-DESIGNACION-
RESOLUCION JM 090402-05

-FECHA-
2009/04/02

-TITULO-
QUINTA RESOLUCION DE FECHA 02 DE ABRIL DEL 2009 QUE APRUEBA LA VERSION DEFINITIVA DEL REGLAMENTO SOBRE RIESGO OPERACIONAL

-MODIFICACION-
DECIMOSEGUNDA RESOLUCION DE FECHA 6 DE NOVIEMBRE DEL 2008

-DESCRIPTORES-
REGLAMENTO; RIESGO OPERACIONAL; ENTIDADES DE INTERMEDIACION FINANCIERA; VERSION DEFINITIVA

-TEXTO-

ADMINISTRACION MONETARIA Y FINANCIERA
JUNTA MONETARIA

AVISO

Por este medio se hace de público conocimiento que la Junta Monetaria ha dictado su **Quinta Resolución** de fecha **2 de abril del 2009**, cuyo texto se transcribe a continuación:

"VISTA la comunicación No.008973 de fecha 31 de marzo del 2009, dirigida al Gobernador del Banco Central y Presidente de la Junta Monetaria por el Subgerente General en funciones de Gerente de dicha Institución, mediante la cual remite su opinión respecto al Proyecto de Reglamento sobre Riesgo Operacional, sometido por la Superintendencia de Bancos a la consideración y aprobación definitiva de la Junta Monetaria;

VISTA la comunicación No.0148 de fecha 26 de marzo del 2009, dirigida al Gobernador del Banco Central y Presidente de la Junta Monetaria por el Superintendente de Bancos, mediante la cual remite el Proyecto de Reglamento sobre Riesgo Operacional, luego de ponderadas y discutidas las observaciones presentadas por las diferentes asociaciones que agrupan a las entidades de intermediación financiera;

VISTO el literal c) del Artículo 9 de la Ley No. 183-02 Monetaria y Financiera, de fecha 21 de noviembre del 2002, que establece que corresponde a la Junta Monetaria dictar los Reglamentos Monetarios y Financieros para el desarrollo de dicha Ley;

VISTO el literal f) del Artículo 46 de la Ley No.183-02 Monetaria y Financiera, de fecha 21 de noviembre del 2002, el cual establece que reglamentariamente se podrán determinar exigencias adicionales de patrimonio técnico en función de riesgos cambiarios, riesgo de tipo de interés, riesgos de liquidez, riesgos de plazo, riesgos de concentración de pasivo, riesgos de colateral, riesgos operacionales, riesgos legales y cualesquiera otros riesgos que en el futuro puedan agregarse;

VISTOS los literales a) y b) del Artículo 55 de la Ley No.183-02 Monetaria y Financiera, de fecha 21 de noviembre del 2002, que establecen que las entidades de intermediación financiera deben contar con adecuados sistemas de control de riesgos, mecanismos independientes de control interno y establecimiento claro y por escrito de sus políticas administrativas. Asimismo, estipulan que dichas entidades deben contar con políticas escritas actualizadas en todo lo relativo a la concesión de créditos, régimen de inversiones, evaluación de la calidad de los activos, suficiencia de provisiones, administración de los diferentes riesgos, entre otras disposiciones;

VISTO el literal g) del Artículo 4 de la Ley No.183-02 Monetaria y Financiera, de fecha 21 de noviembre del 2002, sobre el proceso de elaboración de los Reglamentos de la referida Ley;

VISTA la Decimosegunda Resolución dictada por la Junta Monetaria en fecha 6 de noviembre del 2008, mediante la cual autorizó la publicación para fines de consulta del Proyecto de Reglamento sobre Riesgo Operacional;

VISTO el cuadro comparativo del Proyecto de Reglamento sobre Riesgo Operacional con las observaciones presentadas por los sectores interesados;

CONSIDERANDO que el Proyecto de Reglamento sobre Riesgo Operacional tiene como objeto establecer los criterios y lineamientos generales que deberán aplicar las entidades de intermediación financiera para realizar una adecuada administración del riesgo operacional y comprende, además, las políticas y procedimientos mínimos que deberán implementar dichas entidades para identificar, medir, evaluar, monitorear y controlar el riesgo operacional a que están expuestas;

CONSIDERANDO que el Banco Central recibió las observaciones presentadas por la Asociación de Bancos Comerciales de la República Dominicana (ABA**),** la Liga Dominicana de Asociaciones de Ahorros y Préstamos (LIDAAPI), el Banco Nacional de Fomento de la Vivienda y la Producción (BNV), la Asociación de Bancos de Ahorro y Crédito y Corporaciones de Crédito, Inc. (ABANCORD) y la Asociación de Bancos

de Ahorro y Crédito, Inc. (ADOBAC), las cuales fueron ponderadas y analizadas conjuntamente por técnicos del Banco Central y de la Superintendencia de Bancos, a la luz de las disposiciones legales vigentes sobre el particular, con la finalidad de obtener un documento de consenso entre ambas instituciones;

CONSIDERANDO que entre las observaciones efectuadas al citado Proyecto de Reglamento, se encuentran algunas que son atendibles y otras que no son atendibles,

CONSIDERANDO que la ABA solicitó además eliminar las definiciones relacionadas con las tecnologías de la información, con el argumento de que las mismas salen del contexto del que debe tratar un Reglamento de Riesgo Operacional y solicitó que se incorporaran a nivel de instructivo. Esta observación fue atendida parcialmente, por lo que las políticas, procesos y procedimientos específicos de gestión de recursos humanos en el aspecto tecnológico estarán en función del tamaño y perfil tecnológico de las entidades de intermediación financiera;

CONSIDERANDO que la ABA sugiere ser más específico en la definición de los factores de riesgo, lo cual se estimó como atendible, precisando en dicha definición que las pérdidas por riesgo operacional sean a nivel de actividad o líneas de negocios;

CONSIDERANDO que ABA recomendó que se incluyera a la Alta Gerencia como la responsable de poner en práctica el marco para la gestión del riesgo operacional aprobado por el Consejo de Directores, el que a su vez debería encargarse del desarrollo de las políticas, procesos y procedimientos de la gestión de estos riesgos, sugerencia que fue estimada como atendible;

CONSIDERANDO que en lo que respecta al personal responsable de la administración del riesgo operacional, ABA sugirió que el mismo pueda estar integrado en el Departamento o Unidad de Riesgo ya existente en la entidad o en el grupo financiero. Asimismo, ABANCORD y ADOBAC observaron que los recursos humanos con la capacidad y el conocimiento para la aplicación de los requerimientos del Reglamento son limitados en este momento en nuestro país. En ese sentido, se consideró atendible el planteamiento de ABA y las observaciones de la firma de auditoría;

CONSIDERANDO que la ABA y el BNV sugirieron modificar el Artículo 20 del citado Reglamento, a los fines de que las entidades de intermediación financiera que dependan de un mismo controlador o conformen un grupo financiero puedan contar con una Unidad de Riesgos que incluya el riesgo operacional a nivel global y que pueda adoptar políticas y procedimientos

tanto a nivel individual como a nivel consolidado de sus filiales. Esta sugerencia fue estimada como atendible;

CONSIDERANDO que algunas de las observaciones realizadas por la ABA y el BNV consistían en que la mayor parte de las definiciones corresponden a manejo de tecnología y en ese sentido recomendaron que se incluyeran las definiciones y aspectos necesarios para el manejo del riesgo legal y de procesos, lo cual fue ponderado y se estimó como no atendible ya que no todas entidades de intermediación financiera tienen un personal calificado en materia de informática, sobre todo las pequeñas, por lo que las definiciones sobre aspectos tecnológicos podían coadyuvar a una mejor comprensión y manejo de las disposiciones contenidas en el Reglamento;

CONSIDERANDO que algunas de las observaciones de la ABA, la ABANCORD y la ADOBAC no fueron acogidas, tal como la sugerencia de eliminar el requisito de que cada entidad debe contar con tecnología de información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna, segura y confiable, lo cual fue estimado como no atendible, ya que el dispositivo establece este requisito para el manejo de los riesgos que las entidades asumen en sus operaciones;

CONSIDERANDO que la ABA sugirió que se eliminara el Artículo 32 sobre la planificación y organización para los objetivos de control de alto nivel de las tecnologías de la información, sugerencia que fue estimada como no atendible, ya que, según explicaron, no deben obviarse aquellos aspectos tecnológicos que sean posibles fuentes de riesgo operacional;

CONSIDERANDO que en vista de los planteamientos antes expuestos y tomando en cuenta que el Reglamento sobre Riesgo Operacional fue consensuado por técnicos del Banco Central y de la Superintendencia de Bancos, y que el mismo recoge las observaciones de los sectores interesados, procede acoger favorablemente la versión definitiva del citado Reglamento con las modificaciones introducidas;

Por tanto, la Junta Monetaria

R E S U E L V E:

1. Aprobar la versión definitiva del Reglamento sobre Riesgo Operacional, elaborado en virtud de las disposiciones del literal f) del Artículo 46 y los literales a) y b) del Artículo 55 de la Ley No.183-02 Monetaria y Financiera, de fecha 21 de noviembre del 2002.

2. Ordenar la publicación, en uno o más diarios de amplia circulación nacional del Reglamento sobre Riesgo Operacional, el cual copiado a la letra dice así:

REGLAMENTO SOBRE RIESGO OPERACIONAL
TITULO I
DISPOSICIONES GENERALES

CAPITULO I
OBJETO, ALCANCE Y AMBITO DE APLICACION

Artículo 1.- Objeto. El presente Reglamento tiene por objeto establecer los criterios y lineamientos generales que deberán aplicar las entidades de intermediación financiera para realizar una adecuada administración del riesgo operacional, en cumplimiento con las disposiciones contenidas en los Artículos 46, literal f) y 55, literales a) y b), de la Ley No. 183-02, Monetaria y Financiera, de fecha 21 de noviembre de 2002, en lo adelante la Ley.

Artículo 2.- Alcance. El alcance de este Reglamento comprende las políticas y procedimientos mínimos que deberán implementar las entidades de intermediación financiera para identificar, medir, evaluar, monitorear y controlar el riesgo operacional a que están expuestas.

Artículo 3.- Ambito de aplicación. Las disposiciones establecidas en el presente Reglamento son de aplicación para las entidades de intermediación financiera que se identifican a continuación:

a) Bancos Múltiples;
b) Bancos de Ahorro y Crédito;
c) Corporaciones de Crédito;
d) Asociaciones de Ahorros y Préstamos;
e) Banco Nacional de Fomento para la Vivienda y la Producción; y,
f) Cualquiera otra entidad de intermediación financiera que la Junta Monetaria autorice en el futuro.

CAPITULO II
DEFINICIONES

Artículo 4.- Para los fines de aplicación de las disposiciones contenidas en este Reglamento, los términos y expresiones que se indican a continuación, tanto en mayúscula como en minúscula, singular o plural, tendrán los significados siguientes:

Administración de riesgos: Es el procedimiento mediante el cual las entidades de intermediación financiera identifican, miden, evalúan,

monitorean y controlan los riesgos inherentes al negocio, con el objeto de conocer el grado de exposición a que están expuestas en el desarrollo de sus operaciones y definir los mecanismos de cobertura para proteger los recursos propios y de terceros que se encuentran bajo su control y administración.

Alta gerencia: La integran el presidente y los vicepresidentes, gerentes generales o cargos afines, responsables de ejecutar las disposiciones del Consejo de Directores, quienes toman decisiones de alto nivel, de acuerdo con las funciones asignadas y la estructura organizacional definida en cada entidad.

Arquitectura de la información: Se refiere al diseño de un sistema automatizado de información y sus componentes individuales. El diseño comprende la estructura lógica y física, incluyendo el entorno operativo, así como también la organización de los datos. Los componentes individuales están referidos a las redes de comunicación, hardware y software, los cuales incluyen sistemas operativos y programas de comunicación.

Autenticación: Es el acto de asegurar la identidad de un usuario para tener acceso a la información computarizada.

COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas): Es un marco de gobierno de TI que permite el desarrollo de políticas y buenas prácticas para el control de TI en todas las partes de la organización.

CMMI (Capacidad de Integración del Modelo de Madurez): Modelo para la mejora o evaluación de los procesos de desarrollo y mantenimiento de sistemas y productos de software.

COSO (Comité de Organizaciones Patrocinadores de la Treadway Comission): Es un marco general para la evaluación del control interno basado en la eficiencia y eficacia de las operaciones, la confianza en los sistemas de reportes financieros y la adherencia con las leyes y regulaciones existentes.

Encriptación: Es el proceso mediante el cual la información o archivos son alterados en forma matemática, con el objetivo de evitar que alguien no autorizado al verlos o copiarlos pueda interpretarlos, por lo que se utiliza una llave.

Eventos de pérdidas: Son aquellos incidentes que generan pérdidas a las entidades por riesgo operacional.

Factores de riesgo: Se entiende por factores de riesgos las fuentes generadoras de eventos en las que se originan las pérdidas por riesgo operacional a nivel de la actividad o líneas de negocios.

Información crítica: Es la información considerada esencial para la continuidad del negocio y para la adecuada toma de decisiones.

Infraestructura tecnológica: Equipo y sistemas con que cuenta la entidad para procesar la información, así como las adecuaciones del espacio físico que aloja los equipos y sistemas.

Integridad: Se refiere a la confiabilidad, exactitud y suficiencia de la información entregada a los usuarios finales.

ITIL (Infraestructura de Bibliotecas para Tecnología de Información): Es un marco de trabajo de las mejores prácticas destinadas a facilitar la entrega de servicios de alta calidad de tecnología de la información.

ISO (Organización Internacional para la Estandarización): Organización internacional para la estandarización de normas relativas a productos y seguridad para las empresas u organizaciones a nivel internacional.

Pista de auditoría: Es el registro de datos lógicos de las acciones o sucesos ocurridos en los sistemas aplicativos u operativos, con el propósito de mantener información histórica para fines de control, supervisión y auditoría.

Plan de contingencia: Es el conjunto de procedimientos alternativos a la operatividad normal de la entidad cuya finalidad es la de permitir su funcionamiento, buscando minimizar el impacto operativo y financiero que pueda ocasionar cualquier evento inesperado.

Plan de continuidad: Está orientado a asegurar la continuidad del negocio, la satisfacción del cliente y la productividad a pesar de eventos inesperados. Se ejecuta permanentemente como parte de la administración de riesgos tanto en la información como en la operación.

Procedimiento: Lista detallada de la secuencia lógica y consistente de actividades y cursos de acción, por medio de los cuales se asegura el cumplimiento de una función operativa.

Proceso crítico: Proceso indispensable para la continuidad del negocio y las operaciones de la entidad, y cuya falta de identificación o aplicación deficiente puede generar un impacto financiero negativo.

PMBOK (Cuerpo de Conocimiento para la Administración de Proyectos): Es un estándar para la gestión de proyectos que abarca una gama de procesos y áreas de conocimiento generalmente aceptadas.

Riesgo: Es la posibilidad de que se produzca un hecho que genere pérdidas que afecte los resultados y/o el patrimonio y la solvencia de las entidades de intermediación financiera.

Riesgo inherente: Es el riesgo que por su naturaleza no se puede separar de la situación donde existe. Es el riesgo propio de cada actividad, sin tener en cuenta el efecto de los controles.

Riesgo legal: Es la posibilidad de que se presenten pérdidas o contingencias negativas como consecuencia de fallas en contratos y transacciones que pueden afectar el funcionamiento o la condición de una entidad de intermediación financiera, derivadas de error, dolo, negligencia o imprudencia en la concertación, instrumentación, formalización o ejecución de contratos y transacciones. El riesgo legal surge también de incumplimientos de las leyes y/o normas aplicables.

Riesgo operacional: Es la posibilidad de sufrir pérdidas debido a la falta de adecuación o a fallos de los procesos internos, personas o sistemas internos, o bien a causa de acontecimientos externos. Incluye el riesgo legal pero excluye el riesgo estratégico y reputacional.

Seguridad de la información: Son los mecanismos establecidos para garantizar la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella.

TI (Tecnología de Información): Es el conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el hardware, software (aplicaciones, sistemas operativos, sistemas de administración de bases de datos, etc.), redes, multimedia, servicios asociados, entre otros.

Usuario final: Personal que utiliza los recursos de TI con el fin de alcanzar los objetivos de la entidad.

TITULO II
ADMINISTRACION DEL RIESGO OPERACIONAL

CAPITULO I
RESPONSABILIDAD EN LA ADMINISTRACION DEL RIESGO

Artículo 5.- De conformidad con lo dispuesto en el Artículo 55 de la Ley, las entidades de intermediación financiera deben contar con adecuados sistemas de control de riesgo operacional y establecimiento claro y por escrito de sus políticas y procedimientos administrativos.

Artículo 6.- El Consejo de Directores o de Administración de la entidad de intermediación financiera (en lo adelante el Consejo), será responsable de aprobar las políticas y procedimientos idóneos que le permita una adecuada administración del riesgo operacional a que está expuesta dicha entidad, y de velar por su cumplimiento y la Alta Gerencia responsable de su aplicación. Para su establecimiento deberá considerarse la complejidad y volumen de las operaciones que ésta realiza, asegurándose que la alta gerencia implemente las medidas necesarias para monitorear y controlar estos riesgos.

Artículo 7.- Las entidades de intermediación financiera deberán contar con una Unidad o personal responsable de la Administración del Riesgo operacional que puede estar integrado en el Departamento o Unidad de Riesgo que a nivel del banco o Grupo Financiero exista, con funciones bien definidas, asegurándose de que exista la adecuada separación de funciones en los elementos esenciales del proceso de administración del riesgo y la suficiente independencia para evitar potenciales conflictos de interés en la toma de decisiones.

Artículo 8.- El personal asignado para la Administración de Riesgo Operacional será responsable de identificar, analizar, evaluar y monitorear la exposición a riesgos provenientes de los procesos internos, las personas, los eventos externos y la tecnología de información, así como, analizar las políticas y procedimientos de tecnología de información, especialmente aquellas relacionadas con la seguridad de la información y proponer los cambios cuando amerite. También, tendrá la responsabilidad de vigilar y asegurar que las áreas de negocios estén ejecutando correctamente las estrategias, políticas, procesos y procedimientos de administración de dichos riesgos.

Artículo 9.- La Unidad de Auditoría Interna deberá verificar que la entidad mide y controla adecuadamente los riesgos operativos, de conformidad con las políticas y procedimientos establecidos por el Consejo.

CAPITULO II
LINEAMIENTOS PARA EL ESTABLECIMIENTO DE POLITICAS Y PROCEDIMIENTOS

Artículo 10.- Las entidades de intermediación financiera diseñarán un proceso de administración del riesgo que le permita identificar, medir, controlar/mitigar y monitorear sus exposiciones al riesgo operacional en el desarrollo de sus negocios y operaciones. Cada entidad deberá establecer de manera formal su propio enfoque y procedimiento para la gestión del riesgo operacional, considerando su objeto social, tamaño, naturaleza y complejidad de sus operaciones entre otras características. La implementación del sistema de gestión del riesgo operacional deberá considerar todas las etapas de gestión de riesgo, incluyendo la identificación, evaluación, medición, monitoreo y control. Las entidades de intermediación financiera deberán agrupar sus procesos por líneas de negocio, de acuerdo con el procedimiento que hayan establecido de manera formal.

Artículo 11.- Las entidades de intermediación financiera antes de introducir o emprender productos, actividades, procesos y sistemas nuevos, deberán asegurarse que el riesgo operativo inherente a los mismos esté sujeto a procedimientos adecuados de evaluación.

Artículo 12.- Las entidades de intermediación financiera deberán identificar, por línea de negocio, los eventos de riesgo operacional agrupados por tipo y fallas o insuficiencias en los procesos, las personas, la tecnología de información y los eventos externos, tales como:

a) Fraude interno;
b) Fraude externo;
c) Prácticas laborales y seguridad del ambiente de trabajo;
d) Prácticas relacionadas con los clientes, los productos y el negocio;
e) Daños a los activos físicos;
f) Interrupción del negocio por fallas en la tecnología de información; y,
g) Deficiencias en la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros.

Artículo 13.- Una vez identificados los eventos de riesgo operacional y las fallas o insuficiencias en relación con los factores de este riesgo y su incidencia para la entidad, el Consejo de Directores y la Alta Gerencia podrán decidir si el riesgo se debe asumir, compartir, evitar o transferir, reduciendo sus consecuencias y efectos.

La identificación de los eventos de riesgo operacional permitirá al Consejo de Directores y a la Alta Gerencia de la entidad contar con una visión clara de la importancia relativa de los diferentes tipos de exposiciones al riesgo

operacional y su prioridad, con el objeto de alertarlos en la toma de decisiones y acciones, como son, entre otras:

a) Revisar estrategias y políticas;
b) Actualizar o modificar procesos y procedimientos establecidos;
c) Implantar o modificar límites de riesgo;
d) Constituir, incrementar o modificar controles;
e) Implantar planes de contingencias y de continuidad del negocio;
f) Revisar términos de pólizas de seguro contratadas; y,
g) Contratar servicios provistos por terceros; u otros, según corresponda.

Artículo 14.- Las entidades de intermediación financiera deberán conformar una base de datos centralizada, suficiente y de calidad, que permita registrar, ordenar, clasificar y disponer de información sobre los eventos y factores de riesgo operacional; fallas o insuficiencias; clasificados por línea de negocio, determinando la frecuencia con que se repite cada evento y el efecto cuantitativo de pérdida producida, así como cualquier otra información que se considere necesaria y oportuna, para que a futuro puedan estimar las pérdidas esperadas e inesperadas atribuibles a este riesgo.

Artículo 15.- Cada entidad debe contar con la tecnología de información (TI) que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna, segura y confiable; mitigar las interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones.

Artículo 16.- El proceso de evaluación de riesgo debe conducir a una buena selección de tecnología y control de su implementación, e incorporar las evaluaciones específicas para las responsabilidades funcionales, tales como: seguridad, continuidad de negocio, gestión de suplidores, entre otras. Asimismo, deben evaluar las deficiencias de hardware, software, sistemas, aplicaciones y redes, errores de procesamiento u operativos, fallas en procedimientos, capacidades inadecuadas, vulnerabilidad en las redes, controles instalados, seguridad ante ataques intencionales o incidentes de irrupción y acciones fraudulentas, así como defectos en la recuperación de información.

Artículo 17.- Las entidades deberán asignar responsables que se encarguen de definir y autorizar de manera formal los accesos, cambios funcionales a las aplicaciones y monitorear el cumplimiento de los controles establecidos. Asimismo, deberán definir políticas, procesos y procedimientos de tecnología de información bajo estándares generalmente aceptados (COSO, COBIT, ITIL, ISO, CMMI, PMBOK u otros de aceptación general) que garanticen la ejecución de los criterios de control interno relativos a

eficacia, eficiencia y cumplimiento, alineados a los objetivos y actividades de la entidad; debidamente aprobados por el Consejo.

Artículo 18.- Las entidades de intermediación financiera que contraten proveedores de servicios, deberán incluir una cláusula contractual que indique que la proveedora le asegurará a la entidad pistas de auditorías necesarias, de forma que existan pruebas para cualquier acción legal y las mismas deben estar disponibles por el tiempo que exija la Ley. Además de contar con cláusulas que establezcan que la proveedora le garantice como mínimo planes de contingencia y planes de continuidad de los negocios.

Artículo 19.- Las entidades de intermediación financiera deben implementar planes de contingencia y de continuidad, a fin de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción severa del negocio.

Artículo 20. – Las entidades de intermediación financiera que dependan de un mismo controlador o conformen un Grupo Financiero podrán contar con una Unidad de Riesgo que incluya el riesgo operacional a nivel individual y global y deberán adoptar políticas y procedimientos tanto a nivel individual, como a nivel consolidado de sus filiales.

CAPITULO III
CONTROLES INTERNOS

Artículo 21.- Las entidades de intermediación financiera deberán contar con sistemas de control interno adecuados, esto es, políticas, procesos, procedimientos y niveles de control formalmente establecidos y revisados periódicamente. Estos controles deben formar parte integral de las actividades regulares de la entidad para generar respuestas oportunas ante los eventos de riesgo operacional y las fallas o insuficiencias que los originan.

Artículo 22.- Las entidades de intermediación financiera deben contar permanentemente con un esquema organizado de reportes que permitan disponer de información suficiente y adecuada para gestionar el riesgo operacional en forma continua y oportuna. Los reportes deberán contener al menos la información siguiente:

a) Detalles de los eventos de riesgo operacional, agrupados por tipo de evento; las fallas o insuficiencias que los originaron relacionadas con los factores de riesgo operacional, clasificado por línea de negocio; así como las pérdidas originadas por cada evento.

b) Informes de evaluación del grado de cumplimiento de las políticas relacionadas con los factores de riesgo operacional y los procesos y procedimientos establecidos por la entidad; y,

c) Indicadores de gestión que permitan evaluar la eficiencia y eficacia de las políticas, procesos y procedimientos aplicados.

Los informes deben ser dirigidos a las áreas correspondientes de la entidad de manera que puedan ser analizados con una perspectiva de mejora constante del desempeño en la administración del riesgo operacional y establecer o modificar políticas, procesos, procedimientos, entre otros.

TITULO III
FACTORES DE RIESGO OPERACIONAL

Artículo 23.- Los factores de riesgo operacional a los que mayormente se ven expuestas las entidades son: procesos internos, personas, eventos externos y tecnología de información. Es por tanto determinante para un efectivo control de dichos factores, que las entidades cuenten con una definición apropiada de cada uno de estos, para lo cual deberán observar los criterios que se desarrollan en los capítulos que conforman este Título.

CAPITULO I
PROCESOS INTERNOS

Artículo 24.- La administración de los riesgos asociados a los procesos internos que se implemente en las entidades, deberá definirse de conformidad con la estrategia y las políticas adoptadas, de manera que permita minimizar la posibilidad de pérdidas financieras relacionadas al diseño inapropiado de los procesos críticos, o a políticas y procedimientos inadecuados o inexistentes. El mismo deberá considerar los riesgos asociados a las fallas en los modelos utilizados, los errores en las transacciones, la evaluación inadecuada de contratos o de la complejidad de productos, operaciones y servicios, los errores en la información contable, la inadecuada documentación de transacciones, así como el incumplimiento de plazos y costos planeados, entre otros.

Artículo 25.- Las entidades de intermediación financiera deberán contar con políticas escritas relativas al diseño, control, actualización y seguimiento de los procesos. Dichas políticas se referirán, por lo menos, a los aspectos siguientes:

a) Diseño de los procesos, los cuales deben ser adaptables y dinámicos;

b) Descripción en secuencia lógica y ordenada de las actividades, tareas, y controles;

c) Identificación de las personas responsables de ejecutar los procesos para su correcto funcionamiento, a través de establecer medidas y fijar objetivos, garantizando que las metas globales del proceso se cumplan; definir los límites y alcance; mantener contacto con los clientes internos y externos del proceso para asegurar que se satisfagan y conozcan sus expectativas, entre otros.

d) Difusión y comunicación de los procesos; y,

e) Actualización y mejora contínua a través del seguimiento permanente en su aplicación.

Artículo 26.- Las entidades deberán tener una adecuada separación de funciones que eviten incompatibilidades, entendidas éstas como aquellas tareas cuya combinación en las competencias de una sola persona, eventualmente, podría permitir la realización o el ocultamiento de fraudes, errores, omisiones u otros eventos de riesgo operacional.

Artículo 27.- Las entidades deberán mantener inventarios actualizados de los procesos en funcionamiento, los cuales contarán como mínimo con la información siguiente: tipo de proceso, nombre del proceso, responsable, productos y servicios que genera el proceso, clientes internos y externos, fecha de aprobación, fecha de actualización, además deberá indicar si se trata de un proceso crítico.

CAPITULO II
PERSONAS

Artículo 28.- Las entidades deberán definir formalmente políticas, procesos y procedimientos que aseguren una adecuada planificación y administración del capital humano, los cuales considerarán los procesos de incorporación, permanencia y desvinculación del personal al servicio de la entidad. Asimismo, las normas internas deberán identificar apropiadamente las fallas o insuficiencias asociadas al personal, de tal modo que se minimice la posibilidad de pérdidas financieras originadas por: una inadecuada capacitación del personal, negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, lavado de dinero y similares.

Artículo 29.- Las entidades deberán evaluar su organización con el objeto de determinar si se han definido las necesidades de recursos humanos con las competencias idóneas para el desempeño de cada puesto, considerando no sólo experiencia profesional, formación académica, sino también los valores, actitudes y habilidades personales que puedan servir como criterio para garantizar la excelencia institucional.

Artículo 30.- Las entidades mantendrán información actualizada de los recursos humanos, que permita una adecuada toma de decisiones por parte de los niveles directivos y la realización de análisis cualitativos y cuantitativos de acuerdo con sus necesidades. Dicha información deberá referirse al personal existente en la entidad; a la formación académica y experiencia; a la forma y fechas de selección, reclutamiento y contratación; información histórica sobre los eventos de capacitación en los que han participado; cargos que han desempeñado en la entidad; resultados de evaluaciones realizadas; fechas y causas de separación del personal que se ha desvinculado; y, otra información que se considere pertinente.

CAPITULO III
EVENTOS EXTERNOS

Artículo 31.- La administración del riesgo operacional también debe considerar la posibilidad de pérdidas ocasionadas por la ocurrencia de eventos ajenos al control de la entidad, que pudiesen alterar el desarrollo de sus operaciones y tomar en consideración los riesgos que implican las contingencias legales, las fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y otros actos delictivos, así como las fallas en servicios provistos por terceros.

CAPITULO IV
TECNOLOGIA DE INFORMACION (TI)

SECCION I
OBJETIVOS DE CONTROL DE ALTO NIVEL DE TI

Artículo 32.- Planificación y Organización. Las entidades de intermediación financiera deberán contar con estrategias y tácticas de TI que contribuyan al logro de los objetivos del negocio. La visión estratégica debe ser planeada, comunicada y administrada desde diferentes perspectivas, para lo cual se requiere implementar una estructura organizacional y tecnológica apropiada, tomando en cuenta los aspectos siguientes:

a) **Planificación Estratégica.** Tener un plan estratégico de TI para administrar y dirigir los recursos de acuerdo con la estrategia del negocio y sus prioridades. El plan debe identificar las oportunidades y limitaciones de TI, evaluar el desempeño actual y determinar el nivel de inversión requerido. El presupuesto debe estar alineado con la estrategia, la cual deberá ser ejecutada mediante planes y tareas específicas.

b) **Arquitectura de la Información.** Crear y actualizar de forma regular un modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esa información. Esto debe incluir el desarrollo

de un diccionario corporativo de datos que contenga las reglas de sintaxis utilizada en la entidad, el esquema de clasificación y los niveles de seguridad, responsabilidad sobre la integridad de los datos, la efectividad y control de la información compartida a lo largo de las aplicaciones.

c) **Dirección tecnológica.** Determinar la dirección hacia donde se orientará la tecnológica para dar soporte al negocio, mediante la creación de un plan de infraestructura tecnológica que establezca y administre expectativas realistas y claras de lo que la tecnología puede ofrecer en términos de productos, servicios y mecanismos de aplicación. Ese plan debe actualizarse de forma regular y abarcar aspectos tales como arquitectura de sistemas, dirección tecnológica, planes de adquisición, estándares, estrategias de migración y contingencias.

d) **Procesos, organización y relaciones de TI.** La Tecnología de Información deberá estar definida tomando en cuenta los requerimientos de personal, las funciones, delegación, autoridad, roles, responsabilidades y supervisión. Las mismas deberán asegurar la transparencia y el control, así como el involucramiento de los altos ejecutivos y la gerencia del negocio. Deben existir procesos, políticas administrativas y procedimientos para todas las funciones, con atención específica en el control, aseguramiento de la calidad, administración de riesgos, seguridad de la información, propiedad de los datos, sistemas y la segregación de tareas.

e) **Administración de la inversión de TI.** Establecer un marco de trabajo para administrar los programas de inversión en TI que abarquen costos, beneficios y prioridades dentro del presupuesto e identificar y controlar los costos y beneficios totales dentro del contexto de los planes estratégicos y tácticos de TI, y tomar medidas correctivas según sean necesarias.

f) **Comunicación de las acciones y dirección de la gerencia.** Construir un marco de trabajo de control institucional para TI, definir y comunicar las políticas. Un programa de comunicación continua se debe implantar para articular la misión, los objetivos de servicio, las políticas y procedimientos, etc., aprobados y apoyados por la dirección.

g) **Administración de los recursos humanos de TI.** Las entidades sujetas a supervisión deberán contratar, mantener y motivar al personal para la creación y entrega de servicios de TI, mediante prácticas definidas y aprobadas que apoyen el reclutamiento, entrenamiento, la evaluación del desempeño, la promoción y la terminación.

h) **Administración de la calidad.** Construir y mantener un sistema de administración de la calidad, que incluya procesos y estándares probados

de adquisición y desarrollo. Los requerimientos de calidad se deben manifestar y documentar con indicadores cuantificables y alcanzables; e,

i) **Administración de proyectos.** Establecer programas y marco de controles administrativos de proyectos de TI que garanticen la correcta asignación de prioridades y la coordinación de esos proyectos. Además deberán incluir un plan maestro con asignación de recursos, definición de entregables, aprobación de los usuarios, una guía de entrega por fases, aseguramiento de la calidad, un plan formal de pruebas, revisión de pruebas y revisión post-implantación para garantizar la administración de los riesgos del proyecto y la entrega de valor al negocio.

Artículo 33.- Adquisición e implementación. Las entidades supervisadas deberán llevar a cabo las estrategias de TI mediante soluciones que necesitan ser identificadas, desarrolladas o adquiridas, así como la implementación e integración en los procesos del negocio. Además, los cambios y mantenimientos de los sistemas existentes deberán garantizar que las soluciones sigan satisfaciendo los objetivos del negocio, en cuanto a:

a) **Adquisición de recursos de TI.** Definir y ejecutar estándares, políticas y procedimientos para la adquisición, selección y arreglos contractuales con proveedores para garantizar que los recursos de TI se obtengan de manera legal, oportuna y rentable; y,

b) **Administración del cambio.** Los cambios, incluyendo el mantenimiento de emergencia y parches, relacionados con la infraestructura y las aplicaciones dentro del ambiente de producción, deberán administrarse formal y controladamente. Los cambios (incluyendo procedimientos, procesos, sistema y parámetros del servicio) se deben registrar, evaluar y autorizar previamente a la implementación y revisar contra los resultados planeados.

Artículo 34.- Entrega y soporte. Las entidades de intermediación financiera que provean servicios de TI deberán tomar en cuenta, la prestación del servicio, administración de la seguridad y la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales. Específicamente, deberán:

a) **Administración de niveles de servicio.** Contar con definiciones documentadas de los acuerdos de niveles de servicios de TI, que hagan posible una comunicación efectiva entre la gerencia de TI y los clientes de negocio respecto de los servicios requeridos. Además, deberán monitorear el cumplimiento de los niveles de servicio para verificar la alineación entre los servicios de TI y los requerimientos del negocio.

b) **Administración de servicios de terceros.** Los acuerdos de servicios con terceras partes deberán estar formalizados mediante contrato, donde se definan claramente los roles, responsabilidades y expectativas, así como la revisión y monitoreo de la efectividad y cumplimiento de dichos acuerdos.

c) **Administración del desempeño y capacidad.** El desempeño y capacidades de los recursos de TI deben ser monitoreados y revisados periódicamente. Además, anualmente debe realizarse el pronóstico de las necesidades futuras, basado en los requerimientos de carga de trabajo, almacenamiento y contingencias.

d) **Continuidad de los servicios.** Desarrollar, mantener y probar los planes de continuidad de TI, almacenar respaldos fuera de la instalación y entrenar al personal de forma periódica sobre los planes de continuidad y revisar anualmente la cobertura y necesidades de seguro para TI.

e) **Seguridad de los sistemas.** Mantener la integridad de la información y proteger los activos de TI, mediante un proceso de administración de seguridad. Este deberá incluir el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. Además, deberán realizar monitoreo de seguridad y pruebas periódicas así como ejecutar las acciones correctivas sobre las debilidades o incidentes de seguridad identificados.

f) **Entrenamiento a los usuarios.** Proveer una educación efectiva a todos los usuarios de sistemas de TI, para lo cual deberán identificar las necesidades y elaborar un plan de entrenamiento para cada grupo de usuarios.

g) **Administración de la configuración.** Garantizar la integridad de las configuraciones de hardware y software, mediante el establecimiento y mantenimiento de un repositorio de configuraciones completo y preciso.

h) **Administración de problemas.** Manejar de forma efectiva la administración de problemas e incidentes. Este proceso requiere la identificación, clasificación, análisis de las causas desde su raíz, y la resolución de los mismos. Además, incluye la identificación de recomendaciones para la mejora, el mantenimiento de registros de problemas y la revisión del estatus de las acciones correctivas.

i) **Administración de los datos.** Contar con una efectiva administración de datos que identifique de forma efectiva los requerimientos de datos. El proceso de administración de información también debe incluir el establecimiento de procedimientos efectivos para administrar la librería

de medios, el respaldo y la recuperación de datos y la eliminación apropiada de medios; y,

j) **Administración del ambiente físico.** Velar por la protección de los equipos de cómputo y del personal. Las instalaciones deben estar bien diseñadas y administradas. El proceso de administración del ambiente físico incluye la definición de los requerimientos del centro de datos, la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso.

Artículo 35.- Monitoreo y Evaluación. Los procesos de TI tienen que evaluarse de forma regular en cuanto a su calidad y cumplimiento de los requerimientos de control. En ese sentido, las entidades deberán establecer un programa de control interno efectivo para TI que incluya un proceso bien definido de monitoreo. Además, deberán incluir las excepciones de control, resultados de las autoevaluaciones y revisiones por parte de auditores de sistemas.

Párrafo: Las áreas de auditoría interna de sistemas de información (ASI) y/o tecnología de información (ATI), incluyendo las contratadas de forma externa (Outsourced) y las firmas de auditores externos que brinden estos servicios, deberían contar con personal certificado en ASI y/o ATI, por lo menos con una entidad reconocida internacionalmente.

TITULO IV
SUPERVISION DEL RIESGO OPERACIONAL

Artículo 36.- El ciclo de supervisión de las entidades de intermediación financiera que realiza la Superintendencia de Bancos deberá incluir una revisión de la gestión del riesgo operacional de acuerdo con la metodología de evaluación establecida por la propia Superintendencia. Esta revisión podrá ser realizada con mayor o menor frecuencia dependiendo del resultado de la evaluación.

Párrafo I: La entidad que subcontrate una parte o la totalidad de su procesamiento de datos, y otros servicios, deberá incluir en los contratos que suscriba, una cláusula que permita a la Superintendencia de Bancos la revisión de los procesos tercerizados en el proveedor del servicio.

Párrafo II: La Superintendencia de Bancos podrá objetar la tercerización de procesos cuando no cumplan con la normativa vigente establecida por la Administración Monetaria y Financiera.

TITULO V
DE LA NOTIFICACIÓN PREVIA

Artículo 37.- Las entidades de intermediación financiera deberán notificar previamente y por escrito a la Superintendencia de Bancos, cuando se presente cualquiera de las siguientes situaciones:

a) La instalación y/o implementación de centros de procesamientos de datos y accesos externos a los sistemas de la entidad;

b) La tercerización de servicios críticos, tales como, procesamiento de datos, hosting, telecomunicaciones, entre otros;

c) La descentralización total o parcial del procesamiento de datos fuera del país;

d) Implementación de nuevos sistemas o tecnologías desde la última inspección;

e) Cambios significativos en los recursos humanos, tales como gerentes de tecnología, auditoría y seguridad o conversión de sistemas; y,

f) Cambios en las líneas de negocios en las cuales los controles internos y el sistema de manejo de riesgo, dependan fuertemente de la TI.

TITULO VI
REQUERIMIENTOS DE INFORMACION

Artículo 38.- Las entidades de intermediación financiera deberán en un plazo de un (1) año, contado a partir de la fecha de publicación del presente Reglamento, remitir un plan sobre la implementación de los lineamientos establecidos en este Reglamento, debidamente aprobado por el Consejo, el cual incluirá el programa a ejecutar y las personas responsables del mismo.

Artículo 39.- Las entidades deberán presentar a la Superintendencia de Bancos por medios magnéticos o CD, dentro de los cuarenta y cinco (45) días calendario siguientes al corte de cada semestre, 30 de junio y 31 de diciembre, un informe referido a la evaluación del riesgo operacional que enfrenta la entidad por proceso o unidad de negocio y apoyo. Dicho informe deberá contemplar por lo menos los siguientes aspectos:

a) Metodología empleada para la administración del riesgo operacional;

b) Identificación del riesgo operacional a que está expuesta la entidad por proceso o unidad de negocio y apoyo;

c) Descripción de los riesgos que enfrenta la entidad;

d) Evaluación de los riesgos de operación identificados;

e) Medidas adoptadas para administrar el riesgo operacional material identificado y plazos para su aplicación. Dichas medidas deberán referirse por lo menos a los aspectos siguientes:

- Evitar el riesgo
- Reducir su probabilidad de ocurrencia
- Reducir las consecuencias
- Transferir el riesgo
- Retener el riesgo

f) Funcionarios responsables de las actividades de control de riesgo identificadas; y,

g) Plan de actividades de los responsables de la administración del riesgo operacional.

Artículo 40.- La Superintendencia de Bancos podrá requerir a las entidades, cualquiera otra información que considere necesaria para una adecuada supervisión del riesgo operacional.

Artículo 41.- La entidad deberá tener a disposición de la Superintendencia de Bancos todos los documentos necesarios para la evaluación del riesgo operacional, así como la información de auditoría o revisiones realizadas por la casa matriz, en caso de que ésta no se encuentre en el país.

TITULO VII
REQUERIMIENTO DE CAPITAL POR RIESGO OPERACIONAL

Artículo 42.- Como una forma de ir depurando el proceso para la determinación del requerimiento de capital por riesgo operacional, las entidades de intermediación financiera deberán utilizar el Método Estándar establecido en Basilea II.

A tal fin, la Superintendencia de Bancos, en un plazo de noventa (90) días calendario, contados a partir de la fecha de publicación del presente Reglamento, deberá elaborar un instructivo a fin de establecer las informaciones que las entidades deberán remitir a este Organismo, así como el formato, periodicidad y el medio en que serán remitidas para cuantificar la exposición del Riesgo Operacional.

Artículo 43.- La Superintendencia de Bancos, al término de veinticuatro (24) meses contado a partir de la entrada en vigencia del presente Reglamento, y luego de evaluar las informaciones remitidas por las entidades, podrá proponer a la Junta Monetaria el requerimiento de capital obligatorio por concepto de riesgo operacional, conforme a las mejores prácticas internacionales sobre la materia.

Párrafo I: Establecido el requerimiento de capital, las entidades deberán remitir a la Superintendencia de Bancos los resultados de la medición del riesgo operacional a que están expuestas, conforme a la metodología que se establezca.

Párrafo II: Las entidades de intermediación financiera deberán divulgar información correspondiente a la gestión del riesgo operacional según le sea requerida por la Superintendencia de Bancos, de forma que los usuarios puedan determinar si la entidad identifica, evalúa, monitorea y controla / mitiga efectivamente este riesgo.

Artículo 44.- La Superintendencia de Bancos remitirá mensualmente al Banco Central un reporte sobre los resultados de la medición del riesgo operacional, así como cualquier otra información relativa al presente Reglamento que sea de interés para el Banco Central.

TITULO VIII
DISPOSICIONES FINALES

Artículo 45.- Las entidades de intermediación financiera que infrinjan las disposiciones contenidas en el presente Reglamento, se harán pasibles de la aplicación de las sanciones establecidas en la Ley Monetaria y Financiera No. 183-02 y su Reglamento de aplicación.

Artículo 46.- Entrada en Vigencia. El presente Reglamento entrará en vigencia a partir de su promulgación.**”**

14 de abril del 2009

-END-