Enlace a Legislación Relacionada

NORMA SOBRE GESTIÓN DE RIESGO OPERACIONAL

RESOLUCIÓN N°. CD-SIBOIF-611-1-ENE22-2010, aprobada el 22 de enero de 2010

Publicada en La Gaceta, Diario Oficial N°. 64 del 08 de abril de 2010

El Consejo Directivo de la Superintendencia de Bancos y de Otras Instituciones Financieras,

CONSIDERANDO

I

Que el artículo 38, numeral 4), de la Ley General de Bancos, referente a las obligaciones de la junta directiva de las instituciones financieras, señala que, esta última, tiene entre sus responsabilidades el "velar porque se implementen e instruir para que se mantengan en adecuado funcionamiento y ejecución, las políticas, sistemas y procesos que sean necesarios para una correcta administración, evaluación y control de los riesgos inherentes al negocio", estableciendo dicho artículo la facultad del Consejo Directivo de dictar normas sobre esta materia.

II

Que el artículo 40, numerales 6) y 10) de la Ley No. 561, Ley General de Bancos, Instituciones Financieras no Bancarias y Grupos Financieros, publicada en La Gaceta, Diario Oficial No. 232, del 30 de noviembre de 2005, en sus partes conducentes establece que los preceptos que regulan el gobierno corporativo de las instituciones financieras, deben incluir, entre otros, políticas sobre procesos integrales que incluyan la administración de los diversos riesgos a que pueda estar expuesta la institución, establecimiento de sistemas de información adecuados, así como políticas escritas sobre la administración de los diferentes riesgos.

III

Que de acuerdo a lo antes expuesto y con base a las facultades establecidas en el artículo 3, numeral 13), y artículo 10, incisos 1), 2) y 3) de la Ley N° 316, Ley de la Superintendencia de Bancos y de Otras Instituciones Financieras y sus reformas.

En uso de sus facultades

HA DICTADO

La siguiente:

CD-SIBOIF-611-1-ENE22-2010
NORMA SOBRE GESTIÓN DE RIESGO OPERACIONAL

TÍTULO I
DISPOSICIONES GENERALES

CAPÍTULO ÚNICO
CONCEPTOS, OBJETO Y ALCANCE

Artículo 1. Conceptos.- Para los fines de la presente norma, los términos indicados en este artículo, tanto en mayúsculas como en minúsculas, singular o plural, tendrán los significados siguientes:

a) Análisis de impacto en el negocio: Es un componente de la gestión de continuidad del negocio. Es el proceso de identificar y medir (cuantitativa y cualitativamente) el impacto o pérdida de los procesos del negocio en el caso de una interrupción. Es utilizado para identificar los aspectos prioritarios para la recuperación, los requisitos de recursos para la recuperación, el personal esencial y para ayudar a darle forma al plan de continuidad del negocio.

b) Continuidad del negocio: Estado continuo e ininterrumpido de operación de un negocio.

Factores de riesgo operacional: Se refiere a las fuentes generadoras de eventos en las que se originan las pérdidas

por riesgo operacional a nivel de la actividad o líneas de negocios, entre los cuales se encuentran: procesos internos, personas, eventos externos y tecnología de información**.**

e) Gestión de riesgos: El conjunto de objetivos, políticas, procedimientos y acciones que se implementan para identificar, medir, monitorear, limitar, controlar, informar y revelar los distintos tipos de riesgo a que se encuentran expuestas las instituciones.

f) Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios, susceptible de ser procesada, distribuida y almacenada.

g) Institución o Institución Financiera: Se refiere a los bancos y sociedades financieras que de acuerdo a la Ley General de Bancos pueden captar depósitos del público. Incluye a las sucursales de bancos y sociedades financieras extranjeras establecidas en el país.

h) Interrupción operacional mayor: Interrupción significativa en las operaciones normales de la institución, que afecta un área geográfica y las comunidades adyacentes económicamente integradas con ella. Las interrupciones operacionales mayores pueden ser el resultado de una amplia gama de eventos, tales como: terremotos, huracanes y otros eventos relacionados con el clima, ataques terroristas, asonadas, virus informáticos, epidemias, pandemias y otros incidentes biológicos y otros actos intencionales o accidentales que pueden causar daños generalizados, directos o indirectos, a la infraestructura física.

i) Ley General de Bancos: Ley 561, Ley General de Bancos, Instituciones Financieras no Bancarias y Grupos Financieros, publicada en la Gaceta Diario Oficial N° 232, del 30 de noviembre de 2005.

j) Mejores Prácticas Aplicables: Se refiere a los marcos de referencia de control, estándares internacionales u otros estudios que ayuden a monitorear y mejorar las actividades críticas, aumentar el valor de negocio, y reducir riesgos, tales como; recomendaciones del Comité de Basilea, COSO, COBIT, ITIL, ISO 17799, ISO 9001, CMM y PRINCE2, entre otros.

k) Nivel de recuperación: Es el nivel de servicio a ser proveído con respecto a operaciones de negocios específicas después de una interrupción.

l) Objetivo de recuperación: Meta predefinida para la recuperación de operaciones específicas de negocios y sistemas de soportes a un nivel determinado de funcionamiento (nivel de recuperación) dentro de un periodo de tiempo definido después de ocurrida una interrupción.

m) Plan de continuidad del negocio: Un componente de la gestión de continuidad del negocio. Es un plan de acción detallado que establece los procedimientos y sistemas necesarios por línea de negocio para continuar o reestablecer las operaciones de una institución en el evento de una interrupción.

n) Políticas: Conjunto de prácticas establecidas por la junta directiva de la institución, por medio de las cuales se definen los cursos de acción a seguir por la administración.

o) Procedimiento: Método o sistema estructurado para ejecutar instrucciones. Lista detallada de la secuencia lógica y consistente de actividades y cursos de acción, por medio de las cuales se asegura el cumplimiento de una función operativa.

p) Proceso: Conjunto de actividades, tareas y procedimientos organizados y repetibles.

q) Proceso crítico: Proceso considerado indispensable para la continuidad de las operaciones y servicios de la institución, cuya falta o ejecución deficiente puede tener un impacto significativo para la institución

r) Recuperación: La restauración de operaciones especificas del negocio a un nivel suficiente para cumplir con las obligaciones de la institución, después de ocurrida una interrupción.

s) Resistencia: La capacidad de una institución financiera para absorber el impacto de una interrupción operacional mayor y continuar proveyendo operaciones y servicios críticos.

t) Riesgo: Es la posibilidad de que se produzca un hecho generador de pérdidas que afecten el valor económico de las instituciones.

u) Riesgo Legal: Pérdida potencial por el incumplimiento de las disposiciones legales y administrativas aplicables, la

afectación por resoluciones administrativas o judiciales desfavorables y la aplicación de sanciones, en relación con las operaciones que las instituciones llevan a cabo.

v) Riesgo de Tecnología de Información: Daño, interrupción, alteración o fallas derivadas del uso de la TI que soporta los procesos críticos de la Institución y que conlleve a una pérdida potencial.

w) Riesgo Operacional: Es el riesgo de pérdidas resultantes de la falta de adecuación o fallas en los procesos internos, las personas o los sistemas o por eventos externos. Esta definición incluye al riesgo legal y tecnológico, pero excluye el riesgo estratégico y reputacional.

x) Servicios críticos provistos por terceros: Servicios relacionados a procesos críticos provistos por terceros, cuya falta o ejecución deficiente puede tener un impacto financiero significativo para la institución.

y) Sitio alterno: Lugar habilitado para ser usado durante una interrupción, con el fin de mantener la continuidad del negocio de una institución. El término aplica tanto a espacio físico, como a requerimientos tecnológicos, localizado en un lugar distinto al lugar primario de negocios afectado. Las instituciones pueden contar con más de un sitio alterno. En algunos casos, un sitio alterno puede estar constituido por la infraestructura utilizada en las operaciones normales diarias de la institución pero con la capacidad para acomodar funciones adicionales de negocios cuando el lugar primario de negocios se vea afectado.

z) Superintendencia: Superintendencia de Bancos y de Otras Instituciones Financieras

aa) Superintendente: Superintendente de Bancos y de Otras Instituciones Financieras.

bb) Tecnología de información (TI): Conjunto de recursos necesarios para procesar la información, convertirla, almacenarla, administrarla, transmitirla y encontrarla, tales como: Hardware, Software, Sistemas de Información, Investigación Tecnológica, Redes Locales, Bases de Datos, Ingeniería de Software, Telecomunicaciones, Servicios y Organización de Informática.

cc) Tiempo de recuperación: Es el periodo de tiempo en que se espera restablecer una operación de negocios específica. El tiempo de recuperación tiene dos componentes: el lapso entre la interrupción y la activación del plan de continuidad del negocio; y el lapso entre la activación del plan de continuidad del negocio y la recuperación de una actividad específica del negocio.

dd) Unidad de negocio: Las áreas originadoras y tomadoras de riesgos discrecionales al interior de las instituciones.

ee) UAIR: Unidad de Administración Integral de Riesgos establecida en la normativa que regula la materia sobre la administración integral de riesgos.

Artículo 2. Objeto.- La presente norma tiene por objeto establecer las responsabilidades y lineamientos generales a seguir por las instituciones financieras para una adecuada gestión del riesgo operacional, a fin de controlar o mitigar el posible impacto negativo de dicho riesgo. Asimismo, tiene por objeto establecer criterios especiales a tomar en cuenta para mantener en dichas instituciones un efectivo control de los principales factores de riesgo operacional a los que pueden estar expuestas.

Artículo 3. Alcance.- Las disposiciones de la presente norma son aplicables a las instituciones financieras sujetas a la autorización, supervisión y vigilancia de la Superintendencia.

TÍTULO II
GESTIÓN DEL RIESGO OPERACIONAL

CAPÍTULO I
RESPONSABILIDADES EN LA GESTIÓN DEL RIESGO

Artículo 4. Sistema de gestión de riesgo.- Las instituciones financieras deberán contar con un sistema de gestión de riesgo que les permita identificar, medir, controlar, mitigar y monitorear su exposición al riesgo operacional en el desarrollo de sus negocios y operaciones. Cada institución deberá establecer de manera formal sus propios controles y procedimientos para la gestión de dicho riesgo, considerando, entre otros elementos, su objeto social, tamaño, naturaleza y complejidad de las operaciones. La implementación de este sistema deberá tomar en cuenta todas las etapas de gestión del riesgo, agrupando los procesos por líneas de negocio, de acuerdo con el procedimiento que hayan establecido de manera formal.

Artículo 5. Responsabilidades de la junta directiva en la gestión del riesgo.- La junta directiva de la institución financiera será responsable de aprobar los objetivos, lineamientos y políticas que le permitan realizar una adecuada gestión del riesgo operacional al que está expuesta la institución. Asimismo, será su responsabilidad velar por el cumplimiento de dichos objetivos, lineamientos y políticas, los cuales deberán ser implementados por la alta gerencia de la institución.

Los objetivos, lineamientos y políticas antes mencionados deberán estar claramente definidos en los manuales previstos en el artículo siguiente, los cuales deberán ser consistentes con el tamaño y naturaleza de la institución y con la complejidad y volumen de sus operaciones y servicios.

Artículo 6. Manuales para la gestión del riesgo.- Los objetivos, lineamientos y políticas antes indicadas deberán constar en manuales que servirán como soporte funcional y operativo al proceso de gestión del riesgo operacional. De manera general, estos manuales deberán ser documentos técnicos que contengan, entre otros, los diagramas de flujo de información, modelos y metodologías para la evaluación de este tipo de riesgo, así como, los requerimientos de los sistemas de procesamiento de información y análisis de riesgos. Las juntas directivas deberán aprobar, al menos, los manuales siguientes:

a) Manual de Políticas y Procedimientos: Contiene las políticas y procedimientos establecidos por la institución para la identificación, medición, control, adecuación, seguimiento y administración de todos los riesgos a los que está expuesta; así como, de las acciones correctivas a ser implementadas y del seguimiento de las instrucciones impartidas, según sea el caso. Contempla, entre otros, los sistemas preventivos para detectar los riesgos a que pudiese estar expuesta la institución y los mecanismos de vigilancia a los fines de no exceder los límites por riesgo para las actividades u operaciones que ésta realiza; así como, los mecanismos dispuestos para elaborar e intercambiar información, tanto interna como externa y las acciones previstas para la difusión de las actividades que corresponden a los diferentes niveles directivos y al personal sobre el control de sus tareas.

b) Manual de organización y descripción de funciones: Detalla la organización funcional de la institución, así como, las funciones, cargos y responsabilidades de los funcionarios en todos sus niveles.

c) Manual de Control de Riesgo Operacional: El manual deberá contemplar una definición clara de riesgo operacional y establecer los principios para su identificación, evaluación, monitoreo, control y mitigación. Asimismo, el manual de control de riesgos deberá contener una sección especial sobre el riesgo operacional. Sin perjuicio de lo establecido en el literal a) del presente artículo, dicha sección deberá contener, al menos, los siguientes aspectos:

1) Políticas para la administración del riesgo operacional;

2) Funciones y responsabilidades de la unidad responsable del control y análisis del riesgo operacional; así como, de las unidades de negocio y de apoyo en la administración de dicho riesgo;

3) Descripción de la metodología aplicada para la medición y evaluación del .riesgo operacional;

4) La forma y periodicidad con la que se deberá informar a la junta directiva y a la alta gerencia, entre otros, sobre la exposición al riesgo operacional de la institución y de cada unidad de negocio; y

5) El proceso para la aprobación de propuestas de nuevas operaciones, productos y servicios que deberá contar, entre otros aspectos, con una descripción general de la nueva operación, producto o servicio de que se trate, los riesgos identificados y las acciones a tomar para su control.

Artículo 7. Unidad responsable de la gestión del riesgo.- La unidad responsable del control y análisis del riesgo operacional en las instituciones financieras es la UAIR a la que se refiere la normativa que regula la materia sobre administración integral de riesgo y tendrá las funciones y responsabilidades establecidas tanto en la presente norma, como en la normativa antes referida.
La UAIR para dar cumplimiento a las funciones indicadas en la presente norma podrá auxiliarse en las áreas o instancias que estime conveniente, siempre y cuando, exista independencia entre las áreas tomadoras de riesgos y la UAIR.

CAPÍTULO II
LINEAMIENTOS GENERALES PARA GESTIONAR EL RIESGO OPERACIONAL

Artículo 8. Lineamientos generales.- Las instituciones financieras deberán tomar en cuenta los siguientes lineamientos generales mínimos en el establecimiento de sus objetivos, políticas y procedimientos para gestionar el riesgo operacional:

a) Identificación de eventos generadores de riesgos: Las instituciones financieras 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, entre otros:

1) Fraude interno;
2) Fraude externo;
3) Prácticas laborales y seguridad del ambiente de trabajo;
4) Prácticas relacionadas con los clientes, los productos y el negocio;
5) Interrupción del negocio por fallas en la tecnología de información; y
6) Deficiencias en la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros.

b) Implementación de acciones: 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 institución, la junta directiva y la alta gerencia deberán decidir si el riesgo lo aceptan, comparten, evitan o transfieren, reduciendo sus consecuencias y efectos, para lo cual deberán adoptar, entre otras, las siguientes acciones:

1) Revisar estrategias y políticas;
2) Actualizar o modificar procesos y procedimientos establecidos;
3) Implantar o modificar límites de riesgo;
4) Constituir, incrementar o modificar controles;
5) Implantar planes de contingencias y de continuidad del negocio;
6) Revisar términos de pólizas de seguro contratadas; y,
7) Contratar servicios provistos por terceros, u otros, según corresponda

c) Conformación de base de datos: Las instituciones financieras deberán conformar una base de datos centralizada 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, según la normativa que regule esta materia.

d) Tecnología de información: Cada institución debe contar con 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.

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. Lo anterior de conformidad con lo establecido en la normativa que regula la materia sobre gestión de riesgo tecnológico.

e) Generación de reportes: Las instituciones financieras deberán 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 siguiente información:

1) 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.

2) Informes de evaluación por parte de la auditoría interna con respecto del grado de cumplimiento de las políticas relacionadas con los factores de riesgo operacional y los procesos y procedimientos establecidos por la institución; e

3) 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 institución 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.

f) **Mejores prácticas aplicables:** Las instituciones financieras 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 bajo las mejores prácticas aplicables que garanticen la ejecución de los criterios de control interno relativos a eficacia, eficiencia y cumplimiento de éstos, alineados a los objetivos y actividades de la institución, los cuales deberán ser aprobados por la junta directiva.

g) Evaluación previa de nuevos productos, actividades, procesos y sistemas: Las instituciones financieras antes de lanzar o emprender nuevos productos, actividades, procesos o sistemas, deberán asegurarse que el riesgo

h) Subcontratación de servicios: Cuando ciertas funciones o procesos puedan ser objeto de una subcontratación o tercerización, la institución deberá proceder conforme la normativa que regula la materia sobre la contratación de proveedores de servicios.

i) Gestión efectiva de la continuidad del negocio: La gestión efectiva de la continuidad del negocio es un componente importante de la administración del riesgo operacional. Es un enfoque que enmarca todas las operaciones de negocios de la institución, e incluye las políticas y procedimientos para asegurarse que operaciones específicas puedan ser mantenidas o recuperadas de manera oportuna en caso de una interrupción. Esta gestión tiene como propósito minimizar las consecuencias operacionales, financieras, legales, reputacionales y otras consecuencias materiales originadas por una interrupción de servicios.

Para la implementación de una gestión efectiva de la continuidad del negocio, las instituciones financieras deben tomar en cuenta los elementos y principios básicos establecidos en el Anexo de la presente norma, el cual es parte integrante de la misma.

CAPÍTULO III
CONTROLES INTERNOS

Artículo 9. Sistema de control interno.- Las instituciones financieras deberán contar con un sistema de control interno que cumpla con los requerimientos establecidos en la presente norma y en la normativa que regula la materia sobre control y auditoría interna. Dicho sistema debe estar enfocado en proveer una seguridad razonable en la salvaguarda de los activos de la institución y a lograr una adecuada organización administrativa y eficiencia operativa; confiabilidad de los reportes que fluyen de sus sistemas de información; apropiada identificación y administración de los riesgos que enfrenta; y cumplimiento de las disposiciones legales que le son aplicables.

Todo sistema de control interno implementado por las instituciones financieras deberá estar basado en los siguientes componentes:

a) Entorno de Control: Las instituciones deben tomar en cuenta, entre otros, elementos relacionados con: la integridad, los valores éticos, la capacidad de los empleados, la filosofía de la institución, el estilo de gestión, la asignación de la autoridad y sus responsabilidades, la organización y desarrollo de los empleados y las orientaciones de la junta directiva.

b) Evaluación de los Riesgos: Las instituciones deben identificar primeramente los objetivos organizacionales y, posteriormente, identificar y evaluar los riesgos relevantes que puedan afectarle alcanzar dichos objetivos. Los riesgos deben ser administrados, atendiendo a la existencia de un medio interno y externo cambiante.

c) Actividades de Control: Son las políticas y procedimientos que ayudan a asegurar que se toman las medidas para limitar los riesgos que pueden afectar que se alcancen los objetivos organizacionales. Entre otras actividades están las siguientes: autorizaciones, verificaciones, conciliaciones, segregación de funciones y revisiones de rentabilidad operativa.

d) Información y **Comunicación:** Se debe identificar, ordenar y comunicar en forma oportuna la información necesaria para que los empleados de la institución puedan cumplir con sus obligaciones. Dicha información puede ser operativa o financiera, de origen interno o externo; y las instituciones deben asegurar la existencia de adecuados canales de comunicación entre el personal, el cual debe estar informado de la importancia de su participación en el esfuerzo de aplicar el control interno.

e) Supervisión: Las instituciones financieras deben implementar procesos que conlleven realizar actividades de supervisión continua, evaluaciones periódicas o una combinación de ambas, para comprobar que sus sistemas de control interno se mantienen funcionando adecuadamente.

TÍTULO III
FACTORES DE RIESGO OPERACIONAL

Artículo 10. Factores de riesgo operacional.- Los factores de riesgo operacional a los que mayormente se ven expuestas las instituciones financieras son los siguientes:

a) Procesos internos;
b) Personas;
c) Eventos externos; y
d) Tecnología de información.

Es determinante para un efectivo control de dichos factores, que las instituciones financieras 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 el presente Título.

CAPÍTULO I
PROCESOS INTERNOS

Artículo 11. Gestión de riesgos asociados a procesos internos.- Las instituciones financieras deberán gestionar apropiadamente los riesgos asociados a los procesos internos implementados para la realización de sus operaciones y servicios, de tal forma que se minimice la posibilidad de pérdidas relacionadas al diseño inapropiado de los procesos, o a políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos.

En tal sentido, podrán considerarse entre otros, los riesgos asociados a las fallas en los procesos y/o 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 compensación, liquidación o pago; la insuficiencia de recursos para el volumen de operaciones; la inadecuada documentación de transacciones; así como, el incumplimiento de plazos y costos planeados.

Artículo 12. Desarrollo de políticas.- Las instituciones financieras deberán contar con políticas escritas relativas al diseño, control, actualización y seguimiento de los procesos. Dichas políticas se referirán, al 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 continúa a través del seguimiento permanente en su aplicación.

Artículo 13. Segregación de funciones.- Las instituciones financieras deberán tener una adecuada segregación 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 14. Inventarios.- Las instituciones financieras 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, así como, deberá indicar si se trata de un proceso critico

CAPÍTULO II
PERSONAS

Artículo 15. Gestión de riesgos asociados a personas.- Las instituciones financieras deberán gestionar apropiadamente los riesgos asociados a las personas de la institución, de tal modo que se minimice la posibilidad de pérdidas asociadas a inadecuada capacitación del personal, negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, lavado de dinero y similares.

Las instituciones 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 la experiencia profesional y la formación académica, sino también los valores, actitudes y habilidades personales que

puedan servir como criterio para garantizar la excelencia institucional.

Asimismo, las instituciones deberán mantener 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 institución; a la formación académica y experiencia; a la forma y fechas de selección, reclutamiento y contratación; a información histórica sobre los eventos de capacitación en los que han participado; a los cargos que han desempeñado en la entidad; a los resultados de evaluaciones realizadas; a las fechas y causas de separación del personal que se ha desvinculado; y, á cualquier otra información que se considere pertinente.

CAPÍTULO III
EVENTOS EXTERNOS

Artículo 16. Gestión de riesgos asociados a eventos externos.- Las instituciones financieras deberán tomar en cuenta en la gestión del riesgo operacional la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos al control de la institución que pudiesen alterar el desarrollo de sus actividades, afectando los aspectos que dan origen al riesgo operacional referidos en los artículos precedentes. En tal sentido, entre otros eventos, se podrán tomar en consideración los siguientes:

a) Las contingencias legales;
b) Las fallas en los servicios públicos;
c) La ocurrencia de desastres naturales, atentados y actos delictivos; y
d) Las fallas en servicios críticos provistos por terceros.

CAPÍTULO IV
TECNOLOGÍA DE INFORMACIÓN

Artículo 17. Gestión de riesgos asociados a tecnología de información.- Las instituciones financieras deberán gestionar los riesgos asociados a TI, cumpliendo los requerimientos establecidos en la presente norma, en la normativa que regula la materia sobre administración integral de riesgos y en la normativa sobre gestión de riesgo tecnológico.

TÍTULO IV
DISPOSICIONES FINALES

CAPÍTULO ÚNICO
TRANSITORIOS, FACULTAD DEL SUPERINTENDENTE Y VIGENCIA

Artículo 18. Transitorios.- Se establecen las siguientes disposiciones transitorias:

a) Las instituciones financieras tendrán hasta el 31 de julio de 2010 para adecuarse a los requerimientos establecidos en la presente norma.

b) Las instituciones financieras deberán remitir al Superintendente a más tardar dentro de los sesenta (60) días posteriores a la entrada en vigencia de la presente norma, un plan de adecuación a las disposiciones contenidas en la misma. Dicho plan deberá incluir un diagnóstico preliminar de la situación actual de la institución que refleje su grado de avance en el cumplimiento de los requerimientos establecidos en la norma, las acciones previstas' para la total adecuación y el cronograma de las mismas; así como, los funcionarios responsables del cumplimiento de dicho plan.

Artículo 19. Facultad del Superintendente.- Se faculta al Superintendente a prorrogar de manera individual los plazos establecidos en el artículo anterior, en base a solicitud debidamente justificada y sustentada por parte de la institución financiera interesada.

Artículo 20. Vigencia.- La presente norma entrará en vigencia a partir de su notificación, sin perjuicio de su posterior publicación en La Gaceta, Diario Oficial.

ANEXO

ELEMENTOS Y PRINCIPIOS BÁSICOS PARA LA GESTIÓN EFECTIVA DE LA CONTINUIDAD DEL NEGOCIO

I. ELEMENTOS:

a) Análisis de impacto: Es el punto de partida de una gestión efectiva de continuidad del negocio. Es el proceso

dinámico de identificación de las operaciones y servicios críticos, dependencias internas y externas claves y niveles apropiados de resistencia. Evalúa los riesgos e impactos potenciales de varios escenarios de interrupción en las operaciones y reputación de la institución.

b) Estrategia de recuperación: Establece objetivos de recuperación y prioridades basadas en el análisis de impacto en el negocio. Entre otros aspectos, establece los objetivos para el nivel de servicios que la institución procuraría prestar en caso de interrupción y la infraestructura necesaria para el restablecimiento total de las operaciones del negocio.

c) Planes de continuidad del negocio: Proporcionan una guía detallada para la implementación de la estrategia de mantenimiento y recuperación. Establecen los roles y delegan responsabilidades para el manejo de interrupciones operacionales y proporcionan pautas claras con respecto a la sucesión de la autoridad en casos de interrupciones que perjudiquen al personal clave. También establecen de manera clara la autoridad para la toma de decisiones y establecen las circunstancias o eventos que activan el plan de continuidad de negocios de la institución. La seguridad del personal debe ser la consideración principal del plan de continuidad de negocios.

II. PRINCIPIOS:

a) Responsabilidades de la junta directiva y de la alta gerencia: La junta directiva y la alta gerencia son conjuntamente responsables por la continuidad de las operaciones de la institución.

La gestión de la continuidad del negocio debe ser un componente clave de la gestión integral de los riesgos de la institución. Las políticas y procesos de la gestión de la continuidad del negocio deben ser implementados a nivel global de la institución o, como mínimo, a las operaciones criticas de la misma. La gestión efectiva de la continuidad del negocio trata no solo de los aspectos técnicos, sino también de los recursos humanos. De esta manera reconoce que los empleados y posiblemente sus familias, puedan verse afectados por el mismo evento que dio origen a la interrupción, y como consecuencia, no todos los empleados estarán disponibles para la institución durante o inmediatamente después de la ocurrencia del evento.

La junta directiva y la alta gerencia de la institución son responsables de la gestión efectiva de sus políticas de continuidad de negocio y por el desarrollo e implementación de políticas que promuevan la resistencia a, y continuidad en el evento de, interrupciones operacionales. Estos deben reconocer que la subcontratación de operaciones no transfiere las responsabilidades que tienen sobre la gestión de la continuidad del negocio al proveedor de servicios. La junta directiva y la alta gerencia deben crear y promover una cultura organizacional que tenga como una de sus prioridades la continuidad del negocio. La junta directiva y la alta gerencia deben proveer los recursos financieros y humanos para desarrollar e implementar el enfoque de la institución a la gestión de la continuidad del negocio.

Se deben establecer los sistemas que permitan informar a la junta directiva y alta gerencia sobre los temas relacionados a la continuidad del negocio, incluyendo el grado de implementación, notificación de incidentes, resultados de las pruebas y acciones relacionadas al fortalecimiento de la resistencia de la institución o habilidad para reanudar operaciones específicas. La gestión de la continuidad del negocio de una institución deben estar sujetas a revisión por los auditores, tanto externos como internos y los hallazgos significativos deben ser puestos en conocimiento de la junta directiva y la alta gerencia de manera oportuna.

La confusión puede ser un serio obstáculo para llevar a cabo una respuesta efectiva a una interrupción. Consecuentemente, las responsabilidades, así como los planes de sucesión, deben estar claramente definidas en las políticas de gestión de continuidad del negocio de una institución.

b) Interrupciones operacionales mayores: Las interrupciones operacionales mayores presentan un riesgo sustancial a la continuidad de las operaciones del sistema financiero. Por tal razón, las instituciones financieras de manera particular deben incluir el riesgo de una interrupción operacional mayor dentro de sus planes de continuidad del negocio. El grado en que una institución en particular se prepara para una recuperación en caso de una interrupción mayor debe estar en concordancia a sus características propias y a su perfil de riesgo. Debido a que el acceso a los recursos necesarios para una recuperación total puede que sean limitados durante una interrupción mayor, la institución debe identificar a través de un análisis de impacto, aquellas funciones y operaciones de negocios que deben ser recuperados prioritariamente, estableciendo objetivos apropiados de recuperación para dichas operaciones.

Las interrupciones mayores de las operaciones varían en alcance y duración. Al evaluar si su gestión de continuidad del negocio es suficiente para dar respuesta a una interrupción mayor, las instituciones deben revisar la adecuación de sus mecanismos de recuperación en las tres áreas siguientes:

1) La institución debe tener el cuidado de que su sitio alterno se encuentre lo suficientemente alejado del lugar donde llevan a cabo sus operaciones principales.

2) La institución debe asegurar que el sitio alterno cuente con la información actualizada suficiente y los equipos y sistemas necesarios para minimizar los efectos de las interrupciones de los servicios, mediante restauración temporal y recuperación definitiva de sus procesos y servicios críticos, en caso de que sus oficinas principales sean severamente dañadas o el acceso a la zona afectada se encuentre restringido.

3) Dado que el personal de la oficina principal pueda que no se encuentre disponible, el plan de continuidad de negocio debe incluir la forma en que la institución proveerá el personal adecuado en términos numéricos y de experiencia, para la reanudación de las operaciones y servicios críticos que sean consistentes con sus objetivos de recuperación.

c) Objetivos de recuperación: Las instituciones financieras deben establecer objetivos de recuperación que reflejen los riesgos que representan para la estabilidad del sistema financiero.

La institución que sufra una interrupción operacional mayor podría afectar la capacidad de los demás miembros de continuar con sus operaciones normales de negocios. Consecuentemente, las instituciones financieras deben tomar en cuenta dicho riesgo y mejorar su gestión de continuidad del negocio en los casos en que determinen que una interrupción de sus operaciones afectaría la estabilidad del sistema financiero.

Los objetivos de recuperación deben identificar tanto niveles esperados de recuperación como el tiempo que tomaría alcanzarlos.

d) Comunicaciones: Las instituciones financieras deben incluir en sus planes de continuidad de negocio los mecanismos y procedimientos para comunicarse tanto dentro de la organización, como con las partes interesadas externas en caso de una interrupción operacional mayor.

Las instituciones financieras deben estar en capacidad para comunicarse de manera efectiva con las partes interesadas relevantes tanto dentro, como fuera de la institución, en caso de una interrupción operacional mayor. Particularmente en las primeras etapas de la interrupción, donde la comunicación efectiva es necesaria para estimar el impacto de ésta, en el personal y operaciones de la institución y en el sistema financiero en general, y tomar la decisión de implementar o no el plan de continuidad del negocio. En la medida en que el tiempo transcurre, la capacidad para comunicar la información más importante disponible a las partes interesadas de manera oportuna es un factor crítico para la recuperación de las operaciones de la institución y para el retorno del sistema financiero a su funcionamiento normal. El mantenimiento de la confianza del público, en la institución financiera, requiere de la capacidad para comunicarse de manera clara y regular durante el tiempo que dure la interrupción.

Asimismo, los procedimientos y sistemas de comunicación de las instituciones financieras deben incluir, como mínimo, los aspectos siguientes:

1) Identificación de las personas responsables de comunicarse con el personal y demás partes interesadas externas. Este grupo puede incluir la alta gerencia, el personal de relaciones públicas, asesores legales y el personal responsable de los procedimientos de continuidad del negocio de la institución. Este grupo debe estar en capacidad para comunicarse con personal ubicado en lugares remotos, disperso a través de múltiples ubicaciones, o que simplemente se encuentre lejos de las oficinas principales de la institución; y

2) Solucionar aspectos relacionados que podrían suscitarse como resultado de una interrupción operacional mayor tales como, la respuesta que se le daría a fallas en los sistemas de comunicación primarios. Esto puede incluir por ejemplo, desarrollar sistemas e información de contacto para el personal clave que facilitaría múltiples métodos de comunicación (líneas telefónicas terrestres, digitales o analógicas; teléfonos celulares, teléfonos satelitales, mensajes de texto, páginas de Internet, entre otros).

e) Pruebas: Las instituciones financieras deben realizar pruebas de sus planes de continuidad de negocios, evaluar su efectividad y actualizar su gestión de continuidad de negocios, según fuere necesario.

Probar la capacidad de recuperación de operaciones criticas tal y como fue planeado es un componente esencial de una gestión efectiva de la continuidad del negocio. Dichas pruebas deben ser llevadas a cabo de manera periódica, tomando en cuenta la naturaleza, alcance y frecuencia, según fuere determinado por la importancia de las aplicaciones y funciones de negocios, el rol de la institución dentro del mercado y cambios materiales en el entorno, tanto externo como interno de la institución. Adicionalmente, dichas pruebas deben identificar la necesidad de modificar el plan de continuidad de negocios y sus aspectos relacionados. En algunos casos, esta necesidad de cambio puede ser el resultado de modificaciones en su negocio, sistemas, software, hardware, personal, instalaciones o el ambiente externo. Tanto la auditoría interna como la externa, deben evaluar la efectividad del programa de pruebas de la institución, revisar los resultados de las pruebas e informar sus hallazgos al comité de auditoría, la alta gerencia y la junta directiva. La junta

directiva y la alta gerencia deben asegurar que cualquier deficiencia encontrada sea subsanada de manera oportuna.

Adicionalmente, a la comprobación que los planes de continuidad del negocio son evaluados y actualizados cuando fuere necesario, las pruebas también son esenciales para promover el entendimiento y familiaridad entre el personal clave de sus roles y responsabilidades en el caso de una interrupción mayor. Es importante por lo tanto, que los programas de pruebas incluyan al personal que seguramente estará involucrado en caso de interrupciones operacionales mayores.

La alta gerencia debe instruir a las áreas funcionales y éstos a su vez al personal bajo su supervisión, en los pasos a seguir en caso de una interrupción, de tal manera que estos sean del conocimiento de todo el personal, así como elaborar los planes de continuidad de los servicios críticos que están bajo su responsabilidad.

(f) A. Rosales B. (f) V. Urcuyo V. (f) Fausto Reyes B. (f) ilegible (Silvio Moisés Casco Marenco) (f) U. Cerna B. (F) **URIEL CERNA BARQUERO,** Secretario Consejo Directivo SIBOIF.