BCU
SUPERINTENDENCIA
DE SERVICIOS FINANCIEROS

Estándares Mínimos de Gestión para Empresas de Seguros

Julio 2013

BANCO CENTRAL DEL URUGUAY

BCU
SUPERINTENDENCIA
DE SERVICIOS FINANCIEROS

Índice

ESTÁNDARES MÍNIMOS DE GESTIÓN PARA EMPRESAS DE SEGUROS

INTRODUCCIÓN

Se hace saber a las Empresas de Seguros 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 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 sintetizar los resultados de la evaluación, se ha definido una metodología 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.

LA METODOLOGÍA CERT

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

C – Gobierno Corporativo: el sistema a través del cual las instituciones son dirigidas, monitoreadas y controladas.

E – Evaluación Económica Financiera: la situación económica financiera de la institución 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 asegurados y beneficiarios.

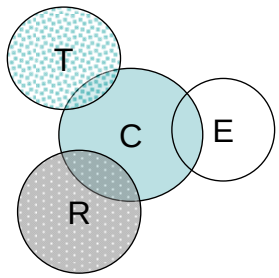
R – Riesgos: el sistema de gestión de riesgos de la institución y la capacidad de la misma de identificar, controlar, medir y monitorear los siguientes riesgos:

- Riesgo de Seguros
- Riesgo de Crédito
- Riesgo de Mercado
- Riesgo de Liquidez
- Riesgo Operacional
- Riesgo de Lavado de Activos y Financiamiento de Terrorismo
- Riesgo de Reputación
- Riesgo Estratégico

T – Tecnología: gestión de los riesgos tecnológicos y 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 el 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:



En aras de una mayor transparencia sobre la aplicación del nuevo 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 asociado a los cuatro 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 empresas de seguros 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 fundamentalmente 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 la 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.

El supervisor no certifica la adherencia estricta a los puntos específicos contenidos en estos estándares.

ESTANDARES DE GOBIERNO CORPORATIVO (C)

Definición - 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 y la Auditoría Externa.

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

- La existencia de una clara definición de roles y responsabilidades dentro de la organización 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 la institución, asegurar al mismo tiempo un fuerte control interno, un buen sistema de administración de riesgos, sistemas contables que garanticen integridad y confiabilidad, y un sistema de información íntegro, oportuno y de fácil acceso.

- El Directorio y la Alta Gerencia de la Institución deben ser integrados por personas con los conocimientos y competencias necesarias para cumplir sus roles respectivos. Deben planificar y dirigir la gestión comercial y de riesgos y manejar eficazmente la solvencia de la entidad.

- Debe existir un ambiente de control adecuado en relación al volumen y complejidad de las operaciones y al perfil de riesgo de la institución. El mismo debe permitir un control eficiente y alentar un uso eficaz de los recursos.

Se consideran en este capítulo los estándares mínimos que deben cumplir el Directorio, la Alta Gerencia, el Comité de Auditoria, la Auditoría Interna y la Auditoría Externa.

DIRECTORIO

En adelante, cuando se habla del Directorio debe entenderse como el órgano que ejerce la administración efectiva de la entidad. En las empresas de seguros organizadas como sociedades anónimas el Directorio y en las organizadas como cooperativas, el Consejo Directivo o Mesa Directiva.

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 La cantidad de miembros del Directorio, su experiencia y sus capacidades considerados colectivamente debe ser apropiada.

1.2 Los integrantes del Directorio deben tener un claro entendimiento de su rol dentro del Gobierno Corporativo.

1.3 El Directorio debe poseer la capacidad de ejercer un juicio independiente sobre los asuntos de la institución. 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.

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

1.5 Los Directores No Ejecutivos[1] no deben tener injerencia en las decisiones diarias de la gestión.

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

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 la entidad y su controlante.

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

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

2.3. 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 seleccionar, monitorear y si es necesario reemplazar a la Alta Gerencia.*

Para ello, el Directorio debe:

3.1. Evaluar regularmente la efectividad y prudencia de la Alta Gerencia en la gestión de las operaciones y de los riesgos.

[1] 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 como Directores.

3.2. Asegurar que la Alta Gerencia que se designe cumple con los criterios de capacidad e integridad.

3.3. Aprobar los roles y responsabilidades de la Alta Gerencia.

3.4. Considerar un plan de sucesión para el equipo gerencial.

4. *El Directorio debe aprobar los objetivos estratégicos de la institución y supervisar su implementación.*

Para ello, el Directorio debe:

4.1. Aprobar un marco estratégico adecuado al nivel de capital de la empresa que defina claramente el negocio objetivo y los retornos esperados y que sea consistente con el nivel de riesgo definido.

4.2. Aprobar el Plan de Negocios que contemple los objetivos estratégicos definidos.

4.3. Evaluar regularmente los resultados contra el presupuesto diseñado.

4.4. Revisar por lo menos anualmente la estrategia, los objetivos, y los planes para asegurar que siguen siendo válidos.

4.5. 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.

4.6. Aprobar una estrategia y políticas de Tecnología de la Información (TI), adecuadas a la estrategia general de la empresa y asegurar que la Alta Gerencia implementa los procedimientos que las hacen aplicables. Para lo cual debe asegurar que:

- La Institución 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.

5. *El Directorio debe aprobar una estrategia de riesgos y políticas asociadas que permitan la identificación y análisis 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:

5.1. Entender los riesgos que enfrenta la entidad, así como definir el nivel de exposición a cada tipo de riesgo.

5.2. Promover una cultura de riesgos en la organización.

5.3. Aprobar al menos anualmente la estrategia de riesgos, la que debe incluir todos los riesgos que quiere asumir y la tolerancia a los mismos. La estrategia de riesgos debe:

- Ser consistente con el perfil general de riesgo y el capital de la institución.
- Ser consistente con la estrategia general y el Plan de Negocios definidos.
- Considerar los factores internos y externos que afectan la entidad, (aspectos coyunturales de la economía, su posición en el mercado, las ramas o productos en que opera, las capacidades del personal, la tecnología, etc.).
- Estar definida por escrito y ser coherente con prácticas aseguradoras prudentes y con los requisitos regulatorios.

5.4. Asegurar que la Alta Gerencia toma las medidas necesarias para implementar un sistema de gestión de riesgos que involucra a todo el personal y es proactivo.

5.5. Asegurar que existan políticas y procedimientos por escrito 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.

5.6. Asegurar que existe un sistema de Evaluación de Riesgos que garantiza el logro de los objetivos de TI y que permita responder a las amenazas.

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

5.8. Comunicar oportunamente las políticas a toda la Institución. Todo el personal pertinente debe entender claramente el enfoque de la Institución respecto a cada riesgo y deben cumplir con las políticas y procedimientos establecidos.

6. *El Directorio debe asegurar que la función actuarial cumple su cometido.*

La función actuarial comprende la participación en:

- la definición de las políticas de riesgo de seguro y en el lanzamiento de nuevos productos.
- la gestión de los riesgos propios de los seguros
- la valuación de las reservas técnicas

Sin perjuicio de esto, la responsabilidad última sobre estos aspectos recae sobre el Directorio de la Institución.

Para ello el Directorio debe:

6.1. Reconocer la importancia de esta función asignando los recursos necesarios para un adecuado desempeño de la misma.

6.2. Asegurar que esta función es llevada a cabo por personal independiente del área comercial.

6.3. Asegurar que quien realice la función cuenta con la competencia y capacidad necesaria para cumplir su función adecuadamente.

6.4. En el caso que dicha función se tercerice se deberá asegurar que se cumplan los estándares anteriormente detallados.

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 los estándares éticos (a través de un Código de Ética) que guíen el accionar de la compañía.

7.2. Asegurar que los mismos son comunicados a toda la organización.

7.3. Actuar como ejemplo del cumplimiento de los estándares éticos.

7.4. Asegurar que existen políticas y procedimientos claramente definidos para el tratamiento de operaciones con partes relacionadas para que todas las transacciones se realicen en condiciones de equidad o mercado y se adopten códigos de gobierno corporativo adecuados. Estas políticas deberían incluir la aprobación por parte del Directorio de las operaciones más significativas.

7.5. Asegurar que las políticas de remuneración y compensación son transparentes y consistentes con la estrategia global de largo plazo de la institución y que existen mecanismos para verificar su cumplimiento.

7.6. Asegurar que las políticas de comisiones por intermediación son consistentes con la estrategia global definida por la institución y que ello es monitoreado regularmente.

8. *El Directorio debe promover una cultura de control en la organización, 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. 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 existe una adecuada segregación de funciones que facilite los controles cruzados.

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

8.3. 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.

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

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

9. *El Directorio debe asegurar que el Comité de Auditoria 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.

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

Para ello el Directorio debe:

10.1. Reconocer y comunicar la importancia de la Auditoría Interna dentro de la organización.

10.2. Asegurar que la Auditoría Interna le reporta directamente.

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

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

10.6. En el caso que dicha función se tercerice se deberá asegurar que se cumplan los estándares anteriormente detallados.

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 definir el nivel y calidad de capital requerido para respaldar los riesgos asumidos y proveer protección a los asegurados y beneficiarios.*

El Directorio debe asegurar que la institución cuenta con un nivel suficiente de capital para hacer frente a las reclamaciones y gastos esperados (Reservas Técnicas), pérdidas significativas inesperadas (nivel no cubierto por Reservas técnicas) y los otros riesgos a los que se encuentra expuesta la entidad, protegiendo así los derechos de los asegurados y beneficiarios. Este capital no podrá ser menor al que se determine en función de los requisitos regulatorios.

Para ello el Directorio debe:

12.1. Implementar un proceso sistemático e integral para determinar los requisitos de capital.

12.2. Establecer políticas que permitan asegurar que el nivel de capital es adecuado y prudente.

La evaluación de cumplimiento de este estándar se realizará teniendo en cuenta la naturaleza, complejidad y volumen de las operaciones que realiza la entidad, su perfil de riesgos y el nivel de solvencia que presenta.

13. ***El Directorio debe asegurar que la información provista al Supervisor representa fielmente la situación económico-financiera y los riesgos asumidos***

Para ello, el Directorio debe asegurar que:

13.1. Los procesos de elaboración de información son confiables.

13.2. La contabilidad utiliza criterios conservadores y de acuerdo con la normativa existente.

13.3. Todos los hechos relevantes que pudieran impactar negativamente a la institución son informados al Supervisor oportunamente.

14. ***El Directorio debe asegurar que se provee información financiera regular y otras informaciones que facilite a los agentes del mercado la evaluación de la entidad. El alcance y el contenido de la información provista y el nivel de desagregación debe ser consistente con el tamaño, complejidad y naturaleza de las operaciones de la institución.***

La divulgación de información a los agentes del mercado debe enfocarse, por lo menos, en las siguientes áreas, de forma de lograr un nivel satisfactorio de transparencia:

- Gestión financiera.
- Posición financiera (nivel de solvencia y rentabilidad).
- Prácticas de manejo de riesgos.
- Exposiciones a los riesgos.
- Líneas de negocios relevantes.

- Información sobre el funcionamiento del Gobierno Corporativo.
- Operaciones con personas o empresas relacionadas.
- Código de Ética.

Este estándar se evaluará en función de las prácticas del mercado y de las regulaciones existentes.

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 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:

15. *La Alta Gerencia como equipo y cada uno de sus integrantes deben poseer los conocimientos y habilidades para gestionar y supervisar los negocios bajo su responsabilidad.*

Para ello, la Alta Gerencia debe:

15.1. Estar integrada por personas con capacidad y experiencia en las áreas de responsabilidad y trabajar como equipo respetando los roles de los distintos integrantes y asegurar el cumplimiento de las directivas establecidas por el Directorio.

16. *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:

16.1. Desarrollar y presentar al Directorio para su aprobación:

- El plan de negocios en base a los lineamientos estratégicos definidos por el Directorio, que considere las características del

entorno económico y de negocios, la situación financiera de la institución y los riesgos en los cuales tiene o tendrá exposiciones.
- El presupuesto anual.

16.2. Implementar la estrategia y el plan de negocios aprobado.

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

16.4. Proveer al Directorio de información completa, relevante y oportuna sobre la implementación de la estrategia y los planes y sobre los resultados reales contrastados con los proyectados.

16.5. Asegurar que la estructura organizacional es consistente con los objetivos estratégicos que se fija la organización.

17. *La Alta Gerencia debe implementar un sistema de gestión integral de riesgos que contemple la visión de los riesgos, involucre a todo el personal y sea proactivo.*

Para ello, la Alta Gerencia debe:

17.1. Implementar la estrategia de riesgos aprobada por el Directorio.

17.2. Asegurar que se implemente un sistema que permita obtener una visión de todos los riesgos que asume la entidad.

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

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

17.5. Implementar un proceso para la aprobación y puesta en producción de nuevas ramas o productos que asegure un adecuado control y gestión de riesgos antes de su implementación.

17.6. Asegurar que el sistema de gestión de riesgos es integral.

17.7. Asegurar que existe un sistema de revisión independiente de los procesos y procedimientos de riesgos para identificar y resolver debilidades.

17.8. Asegurar que existe un responsable por cada uno de los riesgos relevantes.

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

Para ello, la Alta Gerencia debe:

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

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

18.3. Mantener un seguimiento estricto de los riesgos derivados de las actividades tercerizadas, asegurando la calidad del sistema de control de la institución.

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

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

19. *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 que aseguren su cumplimiento.*

Para ello, la Alta Gerencia debe:

19.1. 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.

20. *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:

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

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

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

20.4. La responsabilidad de TI está ubicada dentro de la estructura general de la organización de modo de garantizar la competencia técnica e independencia respecto de las áreas usuarias, en la medida necesaria para garantizar soluciones de tecnología de la información, útiles para la organización.

20.5. La Alta Gerencia asegura que existen procedimientos de control de la gestión de TI. La evaluación del desempeño de TI debe llevarse a cabo en forma periódica.

20.6. La Alta Gerencia, a intervalos regulares, mide la satisfacción del cliente sobre los servicios prestados por TI para identificar el déficit en los niveles de servicio y establecer objetivos de mejoras.

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

21. *La Alta Gerencia debe definir e implementar un sistema de información confiable, oportuna, fácilmente accesible y en un formato consistente.*

El sistema de información debe:

21.1. Cubrir todas las actividades significativas de la institución.

21.2. Estar integrado por información técnica, financiera, operativa y de cumplimiento adecuada y completa.

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

21.4. 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** - La relevancia de la información está directamente relacionada con las necesidades de la Gerencia y la Dirección para el desarrollo de su trabajo. Debe evitarse la información con excesivo detalle, generando una sobrecarga de información.

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

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

COMITE DE AUDITORIA

22. *El Comité de Auditoria 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:

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

22.2. Tomar medidas para que la gerencia lleve a cabo las acciones correctivas necesarias para subsanar las observaciones de la Auditoría Interna y Externa de manera oportuna.

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

22.4. Vigilar regularmente el adecuado funcionamiento de los mecanismos de control interno.

22.5. 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.

22.6. Aprobar un documento que establezca el propósito de la Auditoría Interna, sus objetivos, su autoridad y responsabilidades.

22.7. 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.

22.8. Verificar que se establezcan las medidas correctivas tendientes a corregir las debilidades detectadas y monitorear su implementación.

22.9. Aprobar la contratación y honorarios de los auditores externos e informar al Directorio. Esta contratación también puede ser realizada por el propio Directorio.

22.10. Revisar el plan de trabajo de la Auditoría Externa y asegurar que otras tareas adicionales (por ejemplo, consultorías) son compatibles y no impactan negativamente su independencia.

22.11. Revisar los informes de la Auditoría Externa.

AUDITORÍA INTERNA

23. *El Auditor Interno debe evaluar y monitorear el sistema de gestión integral de riesgos e informar al Directorio las potenciales debilidades.*

Para el cumplimiento de este estándar, se considera que el Auditor Interno debe:

23.1. Elaborar y someter a la aprobación del Directorio un manual de políticas y procedimientos para el trabajo de Auditoría.

23.2. Implementar procesos que aseguren que las pruebas, hallazgos y acciones correctivas son documentados adecuadamente.

23.3. Desarrollar y presentar al Directorio un plan anual de Auditoría. El plan anual debe contener las metas, cronogramas, recursos humanos necesarios y sistema de reportes.

23.4. Cubrir todas las actividades de la entidad en los ciclos previstos.

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

23.6. Presentar sus informes de actuación con sus conclusiones y recomendaciones al Directorio.

23.7. Mantener un inventario de debilidades encontradas, la fecha inicial de hallazgos y las medidas adoptadas para su corrección.

23.8. 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

24. *La Auditoría Externa debe aportar una visión fiel e independiente de la institución y de los demás agentes que tengan interés en la misma.*

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

24.1. Designa un equipo de Auditoría conformado por un número adecuado de personas competentes para la función que incluya personal propio o contratado con experiencia específica en métodos y técnicas actuariales para revisar la metodología y los cálculos implícitos en las reservas técnicas.

24.2. Comprende su deber hacia la institución y todas las partes interesadas.

24.3. Actúa con independencia en la realización de los procedimientos y en la planificación de las actividades.

24.4. 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 DE RIESGOS

Una competencia clave de las empresas de seguros es su capacidad de gestionar los riesgos que asume en forma prudente y rentable.

La empresa de seguros debe por lo tanto implementar un Sistema de Gestión de Riesgos, definido como el conjunto de políticas, procedimientos y mecanismos de control para propiciar una apropiada identificación, medición, control y monitoreo de los riesgos a los que se encuentra expuesta.

RIESGO DE SEGURO

El riesgo de seguro se define como la posibilidad de que la entidad vea afectado su patrimonio debido a la modificación adversa del valor de los compromisos asumidos en virtud de los seguros, debido a la inadecuación de las hipótesis de tarificación y constitución de reservas técnicas.

El riesgo de seguro surge como consecuencia de políticas y prácticas inadecuadas en el diseño de productos, la suscripción y la estimación del pasivo debido a errores en las hipótesis asumidas para la constitución de reservas técnicas.

El reaseguro y el coaseguro (especialmente en seguros generales) permiten mitigar este riesgo transfiriéndolo a compañías de reaseguro o compartiéndolo con otras entidades aseguradoras. Por su parte, el reaseguro constituye una fuente potencial de riesgo asociada a errores en el diseño y la administración del programa de reaseguro.

25.*El Directorio debe aprobar las políticas de suscripción de riesgos, constitución de reservas técnicas y reaseguro de la Institución.*

Para ello el Directorio debe:

25.1. Aprobar las políticas referidas al riesgo de seguro, las que deben:

- Ser consistentes con la naturaleza, volumen y complejidad del negocio.
- Estar detalladas por rama, producto o línea de negocio e incluir límites de exposición.
- Establecer los niveles de aprobación.
- Establecer el régimen de excepciones y nivel de aprobación para las mismas.
- Ser revisadas periódicamente.

25.2. En particular, las políticas de suscripción deben:

- Considerar los riesgos asegurables y las coberturas que la compañía mantendrá cautela o directamente no asumirá.
- Establecer límites de concentración relevantes por ejemplo por región geográfica, producto, industria, grupo, características de salud específicas u otro perfil de riesgo.

25.3. En particular, las políticas de constitución de reservas técnicas deben:

- Estar basadas en estándares actuariales internacionales
- Considerar la constitución de reservas adicionales en caso de no ser suficientes.

25.4. En particular, el programa de reaseguro debe considerar[2]:

- Los objetivos de la estrategia de reaseguro y establecer los parámetros bajo los cuales esta estrategia será controlada.
- La definición de los tipos de reaseguro apropiados para las distintas coberturas que comercializa considerando la capacidad técnica y financiera de la entidad.
- La posición respecto al uso de financiamiento a través de reaseguro financiero y fronting.

25.5. Revisar periódicamente la efectividad de la gestión del riesgo de seguro.

25.6. Asegurar que la Alta Gerencia implementa procedimientos adecuados para que los riesgos asumidos sean consistentes con las

[2] Los estándares relacionados a la selección de los reaseguradores se incluyen dentro de riesgo de crédito.

políticas aprobadas y el riesgo se mantiene dentro de los límites establecidos.

26. ***La Alta Gerencia debe implementar las políticas aprobadas por el Directorio para el riesgo de seguro y desarrollar procedimientos para su identificación, medición, monitoreo y control.***

Para ello, la Alta Gerencia debe:

26.1. Implementar procesos acordes con la política definida por el Directorio que permitan una suscripción adecuada de los riesgos, la valoración adecuada de las reservas y el cumplimiento del programa de reaseguro.

26.2. Informar al Directorio sobre la exposición de la entidad a las distintas fuentes de riesgo de seguro.

26.3. Asegurar que las personas involucradas en el proceso de gestión de este riesgo tienen las capacidades, conocimientos y herramientas para cumplir con sus responsabilidades, incluyendo la capacitación de agentes y corredores de seguros.

26.4. Autorizar las notas técnicas de los nuevos productos de seguros, considerando las bases técnicas utilizadas y el cumplimiento de las disposiciones normativas establecidas al respecto.

27. ***La institución debe contar con una función actuarial profesional y permanente que participe en la definición de las políticas y procedimientos del riesgo de seguro y en la valuación de las reservas técnicas.***

Para ello la función actuarial debe:

27.1. Contar con la capacidad, calificación y experiencia necesarias para la identificación del riesgo de seguro y su control. La calificación no necesariamente está relacionada con una membresía a una determinada asociación profesional o a un grado universitario, sin embargo quien desempeñe la función deberá tener conocimientos suficientes de matemática actuarial y financiera acordes con la naturaleza, el volumen y la complejidad de los riesgos asumidos.

27.2. Ser desarrollada en forma objetiva e independiente, ya sea por personal propio o contratado.

28. *La institución cuenta con una adecuada clasificación de riesgos asegurables y tarificación.*

Para ello:

28.1. La clasificación de riesgos y tarificación se efectúa con base en las políticas de suscripción y notas técnicas definidas y considera todos los aspectos relevantes en cada rama, producto o línea de negocio.

28.2. Existe predominio de criterios de suscripción sobre la tarificación.

28.3. El material de suscripción que se utiliza (solicitudes, informes de inspección, pólizas, formularios de denuncias) es adecuado y se emplea correctamente.

28.4. Establecer métodos de ajuste de tarifas u otras medidas tendientes a mejorar la insuficiencia de las mismas cuando los resultados técnicos negativos sean recurrentes, o los escenarios extremos por cambios en mortalidad, morbilidad, tasas y pérdidas máximas de exposición determinen que las primas resultan insuficientes después de la cobertura de reaseguro.

29. *La Institución debe definir procedimientos para asegurar que las reservas técnicas representan adecuadamente los pasivos asumidos más allá de los requisitos regulatorios.*

Para ello la Institución debe:

29.1. Garantizar la adecuación, integridad y exactitud de los datos utilizados en el cálculo de las reservas técnicas.

29.2. Asegurar la adecuación de las metodologías y modelos de base utilizados, así como las hipótesis utilizadas en los cálculos.

29.3. Revisar periódicamente dichos procedimientos.

30. *La institución debe contar con un proceso adecuado para la gestión de siniestros.*

La institución debe:

30.1. Contar con procedimientos para la gestión de los siniestros, que establezcan los criterios de apertura, liquidación y cierre, así como los criterios para acuerdos transaccionales.

30.2. Asegurar que la documentación de los expedientes de siniestros y el sistema de archivo contenga toda la información relevante.

31. ***La institución debe desarrollar procedimientos para asegurar que los contratos de reaseguro son apropiadamente suscritos.***

Para ello la Institución debe asegurar que los reaseguros contratados:

31.1. Son consistentes con el programa de reaseguro

31.2. Son adecuadamente suscritos de forma de garantizar que es posible beneficiarse de los derechos adquiridos bajo los mismos.

32. ***La institución cuenta con un sistema adecuado para la medición, monitoreo y control del riesgo de seguro.***

Para ello la institución debe:

32.1. Medir la exposición al riesgo de seguro (insuficiencia de primas, valuación de reservas técnicas y adecuación del programa de reaseguro) y el impacto que su realización ocasionaría en los resultados y el patrimonio de la entidad.

32.2. Contar con un sistema que suministre información oportuna y relevante que permita al Directorio y la Alta Gerencia cumplir con su rol de supervisión.

RIESGO DE CRÉDITO

El riesgo de crédito se define como la posibilidad de que la entidad vea afectado su patrimonio debido a la incapacidad de los deudores o las contrapartes de cumplir con los términos originalmente pactados.

33. El Directorio debe aprobar las políticas para la contratación de reaseguros y la colocación en Instituciones Financieras.

Para ello el Directorio debe:

33.1. Aprobar las políticas respecto al riesgo de crédito las que deben:

- Considerar la selección de empresas reaseguradoras con una calificación crediticia igual o superior a la establecida en la regulación.
- Considerar la selección de los intermediarios de reaseguros.
- Establecer la tolerancia al riesgo de crédito en las colocaciones en las Instituciones Financieras.
- Ser revisadas periódicamente

33.2. Establecer límites y asignar facultades de aprobación las que deberán ser consistentes con la capacidad y experiencia de los designados.

33.3. Establecer límites a nivel de contrapartes individuales y de contrapartes relacionadas entre sí (conjuntos económicos).

33.4. Estar permanentemente informado de las contrapartes relevantes con problemas o potencialmente problemáticas.

33.5. Promover la aplicación de principios contables que reflejen las condiciones de deterioro.

33.6. Asegurar que la Alta Gerencia implementa procedimientos adecuados para que los riesgos asumidos sean consistentes con las políticas aprobadas y el riesgo se mantiene dentro de los límites establecidos.

34. La Alta Gerencia debe implementar las políticas aprobadas por el Directorio para el riesgo de crédito y desarrollar procedimientos para su identificación, medición, monitoreo y control.

Para ello, la Alta Gerencia debe asegurar que:

34.1. Las actividades de la Institución respecto a las contrapartes son consistentes con la política establecida, existen procedimientos escritos, implementados efectivamente y las responsabilidades de aprobación y revisión de contrapartes se asignan clara y adecuadamente.

34.2. La contratación de reaseguros debe estar sujeta a la política establecida y ser transparente. Los criterios establecidos no deberían ser modificados en función de las características de las operaciones o de las empresas relacionadas.

34.3. Las personas involucradas en el proceso de identificación, medición y control de los riesgos de crédito tienen las capacidades, conocimientos y herramientas para cumplir sus responsabilidades.

34.4. Existen procedimientos para identificar situaciones en las que se deba clasificar un grupo de contrapartes (en especial los reaseguradores) como relacionadas entre sí (conjunto económico) y por ende, como un solo riesgo.

34.5. Se monitorean las exposiciones actuales frente a los límites fijados y se tienen procedimientos para incrementar el monitoreo y tomar medidas adecuadas si se acercan a los límites.

34.6. Las previsiones son adecuadas en relación al nivel de riesgo asumido monitoreando permanentemente la situación de las contrapartes.

34.7. Identificar y monitorear las contrapartes con problemas y las potencialmente problemáticas (alerta temprana).

35. La Institución debe implementar un sistema para administrar el riesgo de crédito. El sistema debe ser coherente con la naturaleza, el tamaño y la complejidad de la institución.

Para ello la Institución debe:

35.1. Contar con un sistema de medición de riesgo de crédito que incorpore las exposiciones con las contrapartes y que capture toda fuente material de riesgo.

35.2. Desarrollar un sistema de información que permita:
- Suministrar información sobre todas las exposiciones con contrapartes.
- Comparar las mediciones y exposiciones contra los límites de riesgo establecidos e informar sobre las excepciones a los mismos de manera oportuna y adecuada.
- Detectar concentraciones de riesgo.

35.3. Implementar procedimientos para:

- o Identificar contrapartes con deterioro actual o potencial de manera temprana.
- o El manejo y resolución de problemas.

36. La institución debe realizar controles para asegurar que las excepciones en las políticas, los procedimientos y límites son reportadas oportunamente al Directorio y la Alta Gerencia.

36.1. Para ello debe asegurar que las excepciones sean reportadas rápidamente, estén claramente documentadas y reciban la atención de la Alta Gerencia en forma oportuna. Debe existir una política explícita para la autorización de excepciones y sobre las acciones a tomar en dichos casos.

RIESGOS DE MERCADO

El riesgo de mercado se define como la posibilidad de sufrir pérdidas en posiciones dentro y fuera de balance debido a movimientos adversos de las variables de mercado. 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 del portafolio de inversiones – Es el riesgo asociado a las eventuales pérdidas en el valor de mercado del portafolio de inversiones 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 del portafolio de inversiones 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, incluyendo las posiciones fuera de balance. Es el riesgo potencial de que el patrimonio de la entidad se vea afectado 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 de los activos y de los pasivos 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 el patrimonio 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, precio de mercancías y/o precio de bienes raíces.

37. El Directorio debe aprobar las políticas con respecto a la gestión de los riesgos de mercado.

Para ello el Directorio debe:

37.1. Aprobar las políticas que influyen sobre el nivel de riesgo de mercado asumido por la institución. Estas políticas deben:

- ser consistentes con la naturaleza, volumen y complejidad de las actividades.
- definir los tipos y niveles de riesgos aceptables
- establecer el régimen de excepciones y el nivel de aprobación para las mismas
- ser revisadas periódicamente

37.2. Identificar líneas de responsabilidad y autoridad en la gestión de los riesgos de mercado.

37.3. Recibir y revisar la información sobre los riesgos de mercado, la cual debe ser suficiente, detallada y oportuna, de forma que permita comprender los riesgos asumidos y evaluar el desempeño de la Alta Gerencia en el monitoreo y control de dichos riesgos

37.4. Evaluar periódicamente el impacto de las estrategias comerciales sobre los riesgos asumidos.

37.5. Asegurar que la Alta Gerencia implementa procedimientos adecuados para que los riesgos asumidos sean consistentes con las políticas aprobadas y el riesgo se mantiene dentro de los límites establecidos.

38. La Alta Gerencia debe implementar las políticas aprobadas por el Directorio para los riesgos de mercado y desarrollar procedimientos para su identificación, medición, monitoreo y control.

Para ello, la Alta Gerencia debe:

38.1. Implementar las políticas y procedimientos aprobados para gestionar los riesgos de mercado en el mediano y largo plazo.

38.2. Implementar un sistema de límites que asegure que las exposiciones a los riesgos se mantienen dentro del marco establecido por el Directorio.

38.3. Definir una metodología para valuar posiciones.

38.4. Desarrollar un sistema de información que le permita evaluar la sensibilidad de la institución a cambios en las condiciones del mercado y otros factores de riesgo.

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

38.6. Asegurar que las personas involucradas en el proceso de identificación, medición y control de los riesgos de mercado tienen las capacidades, conocimientos y herramientas para cumplir sus responsabilidades.

38.7. Definir claramente los responsables que asumen posiciones de riesgos, funciones de control, elaboración de reportes u otras áreas administrativas.

38.8. Contar con un proceso para analizar nuevos productos y actividades para asegurar que los riesgos financieros asociados son comprendidos e incorporados al proceso de Gestión de Riesgos.

39. 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.

En general, el sistema debe:

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

39.2. Evaluar el impacto de los cambios en los resultados y el valor económico.

39.3. Identificar excesos en límites establecidos.

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

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

39.6. 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.

40. La institución debe establecer un sistema de límites y otras prácticas que aseguren que los niveles de riesgo de mercado asumidos son consistentes con las políticas.

El objetivo de un sistema de gestión de riesgos de mercado es mantener la exposición dentro de los parámetros aprobados por el Directorio. Para lograr este objetivo, el sistema debe brindar los lineamientos necesarios y establecer límites a los riesgos.

Para ello, el sistema de límites debe:

40.1. Fijar límites globales para la institución y límites específicos para portafolios individuales, actividades o unidades de negocio.

40.2. 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.

40.3. Ser consistente con la forma de medición de riesgos de la institución y revisado periódicamente.

41. El sistema de gestión de riesgos de mercado debe prever la generación de información sobre las exposiciones a los riesgos de mercado. Los informes deben ser remitidos oportunamente al Directorio y la Alta Gerencia.

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. Los reportes deben:

41.1. Ser emitidos en forma regular y comparar las exposiciones con los límites establecidos.

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

41.3. Ser revisados por el Directorio y la Alta Gerencia regularmente.

RIESGO DE LIQUIDEZ

El riesgo de liquidez es la posibilidad de que la entidad no cuente con suficientes activos líquidos para hacer frente a las obligaciones asumidas. 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. 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.

42. El Directorio debe aprobar la política respecto a la gestión del riesgo de liquidez de la Institución.

Para ello, el Directorio debe:

42.1. Aprobar políticas vinculadas al manejo del riesgo de liquidez de la institución y revisarlas periódicamente. En las compañías que realicen transacciones de reaseguro pasivas materiales (en general seguros generales) deberán aprobar un programa de administración de liquidez en relación a sus actividades de reaseguro.

42.2. Aprobar y revisar periódicamente los planes de contingencia de la Institución para enfrentar eventuales problemas de liquidez.

42.3. Aprobar límites a las exposiciones al riesgo de liquidez y revisarlos regularmente.

42.4. Revisar periódicamente la efectividad de la gestión del riesgo de liquidez.

42.5. Asegurar que la Alta Gerencia implementa procedimientos adecuados para que los riesgos asumidos sean consistentes con las políticas aprobadas y el riesgo se mantiene dentro de los límites establecidos.

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

Para ello, la Alta Gerencia debe:

43.1. Desarrollar procedimientos específicos para la gestión de liquidez que tengan en cuenta el marco definido de gestión de activos y pasivos, las condiciones establecidas en los contratos de reaseguro que afectan la liquidez, diferentes monedas, activos radicados en diferentes países y el uso de los distintos instrumentos financieros.

43.2. Definir límites para asegurar la liquidez adecuada.

43.3. 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.

43.4. Desarrollar una estructura administrativa y un sistema de comunicación y consulta interna para asegurar que la estrategia de liquidez aprobada por el Directorio se implementa efectivamente.

43.5. Asegurar que las personas involucradas en el proceso de identificación, medición y control del riesgo de liquidez tienen las capacidades, conocimientos y herramientas para cumplir sus responsabilidades.

43.6. Desarrollar planes de contingencia para hacer frente a flujos de salida inesperados o problemas en el mercado de capitales que afecten la liquidez de las inversiones y cierren las fuentes alternativas de liquidez.

El plan de contingencia debe:

- 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.

- Incluir las acciones a tomar en el caso de enfrentarse con un problema de liquidez incluyendo que activos se realizarán o las fuentes posibles de fondos (líneas de crédito, apoyo del grupo, etc.). Debe establecer claramente la cantidad de fondos de estas fuentes que la Institución tendría a disposición y bajo qué situaciones podría usarlos.

44. La institución debe medir y monitorear de forma continua la liquidez.

Para ello la institución debe contar con un sistema que debe cumplir las siguientes características:

44.1. Tener la capacidad de calcular las posiciones de liquidez (flujos de efectivo prospectivos) a corto, mediano plazo y en situaciones de stress, por moneda y en forma agregada

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

44.3. Permitir conocer en todo momento los niveles de activos líquidos sostenidos.

45. La institución debe definir mecanismos de control que aseguren el cumplimiento de los límites de liquidez definidos y contar con un proceso adecuado para la identificación y tratamiento de las excepciones.

Para ello, la institución debe:

45.1. Asegurar que existen mecanismos de control interno que aseguren que el manejo del riesgo de liquidez se realiza en el marco general de riesgos y en particular en el contexto de gestión de activos y pasivos aprobado por el Directorio.

45.2. Tener políticas y procedimientos de control que expliciten los procesos de aprobación, límites, revisiones y otros mecanismos apropiados para proporcionar una seguridad razonable de que se logren los objetivos del manejo del riesgo de liquidez

45.3. Definir un proceso que permita identificar y monitorear adecuadamente las excepciones a los límites fijados por el Directorio.

46. La institución debe contar con sistemas de información adecuados para monitorear, controlar e informar el riesgo de liquidez. Los informes deben entregarse periódicamente al Directorio y Alta Gerencia.

Para ello, el sistema debe:

46.1. Proveer información que permita el control de exposiciones al riesgo de liquidez actuales en relación a los límites establecidos y al marco de gestión de activos y pasivos aprobado.

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

RIESGO OPERACIONAL

El riesgo operacional se define como la posibilidad de que el patrimonio de la entidad se vea afectado 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.

47. El Directorio debe aprobar las políticas para la gestión del riesgo operacional.

Para ello, el Directorio debe:

47.1. Aprobar las políticas en relación al riesgo operacional. Las mismas deben:

- Reconocer el riesgo operacional como un riesgo que la entidad debe manejar explícitamente y ser consistentes con la naturaleza, volumen y el nivel de complejidad de las operaciones.
- Constituir una guía clara en relación al control de este riesgo y asegurar que todo el personal está comprometido con dichas actividades de control.
- Ser revisadas periódicamente

47.2. Promover una cultura de control adecuada en la organización.

47.3. Asegurar que la gestión del riesgo operacional se lleva a cabo en forma continua y efectiva.

48. La Alta Gerencia debe implementar las políticas aprobadas por el Directorio en relación al riesgo operacional y desarrollar procedimientos para su identificación, medición, monitoreo y control.

Para ello, la Alta Gerencia debe asegurar que:

48.1. La entidad cuenta con una estructura organizacional adecuada para la gestión del riesgo operacional.

48.2. Se asignan responsabilidades para el manejo del riesgo operacional, independientemente de la estructura organizacional que se defina y se le asignen los recursos necesarios.

48.3. Los procedimientos consideren el riesgo operacional, que como mínimo, comprendan a las principales actividades de la institución.

49. La Alta Gerencia debe implementar procedimientos de identificación y evaluación de las fuentes de riesgo operacional y definir los mecanismos para mitigar o eliminar dichos riesgos.

Para ello, debe:

49.1. Realizar una autoevaluación de los procesos principales que permita su mapeo, revisarla periódicamente y definir controles orientados a mitigar los riesgos.

49.2. Generar un sistema de indicadores de desempeño que alerten sobre debilidades en los procesos principales.

49.3. Llevar un registro de los eventos de pérdidas por riesgo operacional que permita su consolidación y análisis.

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

49.5. Mantener un estrecho contacto con las estructuras de control definidas en la entidad, intercambiando información sobre el resultado de las actuaciones de cada una de ellas.

49.6. Asegurar que existe un proceso que asegure el cumplimiento con las leyes, normas e instrucciones emitidas por el supervisor.

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

49.8. Reportar periódicamente al Directorio sobre la eficacia de las políticas implementadas.

50. La información suministrada al supervisor debe ser confiable y oportuna.

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.

Los sistemas de contabilidad y procedimientos utilizados 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:

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

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

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

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

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

50.6. Contar con un responsable por la generación de información hacia el supervisor.

50.7. Contar con un proceso automatizado de generación de información, donde ésta fluya naturalmente desde las transacciones a los productos finales de información.

51. El área o responsable de TI[3] debe asegurar que los servicios de TI son proporcionados en un ambiente seguro, que incluya no solamente las condiciones operativas del área de TI sino también factores tales como confiabilidad, confidencialidad e integridad. 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 asegurarse que se cumplan con los siguientes requerimientos:

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

51.2. Contar con políticas de seguridad, procedimientos y prácticas adecuadas, en todas las unidades y en todos los niveles de la institución y por parte de sus proveedores externos.

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

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

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

51.6. Contar con adecuadas políticas operativas, procedimientos y manuales.

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

[3] Para evaluar este punto, se tendrá en cuenta la naturaleza, tamaño y complejidad de las operaciones que realice la institución. En aquellas cuyo porte lo permita, podrá existir un responsable de TI, en lugar de una Gerencia o Área, siempre que se administre el riesgo en forma igualmente satisfactoria

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

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

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

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

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

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

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

52. La entidad 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:

52.1. 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.

52.2. En caso de servicios prestados por terceros, requerir que el proveedor de los mismos cuente con un plan de contingencia y continuidad del negocio.

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

52.4. Revisar periódicamente la aplicabilidad de estos planes.

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

El riesgo de Lavado de Activos y Financiamiento del Terrorismo se define como 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 entre el dinero sucio y 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 empresas aseguradoras así como sus intermediarios (corredores) podrían con o sin su consentimiento verse involucradas en este tipo de actividades ilícitas, lo que podría exponerlas a problemas jurídicos y de reputación además de generar pérdidas en su actividad. En general puede decirse que existe mayor probabilidad de lavado en los seguros de vida y todos aquellos productos que habiliten diferentes formas de inversión, pero también pueden realizarse actividades de lavado mediante la utilización de otro tipo de seguros.

A efectos de mitigar este riesgo, las instituciones deberán instrumentar un sistema que abarque políticas, prácticas y procedimientos que le permitan prevenirse de ser utilizada como instrumento para el lavado o la canalización de fondos destinados al financiamiento del terrorismo. Para hacer más eficiente el funcionamiento del sistema preventivo, las entidades deberán realizar una evaluación del riesgo de LA/FT que enfrentan, teniendo en cuenta el tipo de productos, clientes, zonas geográficas, canales de comercialización y otros factores relevantes, estableciendo mayores exigencias de información y asignando los mayores recursos de control a los de mayor riesgo.

53. El Directorio debe aprobar las políticas en relación al riesgo de Lavado de Activos y Financiamiento del Terrorismo.

Para ello, el Directorio debe:

53.1. Aprobar políticas que:

- Sean consistentes con la naturaleza, tamaño y complejidad de las operaciones desarrolladas.
- Promuevan la conciencia y el compromiso de todo su personal de evitar ser utilizados para el LA/FT mediante un Código de Conducta.
- Establezcan el rol de los intermediarios en la identificación, evaluación, monitoreo y control del riesgo, manteniendo la Institución la responsabilidad sobre este riesgo.
- Aseguren la privacidad en el manejo de información.
- Establezcan mecanismos de revisión periódicos sobre las mismas.

53.2. Definir un marco de riesgos que incluya como mínimo:

- Directivas claras en cuanto al relacionamiento con los clientes en función de su grado de riesgo
- Identificación de productos, canales de comercialización, clientes, condiciones de contrato, países con valoración de riesgo y otros factores relevantes en función de su negocio y nivel de riesgo involucrado.

53.3. Designar un Oficial de Cumplimiento, asignándole jerarquía dentro de la organización y los recursos humanos y materiales necesarios para desarrollar su tarea en forma autónoma y eficiente.

53.4. Recibir y revisar 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.

54. La Alta Gerencia debe implementar las políticas aprobadas por el Directorio en relación al riesgo de lavado de activos y financiamiento del terrorismo.

Para ello, la Alta Gerencia debe:

54.1. Implementar :

- Procedimientos para la administración del riesgo LA/FT, que permitan identificar, medir, monitorear y controlar el riesgo como así también prevenir el ser utilizada en operaciones de lavado de dinero y financiamiento del terrorismo y reportar las operaciones sospechosas o inusuales.
- Procedimientos referidos a su personal que aseguren que cuenta con un alto nivel de integridad moral y capacitación consistente con el cargo desempeñado, teniendo en consideración las necesidades específicas identificadas.
- Asegurar que en el proceso de creación de nuevos productos se considere el riesgo LA/FT.
- Mecanismos que aseguren que los intermediarios cumplen con dichos procedimientos.
- Procedimientos que permitan atender los requerimientos de información por parte de las autoridades competentes.

54.2. Revisar periódicamente las políticas y procedimientos de forma de asegurar que continúan siendo adecuados, prudentes y acordes a los productos comercializados.

54.3. Asegurar que el Código de Conducta aprobado es conocido y aplicado por toda la organización y refleja el compromiso institucional con la prevención de su utilización para el lavado de activos y financiamiento del terrorismo.

55. 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.

En su rol de encargado del sistema de prevención debe:

55.1. Promover la permanente actualización de las políticas y procedimientos aplicados por la institución.

55.2. Controlar que se apliquen adecuadamente los procedimientos definidos.

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

55.4. Instrumentar un adecuado sistema de registro y documentación de la evaluación de riesgos, análisis de operaciones y controles realizados por la entidad.

55.5. Ser el funcionario que sirva de enlace con los organismos competentes.

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

55.7. Mantenerse actualizado, detectar las necesidades de capacitación del personal y establecer, coordinar y monitorear un programa de capacitación permanente y diferenciado, acorde a la entidad, que habilite a los empleados a reconocer las innovaciones relacionadas a estos ilícitos.

56. La institución debe desarrollar un sistema que permita identificar medir, monitorear y controlar el nivel de riesgo de manera que resulte consistente con los límites establecidos en las políticas.

Para ello, la institución debe:

56.1. Implementar un sistema que permita identificar su exposición al riesgo para los distintos productos, clientes, condiciones de contrato, canales de comercialización, métodos de pago y otros factores relevantes.

56.2. Diseñar procedimientos que contengan controles oportunos, efectivos y fáciles de implementar, para todos los factores de riesgo definidos por la Dirección. Los mismos deberán ser parte de un manual interno detallado, práctico y fácilmente consultable, el que deberá mantenerse actualizado.

56.3. Diseñar procedimientos de debida diligencia diferenciales que permitan obtener un adecuado conocimiento de los clientes y prevean su continua actualización y que contemplen criterios de aceptación (determinación de clientes objetivo y no deseados); requisitos de identificación; definición de un perfil de actividad o transaccional atendiendo particularmente la necesidad de requerir respaldo documental para aquellos de mayor riesgo y procedimientos para el seguimiento de las operaciones. Estos procedimientos deberán considerar el tipo de cliente, el tipo de seguro a contratar, el volumen de los fondos involucrados y la evaluación de riesgo realizada por la propia institución.

En particular se debe obtener, verificar, registrar, conservar y actualizar periódicamente la información que permita determinar:

- la verdadera identidad del cliente y si este actúa por cuenta propia o de un tercera persona, en cuyo caso se deberá identificar al beneficiario final
- el propósito de la póliza a contratar
- la actividad económica desarrollada por el cliente, que permita justificar adecuadamente la procedencia de los fondos y el tipo de póliza solicitada,

56.4. Adicionalmente, elaborar procedimientos especiales para situaciones que involucren, a modo de ejemplo:

- clientes residentes en países o territorios que no sean miembros del GAFI o estén siendo objeto de medidas especiales por la aplicación incompleta de sus recomendaciones,
- personas y empresas que se vinculan por medio de operativas en las que no es habitual el contacto directo y personal, tales como clientes no residentes, seguros contratados vía internet y otras en las que el uso de tecnología favorece el anonimato.
- personas políticamente expuestas, sus familiares y asociados cercanos,
- personas físicas o jurídicas que se vinculan por medio de servicios prestados por terceros (corredores)

56.5. Contar con herramientas acordes a la complejidad y volumen de sus actividades, que le permitan realizar un monitoreo de las operaciones.

57. La institución debe detectar las operaciones inusuales y/o sospechosas así como las relacionadas con bienes vinculados al terrorismo, procediendo a reportarlas a la UIAF.

Para ello la institución debe:

57.1. Establecer un mecanismo que le permita asegurarse de detectar en forma rápida, cualquier transacción vinculada directa o indirectamente con alguna de las personas u organizaciones incluidas en la “Lista Unificada” emitida y actualizada por el Comité de Sanciones de la ONU.

57.2. Realizar un seguimiento de las transacciones realizadas, procediendo al análisis de aquellas que resulten inusuales o complejas o de gran magnitud, para permitir la detección de las que correspondan incluirse en la categoría de inusuales o sospechosas. Asimismo se debe implementar el mecanismo de reporte a la UIAF.

58. El sistema de prevención deberá comprender la revisión y evaluación independiente sobre la idoneidad y funcionamiento de las políticas y procedimientos definidos.

Se deberá contar con un proceso regular de revisión independiente (el que podrá ser desarrollado por auditores internos, auditores externos, o consultores especializados) que incluya la evaluación de:

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

58.2. La confiabilidad y corrección en el procesamiento, agregación y cotejo de los datos del registro de operaciones relevantes.

RIESGO DE REPUTACIÓN

El riesgo de reputación es la posibilidad de que el patrimonio de la entidad se vea afectado por una opinión pública negativa. Afecta la capacidad de la institución de establecer nuevas relaciones o servicios, o continuar sirviendo las relaciones ya existentes. Este riesgo puede exponer a la institución a juicios, pérdidas financieras o a una disminución en la base de clientes.

59. *El Directorio debe aprobar y revisar periódicamente las políticas vinculadas al manejo de las relaciones con los clientes que consideren una gestión adecuada de las actividades de asesoramiento y la atención de reclamos por siniestros, ya sea directamente o a través de intermediarios; y que incluyan formalmente el manejo de la información.*

Para ello debe:

59.1. 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.

59.2. Establecer políticas claras con relación a los clientes que incluyan:

- El trato a los mismos de forma justa procurándoles información oportuna y relevante sobre la cobertura del seguro que adquieren, sus derechos, obligaciones, primas y otros cargos a cobrar (sea en forma directa o a través de intermediarios).

- El establecimiento de un proceso formal para reclamaciones por siniestros.

59.3. Establecer políticas claras de relacionamiento con los intermediarios que consideren:

- que posean conocimiento, capacidades adecuadas y que cuenten con buena reputación.
- que estos informen a los clientes de acuerdo a la política de asesoramiento definida en el punto anterior.
- su supervisión.

59.4. Establecer políticas claras de relacionamiento con terceros (proveedores más relevantes incluyendo tercerizaciones)

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

59.6. Revisar periódicamente la efectividad de estas políticas.

60. ***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, debe asegurar que:

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

60.2. Se diseñan procedimientos para el adecuado asesoramiento a los clientes y la atención de reclamos.

60.3. Se provee entrenamiento continuo al personal relevante en esta tarea.

60.4. Existen mecanismos de evaluación independientes de la efectividad de las políticas definidas en torno al relacionamiento con los clientes. Deberá incluirse 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.

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

60.6. Se consideran los riesgos derivados de la administración de información sensible o confidencial por parte de intermediarios y proveedores de servicios tercerizados, cuando existen.

60.7. Existe un responsable del funcionamiento del servicio de atención de reclamos de clientes, que cuenta con los recursos necesarios. 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.

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

60.9. Se supervisa a los intermediarios para el cumplimiento de las políticas y procedimientos definidos.

60.10. Existe una adecuada difusión del servicio de atención al cliente en las oficinas de la institución, en la documentación y en el sitio de Internet de la entidad.

60.11. 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.

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

Para ello,

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

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

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

ESTANDARES DE TECNOLOGIA (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.

62. La Gerencia o responsable 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:

62.1. 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.

62.2. Implementar una metodología de desarrollo de sistemas de la institución que incluye un análisis y gestión adecuada de los riesgos tecnológicos asociados.

62.3. 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, 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 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.

62.4. 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.

62.5. 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.