niveles de activos líquidos.

49.4 Incorporar el monitoreo de factores externos (tendencias económicas, de mercado e información específica sobre la propia institución) con el objetivo de evaluar su potencial impacto sobre la liquidez.

49.5 Analizar las condiciones de mercado que podrían afectar el acceso al mercado de moneda extranjera y saber que los depositantes y prestatarios de moneda extranjera podrían intentar retirar sus fondos más rápidamente que las contrapartes locales.

49.6 Evaluar su acceso a fuentes alternativas de fondos para el reembolso de obligaciones en moneda extranjera.

49.7 Considerar que podrían haber dificultades de acceso a ciertos mercados y que los mercados de divisas podrían carecer de liquidez y/o el tipo de cambio podría depreciarse drásticamente.

50. La institución debe analizar la liquidez utilizando distintos escenarios, llevar a cabo pruebas de estrés y revisar frecuentemente la validez de los supuestos utilizados para administrar la liquidez.

Dado que muchos pasivos y activos no tienen vencimientos definidos, la institución debe:

50.1 Implementar un proceso de evaluación de la experiencia histórica de la institución sobre patrones de comportamiento de los flujos.

50.2 Evaluar en forma periódica el comportamiento de los flujos de efectivo en distintos escenarios, a partir de cambios en los supuestos utilizados. Al hacer una evaluación, la institución debe tomar en cuenta no sólo su propia experiencia histórica, sino también la experiencia de otras entidades en una crisis de liquidez.

50.3 Realizar pruebas de estrés en base a distintos supuestos. Debe considerarse escenarios de crisis idiosincrática y sistémica. En la medida que la posición de liquidez futura puede verse afectada por factores que no siempre pueden ser pronosticados con precisión, los supuestos deben revisarse frecuentemente para determinar su validez, especialmente dada la velocidad de cambio en los mercados financieros

50.4 Los escenarios deben considerar del lado del activo la incapacidad de recuperar las colocaciones y del lado del pasivo un retiro significativo de depósitos de no residentes

50.5 Las pruebas de estrés deben ser oportunas e integradas a la gestión; realizadas con una periodicidad definida y comunicados sus resultados a los comités involucrados y al Directorio.

51. La institución debe revisar regularmente las estrategias de financiación y el nivel de liquidez de los activos.

Para ello, la institución debe:

51.1 Revisar el nivel de activos líquidos de alta calidad y libre de cargas que puedan ser utilizados en periodos de tensión

51.2 Evaluar a intervalos regulares la capacidad para vender activos

51.3 Revisar el perfil de financiación estable en relación con la composición de sus activos y actividades fuera de balance.

51.4 Evaluar periódicamente las opciones disponibles de fondeo, las posibilidades de acceso a las mismas y el monto de fondos que puede esperar recibir del mercado, tanto en circunstancias normales como adversas.

51.5 Evaluar la composición, características y nivel de concentración de sus fuentes de fondos. Se debe considerar en el análisis el financiamiento mayorista.

51.6 Monitorear las variadas opciones de provisión de fondos y sus tendencias actuales.

51.7 Definir e implementar una estrategia de relacionamiento y comunicación con los proveedores clave de fondos para proporcionar una línea de defensa ante un problema de liquidez y formar parte integral de la administración de liquidez de la entidad.

52. La institución debe establecer planes de contingencia que respalden la estrategia para manejar crisis de liquidez e incluir procedimientos.

El plan de contingencia debe:

52.1 Estar adecuadamente documentado

52.2 Contener políticas que permitan gestionar situaciones de tensión (idiosincráticas y sistémicas) establecer líneas de responsabilidad claras e incluir procedimientos de activación y refuerzo del plan. Asimismo deberá someterse a actualizaciones y revisiones periódicos a fin de garantizar que su operativa es robusta

52.3 Incluir procedimientos que estén estrechamente conectados con el continuo proceso de análisis del riesgo de liquidez de la institución y con los resultados de los escenarios y supuestos utilizados en las pruebas de tensión.

52.4 Establecer procedimientos que aseguren que los flujos de información son oportunos e ininterrumpidos y que proporcionan a la Gerencia la información precisa para tomar decisiones rápidas.

52.5 Establecer una clara asignación de responsabilidades de manera que todo el personal conozca lo que se espera de él durante una situación problemática.

52.6 Incluir las acciones a tomar en el caso de enfrentarse con un problema de liquidez incluyendo:

- planes de comunicación claros dirigidos a todos los agentes internos y externos
- considerar los efectos de las tensiones en los mercados sobre su capacidad para vender o titulizar activos;
- la relación entre la liquidez de mercado y la liquidez de fondeo
- efectos de reputación relacionados con la adopción de las medidas de financiación contingente

52.7 Incluir procedimientos para compensar déficits de flujo de efectivo en situaciones adversas. La institución debe tener disponibles varias fuentes posibles de fondos, incluyendo facilidades de crédito no usadas anteriormente. El plan debe establecer tan claramente como sea posible la cantidad de fondos de estas fuentes que la institución tendría a disposición y bajo qué situaciones podría usarlos.

53. La institución debe definir mecanismos de control que aseguren el cumplimiento de los límites de descalce de su flujo de efectivo vigentes y contar con un proceso adecuado para la identificación y tratamiento de las excepciones.

Para ello, la institución debe:

53.1 Contar con mecanismos de control interno que aseguren que el manejo del riesgo de liquidez se realiza de acuerdo con las políticas y procedimientos definidos por el Directorio y Alta Gerencia.

53.2 Establecer procedimientos de identificación, monitoreo documentación y notificación de excepciones a las políticas y límites establecidos.

53.3 Asegurar que las posiciones que exceden niveles predefinidos reciban la atención de la Alta Gerencia en forma oportuna.

54. La institución debe contar con un sistema de información gerencial que suministre información adecuada y oportuna adecuada para monitorear, controlar e informar el riesgo de liquidez. Los informes deben entregarse periódicamente al Directorio y Alta Gerencia.

Para ello, el sistema debe:

54.1 Emitir información en forma regular que permita el control de exposiciones al riesgo de liquidez actuales en relación a los límites establecidos

54.2 Permitir una evaluación del nivel y de las tendencias en la exposición agregada al riesgo de liquidez de la Institución.

54.3 Utilizar supuestos claramente explicitados para que la Gerencia pueda evaluar la validez y consistencia de los supuestos clave y conocer las implicaciones de las distintas situaciones planteadas en las pruebas de estrés.

C – REVISIÓN DEL SISTEMA

55. La institución debe establecer mecanismos de revisión independiente y periódica del proceso de gestión de la liquidez. Los resultados de las revisiones deben ser reportados directamente al Directorio y a la Alta Gerencia.

La revisión independiente debe incluir la evaluación de:

55.1 El sistema en su conjunto y su eficacia en el cumplimiento de los objetivos.

55.2 El cumplimiento efectivo de las políticas y procedimientos y la adecuada documentación de los procesos y las decisiones adoptadas.

55.3 La organización y la suficiencia de los recursos humanos en cuanto a número y competencia técnica para gestionar en forma correcta el riesgo.

55.4 El equilibrio existente entre las áreas comerciales y de control de riesgos.

55.5 La capacidad y eficacia del sistema para capturar todos los elementos materiales de riesgo.

55.6 La confiabilidad y corrección en el procesamiento, agregación y cotejo de los datos.

55.7 Los supuestos utilizados en la formulación de los modelos y si están correctamente documentados.

55.8 Los cambios significativos que puedan afectar la efectividad de los controles, como cambios en los mercados, recursos humanos, tecnología o estructuras de cumplimiento.

RIESGO OPERACIONAL

El riesgo operacional se define como el riesgo presente y futuro de que las ganancias o el patrimonio de la entidad se vean afectados por pérdidas resultantes de procesos, personal 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. Este riesgo también aparece en situaciones en donde las leyes o regulaciones que rigen ciertos productos o actividades son ambiguas.

El riesgo operacional acompaña el desarrollo y evolución de los productos, el desarrollo e implementación de los sistemas, los procesos transaccionales y guarda relación con la complejidad de los productos y servicios, 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 se asume riesgo operacional con el objetivo de obtener un retorno, sino que surge de la actividad normal de la entidad y afecta el manejo integral de riesgos.
La entidad puede tener su propia definición del riesgo operacional, pero cualquiera sea ésta, es crítico que exista una comprensión del concepto por parte de la entidad para su manejo efectivo.

Cada entidad puede tener una forma de organización diferente para esta función debe estar de acuerdo con su tamaño, complejidad y líneas de negocio. Sin perjuicio de ello, la institución debe asignar los recursos necesarios, definir claramente responsabilidades, tener independencia operativa para el ejercicio de la función y estar sujeta a revisiones periódicas por parte de la Auditoría Interna.

56. El Directorio debe aprobar los principios generales para el manejo del riesgo operacional, el apetito de riesgo y las políticas de la institución en base individual y consolidada y revisarlos periódicamente. Asimismo, debe revisar regularmente la exposición al riesgo operacional y asegurar que los niveles de riesgos se encuentran dentro del marco establecido.

Para ello, el Directorio debe:

56.1 Aprobar las políticas en relación al riesgo operacional y revisarlas periódicamente. Estas políticas deben ser consistentes con el apetito de riesgo definido.

Las mismas deben:

- Reconocer el riesgo operacional, (el cual incluye el riesgo de cumplimiento) como un riesgo que la entidad debe manejar explícitamente.
- Constituir una guía clara en relación al control de este riesgo y asegurar que todo el personal está comprometido con dichas actividades de control.
- Asegurar que todo el personal está comprometido con dichas actividades de control.

56.2 Promover una cultura de control adecuada en la organización y el cumplimiento de las leyes, regulaciones, prácticas de la industria y estándares éticos.

56.3 Asegurar que la gestión del riesgo operacional se lleva a cabo en forma continua.

56.4 Revisar periódicamente la efectividad de la gestión del riesgo operacional.

56.5 Asegurar que se cuenta con una estructura organizacional adecuada para la gestión del riesgo operacional.

56.6 Identificar líneas de responsabilidad y autoridad en la gestión del riesgo operacional.

56.7 Aprobar las políticas en relación a seguridad de la información y revisar periódicamente la efectividad de su implementación.

Las mismas deben:

- Reconocer explícitamente los riesgos vinculados a la gestión de activos de información y la necesidad de que su gestión sea consistente con la naturaleza y el nivel de complejidad de las operaciones.
- Constituir una guía clara en relación a la gestión de seguridad de la información.
- Promover una adecuada cultura de seguridad de la información.

56.8 Contar con información suficiente, detallada y oportuna sobre el riesgo operacional de forma que le permita comprender los riesgos asumidos y evaluar el desempeño de la Alta Gerencia en el monitoreo y control de dicho riesgo.

56.9 Asegurar la realización de revisiones independientes para que en forma periódica se validen los procesos, las políticas, los procedimientos. Asegurar que se instrumenten las acciones apropiadas ante las debilidades o fallas significativas detectadas por el auditor interno, externo, supervisor o profesional independiente.

56.10 Asegurar que la Alta Gerencia implemente las políticas y los procesos necesarios para que los riesgos asumidos sean consistentes con las políticas aprobadas.

57. La Alta Gerencia debe implementar las políticas aprobadas por el Directorio y desarrollar procedimientos apropiados para la identificación, medición, monitoreo y control del riesgo operacional Estas políticas y procedimientos deben considerar el riesgo operacional en todas las actividades de la institución.

Para ello, la Alta Gerencia debe:

57.1 Implementar las políticas y desarrollar procedimientos para gestionar el riesgo operacional, de forma consistente con las políticas definidas.

57.2 Asignar responsabilidades en forma explícita para el manejo del riesgo operacional, independientemente de la estructura organizacional que se defina. En particular, se asignan y definen roles y responsabilidades sobre la seguridad de la información.

57.3 Se asignan los recursos necesarios en cantidad, calidad y competencia a efectos de un buen manejo del riesgo operacional.

57.4 Identificar adecuadamente las fuentes potenciales de riesgo operacional y en consecuencia establecer mecanismos que mitigan este riesgo.

57.5 Establecer que la función de seguridad de la información debe ser independiente funcional y presupuestalmente del área de TI.

57.6 Asegurar que en el proceso de creación de nuevos productos o en la revisión de procesos, se considera el riesgo operacional en forma explícita.

57.7 Revisar periódicamente las políticas y procedimientos para asegurar que siguen siendo adecuados y prudentes.

57.8 Desarrollar un sistema de información que permita una oportuna y correcta agregación y notificación al Directorio del riesgo operacional así como que permita evaluar la efectividad de gestión del riesgo.

58. La Alta Gerencia debe implementar las políticas y desarrollar procedimientos apropiados para la identificación, medición, monitoreo y control del riesgo de cumplimiento y reportar al Directorio sobre el manejo de este riesgo.

Para ello, la Alta Gerencia debe:

58.1 Asignar responsabilidades en forma explícita para el manejo del riesgo de cumplimiento, independientemente de la estructura organizacional que se defina.

58.2 Identificar adecuadamente las fuentes potenciales de riesgo de cumplimiento, y en consecuencia establecer mecanismos que mitigan este riesgo.

58.3 Asegurar que el Directorio reciba en forma periódica información sobre la efectividad de la función de cumplimiento y en particular, cualquier aspecto que represente un riesgo de cumplimiento significativo.

58.4 Asegurar que exista un proceso que asegure el cumplimiento con las leyes y las regulaciones bancocentralistas.

58.5 Revisar periódicamente las políticas y procedimientos para asegurar que siguen siendo adecuados y prudentes.

58.6 Desarrollar un sistema de información que permita una oportuna y correcta agregación y notificación al Directorio del riesgo operacional así como que permita evaluar la efectividad de gestión del riesgo.

B - MEDICIÓN, CONTROL Y MONITOREO DEL RIESGO OPERACIONAL

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

Para ello, la institución debe:

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

59.2 Establecer algún mecanismo de auto evaluación de riesgos a nivel de los distintos procesos operativos de la entidad y definir los controles orientados a mitigar dichos riesgos.

59.3 Involucrar al personal vinculado a los distintos procesos en este mecanismo de auto evaluación.

59.4 Llevar un registro de los eventos de riesgo operacional que permita su consolidación y análisis.

59.5 Llevar un registro de las incidencias generadas en el proceso de atención a los clientes.

59.6 Generar un sistema de indicadores que alerten sobre debilidades en los procesos.

59.7 Contar con procedimientos que permitan asegurar el cumplimiento con las leyes, normas e instrucciones emitidas por entes reguladores.

59.8 Informar los resultados de las distintas herramientas de gestión de riesgo operacional al Comité de Riesgos, a la Auditoría Interna y al Comité de Auditoría y comunicarlas al personal involucrado.

60. La institución debe implementar procedimientos de control y monitoreo del riesgo operacional.

Para ello la institución debe:

60.1 Asegurar que exista un estrecho contacto entre las estructuras de control, y se intercambie información sobre el resultado de las actuaciones de cada una de ellas.

60.2 Asegurar que los procesos (o partes de ellos) que se encuentren tercerizados están adecuadamente controlados.

60.3 Asegurar que existan reportes periódicos al Directorio sobre la eficacia de las políticas implementadas.

61. El área de TI debe proporcionar los servicios en un ambiente seguro, que incluya no solamente las condiciones operativas del área de TI sino también factores tales como confiabilidad, confidencialidad, integridad y disponibilidad. Incluye además el soporte y la capacitación a los usuarios del servicio y la habilidad para manejar problemas e incidentes, operaciones, desempeño del sistema, planificación de la capacidad y administración de los datos e instalaciones.

Las prácticas de manejo de riesgos promoverán operaciones de TI efectivas, seguras y sólidas, que aseguren la continuidad de las operaciones y la confiabilidad y disponibilidad de la información. El manejo del riesgo operacional derivado de los sistemas debe comprender a toda la organización y proveedores externos.

Debe asegurar que se cumpla con los siguientes requerimientos:

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

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

61.3 Asegurar la calidad de los procesos y/o los programas que monitorean la capacidad y el desempeño del servicio de TI.

61.4 Asegurar la calidad de la asistencia proporcionada a los usuarios, incluida la habilidad para manejar problemas.

61.5 Contar con adecuadas políticas operativas, procedimientos y manuales.

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

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

61.7 Se han documentado adecuadamente a través de contratos, las condiciones y niveles mínimos de servicio a ser obtenidos del proveedor.
61.8 Se han establecido controles adecuados sobre los proveedores externos y que la institución es capaz de monitorear los mismos.

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

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

62. 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:

62.1 Contar con un Análisis de Impacto al Negocio con el cual se identifiquen las actividades críticas de la institución.

62.2 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 unidades de negocios.

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

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

62.5 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.

63. La institución debe contar con una gestión integral e independiente de la seguridad de la información.

Para ello debe:

63.1 Mantener actualizada la clasificación de sus activos de información. Debe asignarse dueño y custodio a todo dato y software necesario para reconstruir las informaciones emitidas para el Banco Central del Uruguay, los registros contables y cada uno de los movimientos que dan origen a los mismos (hasta el grado de detalle establecido en la normativa vigente).

63.2 Implementar estándares, procedimientos y directrices que permitan preservar la confidencialidad, integridad y disponibilidad de la información, teniendo en cuenta aspectos de seguridad física y lógica.

63.3 Identificar, evaluar, tratar 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.

63.4 Contar con indicadores y medidas que contribuyan al monitoreo de la gestión de la seguridad de la información.

63.5 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.

63.6 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.

63.7 Contar con una política, procedimientos e indicadores de gestión de incidentes de seguridad, y llevar a cabo pruebas frecuentemente de manera de tener actualizados las actividades a realizar.

64. La función de cumplimiento debe contar con mecanismos para identificar, medir, controlar y monitorear el riesgo de cumplimiento asumido.

Para ello debe:

64.1 Asesorar al Directorio y a la Alta Gerencia del cumplimiento por parte de la institución de las leyes, normativas y estándares aplicables.

64.2 Contar con la suficiente autoridad, importancia, independencia, recursos y acceso al Directorio

64.3 Promover y participar activamente en la capacitación de todos los funcionarios en materia de cumplimiento, actuar de punto de contacto para preguntas sobre cumplimiento y guiar sobre la aplicación adecuada de las leyes, normas, estándares aplicables, políticas y procedimientos, códigos de ética y de buenas prácticas.

64.4 Implementar mecanismos para identificar y evaluar el riesgo de cumplimiento existente en las distintas actividades de la entidad, incluyendo los productos nuevos, las propuestas de nuevos tipos de negocios o cualquier cambio en las características del relacionamiento con los clientes.

64.5 Establecer mecanismos para medir el riesgo de cumplimiento y usar estas medidas para mejorar el manejo de este riesgo. Algunos indicadores pueden ser utilizados con el apoyo tecnológico respectivo, para identificar y medir potenciales problemas de cumplimiento.

64.6 Implementar mecanismos para monitorear la efectividad de las políticas mediante pruebas sobre el cumplimiento.

64.7 Reportar al Directorio sobre los resultados del monitoreo y en general, sobre el perfil general del riesgo de cumplimiento basado en los indicadores definidos.

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

La información suministrada por la entidad es un insumo básico para que el supervisor pueda cumplir con sus responsabilidades. Por tanto, la calidad de dicha información es fundamental y constituye un elemento esencial en la definición del alcance de las actividades que debe desarrollar.
Para que el patrimonio cumpla su función, el monto reportado debe existir realmente. Como consecuencia, es crítico que los activos y pasivos estén valuados correctamente. Los sistemas de contabilidad y procedimientos utilizados para informar al Supervisor y al público en general son un elemento crítico en la evaluación del perfil de riesgos de una institución y de su condición financiera y patrimonial.

Para que el proceso de generación de información al supervisor sea confiable debe:

65.1 Tener políticas y procedimientos claros sobre el tratamiento contable consistente con los requisitos regulatorios y los estándares internacionales.

65.2 Asegurar que los procesos de contabilización son eficaces y controlados evitando el diferimiento en la contabilización de las operaciones.

65.3 Existir un proceso automatizado de generación de información, donde ésta fluya naturalmente desde las transacciones a los productos finales de información.

65.4 Estar dotado de un sistema de controles adecuados (separación de funciones, actividades de control, reportes, etc.).

65.5 Contar con recursos suficientes y capacitados para llevar adelante la tarea en tiempo y forma.

65.6 Estar sometido a revisiones independientes periódicas por parte de la Auditoría Interna.

65.7 Contar con un responsable por la generación de información hacia el exterior de la empresa (tanto para el supervisor como para cualquier usuario externo).

C – REVISIÓN DEL SISTEMA

66. La institución debe establecer mecanismos de revisión independiente y periódica del proceso de gestión del riesgo operacional. Los resultados de las revisiones deben ser reportados directamente al Directorio y a la Alta Gerencia.

La revisión independiente debe incluir la evaluación de:

66.1 El sistema en su conjunto y su eficacia en el cumplimiento de los objetivos.

66.2 El cumplimiento efectivo de las políticas y procedimientos y la adecuada documentación de los procesos y las decisiones adoptadas.

66.3 La organización y la suficiencia de los recursos humanos en cuanto a número y competencia técnica para gestionar en forma correcta el riesgo.

66.4 La capacidad y eficacia del sistema para capturar todos los elementos materiales de riesgo.

66.5 La confiabilidad y corrección en el procesamiento, agregación y cotejo de los datos.

66.6 Los supuestos utilizados en la formulación de los modelos y si están correctamente documentados.

66.7 Los cambios significativos que puedan afectar la efectividad de los controles, como cambios en los mercados, recursos humanos, tecnología o estructuras de cumplimiento.

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 operaciones de lavado son realizadas con el propósito de legalizar (o al menos dar apariencia de ello) bienes de origen ilícito; encubrir el origen ilícito de los recursos eliminando el vínculo con la actividad que lo originó, o mezclar dineros ilegales con transacciones financieras legítimas a efectos de justificar el origen de la suma total como proveniente de alguna actividad legal que sirve de fachada. En cambio, los fondos utilizados para apoyar el terrorismo pueden provenir de fuentes legítimas, actividades delictivas, o ambas. En este caso lo que importa es ocultar la fuente del financiamiento, sin reparar en si es legítima o ilícita, ya que si se logra encubrir la fuente, ésta se mantiene disponible para actividades de financiamiento futuras. Las instituciones financieras cumplen un rol importante, ya que se intentará por parte de las personas u organizaciones delictivas, su utilización de diversas formas, desde la introducción del efectivo al circuito legal; la realización de múltiples transferencias o giros bancarios tendientes a borrar el rastro, traspaso de custodia de valores y dificultar el seguimiento de los fondos ilícitos; hasta reincorporarlos formalmente al circuito legal utilizando la fachada de alguna actividad económica lícita y desarrollando transacciones normales para cualquier empresa, como por ejemplo importaciones,

exportaciones, pagos de servicios o intereses sobre préstamos, pero con la característica especial de tener un origen ilegítimo y muchas veces ficticio.

Las instituciones deberán 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 deberán 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. Se deberán implantar reglas estrictas tendientes a conocer cabalmente a sus clientes, logrando identificar quién es el "verdadero beneficiario" de la cuenta. También será necesario establecer estándares éticos que le aseguren sobre la integridad de su personal y definir programas de formación continua para el personal que habiliten a los empleados a reconocer las innovaciones relacionadas a estos ilícitos y a proceder según la situación. Asimismo, los intereses comerciales del banco no deberán oponerse en absoluto al eficaz desempeño de la función de cumplimiento, debiendo la entidad asumir una estructura de funcionamiento y responsabilidades acorde con su tamaño y complejidad de la operativa y nivel de riesgo.

67. El Directorio debe aprobar la estrategia y las políticas que propicien una adecuada gestión del riesgo de Lavado de Activos y Financiamiento del Terrorismo en base individual y consolidada y revisarlas periódicamente. El Directorio debe revisar regularmente la exposición al riesgo de LA/FT y asegurar que los niveles de riesgos se encuentran dentro del marco establecido.

Para ello, el Directorio debe:

67.1 Aprobar las estrategias y políticas en relación al riesgo LA/FT y revisarlas periódicamente. Estas políticas deben ser consistentes con el marco de riesgo definido y deben ser aplicadas en forma consolidada y a nivel de las entidades individuales cuando corresponda.

Las mismas deben:

- Promover normas éticas y profesionales de alto nivel para impedir que la institución sea utilizada con fines delictivos.
- Definir criterios para la prevención y detección de actividades delictivas y la notificación de las actividades sospechosas al supervisor.
- Definir criterios claros de aceptación de inicio y cese de vinculación con clientes y relaciones de corresponsalía.
- Establecer criterios de selección, evaluación y capacitación del personal y de las terceras partes en la que se delegan actividades comerciales o de servicios.
- Prever mecanismos de identificación y notificación de excepciones a las mismas.

67.2 Conocer y entender los riesgos de LA/FT a los que se encuentra expuesta la institución y el grupo a los efectos de definir políticas acordes a los riesgos identificados.

67.3 Promover una cultura de control y presentar un fuerte compromiso con la prevención del riesgo de LA/FT

67.4 Asegurar que exista una estructura organizacional, con una adecuada separación de funciones y una clara asignación de responsabilidades, que incluya la designación del Oficial de Cumplimiento con la preparación e idoneidad adecuada, asignándole jerarquía dentro de la organización, los recursos humanos y materiales necesarios para desarrollar su tarea en forma autónoma y eficiente .

67.5 Contar con información suficiente, detallada y oportuna, de forma que le permita comprender el nivel de riesgo al que se encuentra expuesta la entidad y evaluar el desempeño de la Alta Gerencia y en particular del Oficial de Cumplimiento, en el monitoreo y control de este riesgo.

67.6 Asegurar la realización de revisiones independientes para que en forma periódica se validen los procesos, las políticas, los procedimientos y los controles relativos al sistema de prevención de LA/FT. Asegurar que se instrumenten las acciones apropiadas ante las debilidades o fallas significativas detectadas por el auditor interno, externo, supervisor o profesional independiente.

67.7 Asegurar que se cuenta con un soporte tecnológico adecuado para el sistema de administración del riesgo de LA/FT.

67.8 Asegurar que la Alta Gerencia implemente las políticas y los procesos necesarios para que los riesgos asumidos sean consistentes con las estrategias y políticas aprobadas.

68. La Alta Gerencia debe asegurar la implementación de las políticas de riesgo aprobadas por el Directorio en relación al riesgo de lavado de activos y financiamiento del terrorismo, y el desarrollo de procedimientos para la identificación, medición, monitoreo y control.

Para ello, la Alta Gerencia debe:

68.1 Conocer y analizar periódicamente los riesgos a los que se encuentra expuesta la entidad considerando todos los factores relevantes para determinar su perfil de riesgo y el adecuado nivel de mitigación que se aplicará.

68.2 Instrumentar una estructura organizacional con clara definición de responsabilidades, que cuente con los recursos necesarios en cantidad, conocimiento técnico y experiencia, que aseguren un eficaz cumplimiento de las actividades de análisis, monitoreo y control del riesgo.

68.3 Asegurar que el personal comprenda su rol en el sistema de prevención y esté en conocimiento de los procedimientos y controles internos diseñados de forma de mitigar el riesgo de LA/FT.

68.4 Se asignan los recursos necesarios en cantidad, calidad y competencia a efectos de un buen manejo del riesgo de LA/FT.

68.5 Asegurar que el sistema de gestión del riesgo de LA/FT cuente con:

- Procedimientos y criterios de admisión y desvinculación de clientes
- Procedimientos de debida diligencia
- Procedimientos de gestión de la información
- Criterios de categorización de clientes
- Determinación de niveles máximos de exposición
- Procedimientos y/o sistemas para la identificación y gestión de alertas
- Procedimientos de identificación y reporte de operaciones inusuales o sospechosas

68.6 Asegurar que en el proceso de creación de nuevos productos se considere el riesgo LA/FT en forma explícita.

68.7 Asegurar que el Código de Ética aprobado es conocido y aplicado por toda la organización y refleja el compromiso institucional con el ambiente de control, estimulando la conciencia y el compromiso de control entre todo su personal, la integridad y los valores éticos, en particular en cuanto a prevenir su utilización para el lavado de activos y financiamiento del terrorismo

68.8 Controlar que las áreas de negocios (incluyendo las dependencias) apliquen adecuadamente los procesos de debida diligencia definidos y, cuando corresponda, verificar que el monitoreo aplicado sea acorde a los perfiles de riesgo asignados

68.9 Revisar periódicamente las políticas y procedimientos para asegurar que siguen siendo adecuados y prudentes y acordes al nivel de actividad y complejidad financiera de la operativa desarrollada.

68.10 Desarrollar un sistema de información que permita una oportuna y correcta agregación y notificación al Directorio de las exposiciones al riesgo de LA/FT, así como que permita evaluar la efectividad de gestión del riesgo.

69. 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:

En su rol de encargado del sistema de prevención:

69.1 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 deberán aplicarse en toda la institución, sus subsidiarias y sucursales y en los servicios tercerizados.

69.2 Verificar que los riesgos se encuadren dentro de los niveles fijados por la Dirección y en caso contrario pasen a conocimiento y decisión de los niveles jerárquicos correspondientes.

69.3 Proponer la actualización de políticas y procedimientos en relación al riesgo de LA/FT.

69.4 Verificar a través de muestreos el adecuado funcionamiento del sistema de gestión del riesgo de LA/FT y sus componentes, de forma que permita detectar posibles apartamientos al marco de riesgo aprobado.

69.5 Diseñar programas de capacitación del personal y detectar necesidades de capacitación en materia de prevención de LA/FT.

69.6 Elaborar informes periódicos que incluyan, entre otros aspectos, su evaluación sobre la eficacia del sistema implantado por la institución para gestionar el riesgo y que permitan informar a sus niveles de reporte, en forma completa y oportuna, sobre el cumplimiento de las políticas.

69.7 Asegurar que se cumple, por parte de los prestadores de servicios tercerizados, con los términos y procedimientos acordados.

69.8 Proponer el uso de herramientas adecuadas a la complejidad y el nivel de actividad desarrollado.

69.9 Ser el funcionario que sirva de enlace con los organismos competentes (auditor interno, auditor externo, supervisor, profesionales en materia de LA/FT).

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

B - MEDICIÓN, CONTROL Y MONITOREO DEL RIESGO DE LA/FT

70. SISTEMA GENERAL. La institución debe desarrollar un sistema de administración del riesgo que permita identificar y evaluar los factores de riesgo a los que se encuentra expuesta.

Para ello, la institución debe:

70.1 Establecer y documentar una metodología para segmentar los factores de riesgo (productos, servicios, clientes zona geográfica y canales de distribución), definir eventos asociados a cada factor, determinar la posibilidad de ocurrencia y evaluar el posible impacto.

70.2 A partir de la evaluación de riesgos realizada definir el impacto y las acciones que se derivan, en cuanto a los procedimientos y monitoreo a realizar.

70.3 Contar con un sistema de categorización de clientes que permita segmentarlos según su nivel de riesgo de LA/FT

70.4 Definir procedimientos para el mantenimiento, actualización, custodia y registro de la información de clientes, beneficiarios finales y transacciones.

70.5 Contar con un sistema de información a la Dirección y Alta Gerencia adecuado que permita establecer la evolución y perfil del riesgo, así como la eficacia de los controles en la implementación de las políticas.

71. DEBIDA DILIGENCIA. 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

Los procedimientos de debida diligencia a aplicar deberán comprender como mínimo los siguientes puntos:

71.1 Respecto de los clientes o personas con las que opera la Institución:

- Un detalle de las actividades y mecanismos utilizados para una adecuada verificación de la identidad de los clientes y de los beneficiarios finales de las cuentas o transacciones, que incluyan una definición precisa de la forma en que se mantendrá un contacto personal y los procedimientos alternativos para las excepciones para los casos de menor riesgo.+
- Un detalle de la información y documentación mínima a requerir al cliente y beneficiario final para verificar sus antecedentes, actividad y origen de fondos.
- Entender el propósito de la vinculación del cliente y obtener información suficiente de él y/o del beneficiario final a los efectos de obtener un conocimiento adecuado de los riesgos asociados a la relación comercial y que provea información para su seguimiento posterior. En los clientes considerados de mayor riesgo o aquellos que conforman grupos económicos o financieros vinculados por un mismo titular, beneficiario final o apoderado y operan a través de distintas cuentas, el conocimiento y perfil transaccional asignado debe fundamentarse en un informe circunstanciado.
- Procedimientos de debida diligencia reforzada para las personas políticamente expuestas, para los clientes categorizados como de alto riesgo y para los clientes de banca privada con alta transaccionalidad que incluya, entre otros aspectos, mecanismos para su identificación y aprobación de su vinculación por la alta dirección, confección de informes circunstanciado donde se fundamente la actividad, propósito de la cuenta, vínculo o transacción y el perfil transaccional y verificaciones y requerimientos de documentación más exigentes.
- Procedimientos para la identificación de aquellos clientes que, en forma habitual, realizan o cursan operaciones en sus cuentas transacciones financieras para terceras personas y procedimientos diferenciales de debida diligencia, distinguiendo aquellos que están supervisados por algún organismo nacional o internacional de aquellos que no lo están.

71.2 Respecto de otras relaciones

- Definir procesos específicos para la actividad de corresponsalía. Estos procesos incluyen:
  (a) recabar suficiente información sobre los bancos corresponsales para tener una comprensión plena de la naturaleza de su actividad y base de clientes, así como de la forma en que están supervisados;
  b) verificar que no se establezcan ni mantengan relaciones de corresponsalía con quienes carezcan de adecuados controles frente a actividades delictivas o no estén eficazmente supervisados por las autoridades pertinentes, o con aquellos bancos considerados simulados.
  c) parámetros de información a solicitar y el mecanismo de aprobación de la operativa con corresponsales del exterior, especialmente cuando se les habilite a éstos a canalizar fondos de y para sus clientes por medio de la entidad.

- Definir procesos específicos para los empleados de la institución que incluyan el análisis de antecedentes, cambios en el nivel de vida y comportamiento laboral, entre otros.

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

Para ello la institución debe:

72.1 Implementar procedimientos de seguimiento 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 seguimiento 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.

72.2 Contar con procedimientos especiales para identificar posibles operaciones tendientes a financiar actividades de terrorismo, realizando los controles y búsquedas en listas de individuos o entidades asociadas, confeccionadas en cumplimiento de las Resoluciones del Consejo de Seguridad de la Organización de las Naciones Unidas, para impedir el terrorismo y su financiamiento.

72.3 Contar con un sistema que permita monitorear especialmente y de acuerdo a su nivel de riesgo, a aquellos clientes que canalicen fondos en sus cuentas para terceros, debiendo permitir relevar información del beneficiario final de la transacción (cliente de su cliente) y requerir documentación de respaldo en ciertas condiciones de riesgo. Para los clientes que no se encuentran bajo supervisión y regulación, estos procedimientos de identificación y requerimientos de documentación para respaldar las transacciones no podrán ser menos exigentes que los requeridos para sus propios clientes.

72.4 Definir procedimientos de monitoreo especial y previo a concretar la transacción, para aquellas que presenten características especiales de riesgo como ser el monto involucrado o las realizadas con personas y empresas - incluidas las instituciones financieras- residentes en países o territorios que no sean miembros del Grupo de Acción Financiera Internacional (GAFI) o de alguno de los grupos regionales de similar naturaleza o estén siendo objeto de medidas especiales por parte de éstos por no aplicar o no aplicar suficientemente las recomendaciones del mencionado organismo.

73. OPERACIONES INUSUALES Y SOSPECHOSAS. La institución debe contar con procedimientos para detectar las operaciones inusuales y/o sospechosas, de notificación al supervisor y para atender en forma oportuna sus solicitudes.

Para ello la institución debe:

73.1 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.

73.2 Ofrecer al personal con vínculo directo o el tercerizado, según corresponda, una descripción clara de sus obligaciones, así como instrucciones para el análisis, investigación y notificación de dichas actividades dentro de la entidad.

73.3 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.

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

73.5 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.

73.6 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.

73.7 Definir procedimientos que aseguren atender en forma oportuna y con información precisa las consultas o pedidos de información realizadas por la UIAF. Estos procedimientos deberán 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.

C – REVISIÓN DEL SISTEMA

74. La institución debe establecer mecanismos de revisión independiente y periódica del proceso de gestión del riesgo LA/FT. Los resultados de las revisiones deben ser reportados directamente al Directorio y a la Alta Gerencia.

La revisión independiente debe incluir la evaluación de:

74.1 El sistema en su conjunto y su eficacia en el cumplimiento de los objetivos.

74.2 El cumplimiento efectivo de las políticas y procedimientos y la adecuada documentación de los procesos y las decisiones adoptadas.

74.3 La organización y la suficiencia de los recursos humanos en cuanto a número y competencia técnica para gestionar en forma correcta el riesgo.

74.4 El equilibrio existente entre las áreas comerciales y de control de riesgos.

74.5 La capacidad y eficacia del sistema para capturar todos los elementos materiales de riesgo.

74.6 La confiabilidad y corrección en el procesamiento, agregación y cotejo de los datos.

74.7 Los cambios significativos que puedan afectar la efectividad de los controles, como cambios en los mercados, recursos humanos, tecnología o estructuras de cumplimiento.

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.

75. El Directorio debe aprobar y revisar periódicamente las políticas vinculadas al manejo de las relaciones con los clientes de la Institución, que incluyan formalmente el manejo de la información de los mismos y la atención de los clientes.

Para ello, el Directorio debe:

75.1 Aprobar las políticas en relación al riesgo de reputación. Estas políticas deben reconocer el riesgo de reputación que subyace en el relacionamiento con los clientes como un riesgo que la entidad debe manejar explícitamente. En este sentido, deberá incluir elementos tales como la definición de la estructura y responsabilidades en el servicio de atención a los clientes, el sistema de reportes, la conservación de la documentación, etc.

75.2 Establecer un servicio de atención a los clientes acorde a las características de la institución que permita canalizar las consultas y los reclamos recibidos, velando por los derechos de los clientes reconocidos legalmente y en la normativa del Banco Central del Uruguay, así como en las buenas prácticas bancarias que son razonablemente exigibles para la conducción responsable y diligente de los negocios.

75.3 Considerar el riesgo reputación derivado de pertenecer a un conglomerado financiero, generado por la existencia de entidades subsidiarias y entidades vinculadas, según corresponda.

75.4 Asegurar el cumplimiento de las políticas definidas en relación al riesgo de reputación.

75.5 Revisar periódicamente la efectividad de estas políticas.

76. La Alta Gerencia debe implementar y comunicar las políticas definidas, asegurar que las mismas se cumplen y reportar al Directorio sobre el manejo de este riesgo.

Para ello la Alta Gerencia debe asegurar que:

76.1 Se identifican adecuadamente las fuentes potenciales de riesgo de reputación y en consecuencia, se establecen mecanismos que mitigan o eliminan este riesgo.

76.2 Existen mecanismos de evaluación independientes de la efectividad de las políticas definidas en torno al relacionamiento con los clientes. La Auditoría Interna deberá incluir entre sus actividades la evaluación del funcionamiento del servicio de atención al cliente, en particular, la adhesión a las políticas y procedimientos definidos, la naturaleza y cantidad de reclamos recibidos y las operativas, productos o servicios que puedan presentar problemas extendidos de malas prácticas bancarias.

76.3 Se considera explícitamente el riesgo de reputación en el proceso de lanzamiento de nuevos productos u operativas.

76.4 Se manejan los riesgos derivados del manejo de información sensible o confidencial por parte de los proveedores de servicios tercerizados, cuando existen.

76.5 Existe un responsable del funcionamiento del servicio de atención al cliente. Este servicio debe ser llevado adelante con independencia y objetividad, por personas que cuentan con la experiencia y conocimientos adecuados para ejercer estas funciones. La institución podrá delegar este servicio en una persona física o jurídica externa, que reciba y resuelva los reclamos de los clientes, manteniendo la institución la responsabilidad por la correcta solución de los mismos. Esta delegación debe ser expresa y por escrito.

76.6 Se aplican efectivamente los procedimientos de atención de reclamos establecidos.

76.7 Existe 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 de Internet de la entidad.

76.8 Existen reportes al Directorio en forma periódica sobre cualquier aspecto que represente un riesgo de reputación significativo, en particular en lo que refiere a los resultados de la gestión del servicio de atención al cliente.

77. La institución debe contar con un sistema para gestionar adecuadamente las actividades de asesoramiento y administración y custodia de activos de terceros.

Para ello,

77.1 El Directorio debe establecer políticas claras en relación a estas actividades.

77.2 La Alta Gerencia debe implementar estas políticas y diseñar procedimientos que permitan gestionar los riesgos derivados de estas actividades.

77.3 El sistema de información debe permitir un monitoreo adecuado de los riesgos identificados en estas operativas por parte del Directorio y la Alta Gerencia.

ESTÁNDARES DE TECNOLOGÍA (T)

Los estándares para la evaluación de las áreas de Tecnología de Información (TI) tienen como base el conjunto de principios conocido como COBIT, en particular los vinculados al dominio de Adquisición e Implementación. Los restantes dominios han sido contemplados en los estándares de Gobierno Corporativo y de Riesgo Operacional.

78. La Gerencia de TI debe tener la habilidad para identificar las necesidades y para desarrollar, adquirir, instalar y mantener soluciones de TI apropiadas de acuerdo a las necesidades de la entidad.

Para ello debe:

78.1 Tener procesos para identificar necesidades e implementar, controlar y mantener soluciones de TI adecuadas. Esto incluye compras de hardware o software realizadas por el proveedor interno o externo de TI, desarrollo y programación realizado por la institución o un proveedor externo, compra de servicios a vendedores independientes, centros de procesamiento de datos vinculados a la institución o una combinación de estas actividades.
78.2 Implementar una metodología de desarrollo de sistemas de la institución que incluye un análisis y gestión adecuada de los riesgos tecnológicos asociados.

78.3 Implementar procesos que aseguren que se mejoran y reemplazan componentes de TI en forma prudente y dentro de un ambiente controlado. El comportamiento en el desarrollo y adquisición y en el manejo de los riesgos asociados debe basarse en la evaluación de factores como:

- El nivel y calidad de la supervisión y soporte al desarrollo y adquisición de sistemas por parte de la dirección.
- La adecuación de las estructuras organizacionales y gerenciales para establecer conocimiento y responsabilidad por las iniciativas en materia de sistemas y tecnologías de TI.
- El volumen, naturaleza y extensión de la exposición al riesgo de la institución financiera en el área del desarrollo y adquisición de sistemas.
- La adecuación de los estándares de desarrollo, ciclo de vida y programación de los sistemas de la institución.

- La calidad de las prácticas de administración de proyectos que son seguidos por los desarrolladores, operadores, nivel gerencial/propietario (entendiendo por propietario al usuario final dueño de la aplicación), vendedores independientes o proveedores vinculados (entendiéndose por proveedor vinculado a una empresa externa vinculada al grupo) de servicios de TI y los usuarios finales.
- La independencia de la función de aseguramiento de calidad y la adecuación de los controles sobre los cambios de programas.
- La calidad y exactitud de la documentación de los sistemas.
- La integridad y seguridad del software de red, de base y aplicaciones.
- El desarrollo de soluciones de TI que satisfagan las necesidades de los usuarios finales.
- El grado de compromiso del usuario final en el proceso de desarrollo de los sistemas.

78.4 Tener un proceso que comprende todas las fases necesarias para implementar un cambio de sistemas incluyendo investigación de las alternativas disponibles, selección de la opción más adecuada para la organización como un todo, conversión a un nuevo sistema o integración de un nuevo sistema con los existentes.

78.5 Evaluar en los proveedores externos de servicios de TI los aspectos vinculados a la calidad de las entregas de software y documentación y a la adecuación de la capacitación proporcionada a los clientes.