JUNTA MONETARIA
RESOLUCIÓN JM-4-2016

Inserta en el punto séptimo del acta 1-2016, correspondiente a la sesión celebrada por la Junta Monetaria el 6 de enero de 2016.

PUNTO SÉPTIMO: Superintendencia de Bancos eleva a consideración de la Junta Monetaria el proyecto de Reglamento para la Administración del Riesgo Operacional.

RESOLUCIÓN JM-4-2016. Conocido el oficio número 13289-2015 del Superintendente de Bancos, del 11 de diciembre de 2015, al que se adjunta el informe número 2275-2015 de la Superintendencia de Bancos, por medio del cual eleva a consideración de esta junta el proyecto de Reglamento para la Administración del Riesgo Operacional.

LA JUNTA MONETARIA:

CONSIDERANDO: Que de conformidad con los artículos 55 y 56 de la Ley de Bancos y Grupos Financieros, los bancos y las empresas que integran los grupos financieros deberán contar con procesos integrales que incluyan, entre otros, la administración del riesgo operacional, así como políticas y procedimientos para estos efectos; **CONSIDERANDO:** Que dentro de los Principios Básicos para una Supervisión Bancaria eficaz del Comité de Supervisión Bancaria de Basilea, el Principio Básico 25, sobre Riesgo Operacional, indica que el supervisor determina que los bancos cuentan con un marco adecuado de gestión del riesgo operacional que tiene en cuenta su apetito por el riesgo, su perfil de riesgo y la situación macroeconómica y de los mercados. Esto incluye políticas y procesos prudentes para identificar, cuantificar, evaluar, vigilar, informar y controlar o mitigar el riesgo operacional en el momento oportuno; **CONSIDERANDO:** Que en el citado informe número 2275-2015 de la Superintendencia de Bancos, se indica que de acuerdo al análisis efectuado de los estándares emitidos por el Comité de Basilea de Supervisión Bancaria y de la normativa internacional, se concluye que es importante y necesario implementar buenas prácticas para la gestión del riesgo operacional, con el propósito de minimizar las pérdidas ocasionadas por eventos de riesgo operacional y asegurar la continuidad de las operaciones de las instituciones, por lo se estima conveniente su emisión,

POR TANTO:

Con fundamento en lo dispuesto en los artículos 132 y 133 de la Constitución Política de la República de Guatemala; 26, inciso l, de la Ley Orgánica del Banco de Guatemala; 55, 56, 57, 113 y 129 de la Ley de Bancos y Grupos Financieros; y tomando en cuenta el oficio número 13289-2015 y el informe número 2275-2015, ambos de la Superintendencia de Bancos,

RESUELVE:

1. Emitir, conforme anexo a esta resolución, el **Reglamento para la Administración del Riesgo Operacional**.

2. Autorizar a la secretaria de esta junta para que publique la presente resolución en el diario oficial y en otro periódico, la cual entrará en vigencia el día de su publicación.

BANCO DE GUATEMALA - Junta Monetaria - GUATEMALA, C. A.

Armando Felipe García Salas Alvarado
Secretario
Junta Monetaria

ANEXO A LA RESOLUCIÓN JM-4-2016

REGLAMENTO PARA LA ADMINISTRACIÓN DEL RIESGO OPERACIONAL

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Objeto. Este reglamento tiene por objeto regular los aspectos que, como mínimo, deben observar los bancos, las sociedades financieras, las entidades fuera de plaza o entidades off shore autorizadas por la Junta Monetaria para operar en Guatemala y las empresas especializadas en servicios financieros que formen parte de un grupo financiero, para la administración del riesgo operacional.

Artículo 2. Definiciones. Para los efectos de este reglamento se establecen las definiciones siguientes:

Institución o instituciones: se refiere a los bancos, sociedades financieras, entidades fuera de plaza o entidades off shore autorizadas por la Junta Monetaria para operar en Guatemala y las empresas especializadas en servicios financieros que formen parte de un grupo financiero.

Riesgo operacional: es la contingencia de que una institución incurra en pérdidas debido a la inadecuación o a fallas de procesos, de personas, de los sistemas internos, o bien a causa de eventos externos. Incluye los riesgos tecnológico y legal.

Administración del riesgo operacional: es el proceso que consiste en identificar, medir, monitorear, controlar, prevenir y mitigar el riesgo operacional.

Evento de riesgo operacional: es un suceso potencial u ocurrido, de origen interno o externo, que puede generar o ha generado pérdidas por riesgo operacional a la institución.

Factor de riesgo operacional: es la causa u origen de un evento de riesgo operacional. Los factores pueden ser internos, tales como los recursos humanos, los procesos, la tecnología y la infraestructura, sobre los cuales la organización puede tener control; y externos cuya causa u origen escapan al control de la institución, tales como contingencias legales, fallas en los servicios públicos, ocurrencia de desastres naturales, atentados y actos delictivos, así como las fallas en servicios provistos por terceros.

Línea de negocio: es una especialización del negocio que agrupa procesos que generan productos y servicios orientados a los segmentos del mercado que atiende.

CAPÍTULO II
ORGANIZACIÓN PARA LA ADMINISTRACIÓN DEL RIESGO OPERACIONAL

Artículo 3. Políticas, procedimientos y sistemas. Las instituciones deberán implementar políticas, procedimientos y sistemas que les permitan realizar permanentemente una adecuada administración del riesgo operacional, acorde al nivel de tolerancia al riesgo de la institución, considerando la naturaleza, complejidad y volumen de las operaciones que realiza.

Dichas políticas, procedimientos y sistemas deberán considerar lo dispuesto en los capítulos III y IV de este reglamento; así como comprender los aspectos siguientes:

a) Nivel de tolerancia al riesgo operacional para la institución, en términos de frecuencias y severidades;

b) Metodologías para identificar, medir, monitorear, controlar, prevenir y mitigar el riesgo operacional;

c) Indicadores de riesgo operacional; y,

d) Sistemas de información gerencial relacionados con el proceso de administración del riesgo operacional.

Artículo 4. Responsabilidad del Consejo de Administración. El Consejo de Administración, o quien haga sus veces, en lo sucesivo el Consejo, deberá:

a) Aprobar las políticas, procedimientos y sistemas a que se refiere el artículo anterior; asimismo, conocer y resolver sobre las propuestas de actualización y autorizar las modificaciones respectivas;

b) Aprobar el manual para la administración del riesgo operacional a que se refiere el artículo 8 de este reglamento, así como sus correspondientes modificaciones;

c) Conocer anualmente y cuando la situación lo amerite, los reportes que le remita el Comité de Gestión de Riesgos sobre la exposición al riesgo operacional, los cambios sustanciales de tal exposición y el cumplimiento del nivel de tolerancia, así como las medidas para su mitigación y/o adecuada administración; y,

d) Conocer anualmente y cuando la situación lo amerite, los reportes sobre el nivel de cumplimiento de las políticas y procedimientos aprobados para la administración del riesgo operacional.

Las actuaciones del Consejo deberán hacerse constar en el acta correspondiente a cada reunión.

Artículo 5. Responsabilidad del Comité de Gestión de Riesgos. El Comité de Gestión de Riesgos, en lo sucesivo el Comité, estará a cargo de la dirección, de la implementación y del adecuado funcionamiento y ejecución de las políticas, procedimientos y sistemas, aprobados para la administración del riesgo operacional.

Para cumplir con su responsabilidad, el Comité tendrá las funciones siguientes:

a) Proponer al Consejo las políticas, procedimientos y sistemas para la administración del riesgo operacional;

b) Proponer al Consejo el manual para la administración del riesgo operacional;

c) Analizar las propuestas sobre actualización de políticas, procedimientos y sistemas, así como proponer al Consejo la actualización del manual de administración del riesgo operacional, cuando proceda;

d) Aprobar la estrategia para la implementación de las políticas, procedimientos y sistemas para la administración del riesgo operacional y su adecuado cumplimiento;

e) Analizar semestralmente y cuando la situación lo amerite, los reportes que le remita la Unidad de Administración de Riesgos sobre la exposición al riesgo operacional, los cambios sustanciales de tal exposición, el cumplimiento del nivel de tolerancia y las medidas para su mitigación y/o adecuada administración. Lo anterior deberá reportarse al Consejo anualmente y cuando la situación lo amerite;

f) Analizar semestralmente y cuando la situación lo amerite, la información que le remita la Unidad de Administración de Riesgos sobre el nivel de cumplimiento de las políticas y procedimientos aprobados para la administración del riesgo operacional, así como evaluar las causas de los incumplimientos que hubieren e informar al Consejo sobre las medidas adoptadas con relación a dichos incumplimientos. Lo anterior deberá reportarse al Consejo anualmente y cuando la situación lo amerite;

g) Proponer al Consejo las medidas correctivas a adoptar en caso existan desviaciones con respecto al nivel de tolerancia al riesgo operacional; y,

h) Otras que le asigne el Consejo.

Artículo 6. Funciones de la Unidad de Administración de Riesgos. La Unidad de Administración de Riesgos, en lo sucesivo la Unidad, tendrá las funciones siguientes:

a) Proponer al Comité las políticas, procedimientos y sistemas para la administración del riesgo operacional que incluyan metodologías para identificar, medir, monitorear, controlar, prevenir y mitigar dicho riesgo; para el efecto, la Unidad podrá requerir la colaboración de las unidades administrativas de la institución, en las áreas de su competencia;

b) Revisar anualmente las políticas, procedimientos y sistemas aprobados, así como proponer su actualización al Comité, cuando proceda;

c) Monitorear la exposición al riesgo operacional y consolidar los reportes que le remitan sobre dicho monitoreo;

d) Reportar al Comité semestralmente y cuando la situación lo amerite, sobre la exposición al riesgo operacional, los cambios sustanciales de tal exposición, el cumplimiento del nivel de tolerancia y las actividades relevantes para su mitigación y/o adecuada administración;

e) Verificar e informar al Comité, semestralmente, sobre el nivel de cumplimiento de las políticas y procedimientos aprobados para la administración del riesgo operacional, así como proponer al Comité las medidas correctivas correspondientes;

f) Identificar las causas de los incumplimientos a las políticas y procedimientos aprobados, si los hubiere, incluyendo el nivel de tolerancia al riesgo operacional, determinar si dichos incumplimientos se presentan en forma reiterada e informar sobre los resultados y medidas correctivas al Comité, debiendo mantener registros históricos sobre tales incumplimientos;

g) Administrar la base de datos de eventos de riesgo operacional a que se refiere el artículo 21 de este reglamento; y,

h) Otras que le asigne el Comité.

Artículo 7. Responsabilidad de los gerentes. El Gerente General, o quien haga sus veces, será responsable de implementar la administración del riesgo operacional conforme a las disposiciones del Consejo, así como asegurar que se cumpla con la capacitación, las estrategias y los objetivos de la administración del riesgo operacional.

Los gerentes de las unidades de negocios y unidades operativas, o quienes hagan sus veces, deben cumplir con las políticas y procedimientos aprobados para la administración del riesgo operacional.

Artículo 8. Manual para la administración del riesgo operacional. Las políticas, procedimientos y sistemas a que se refiere el artículo 3 de este reglamento deberán constar por escrito en un manual para la administración del riesgo operacional que será aprobado por el Consejo.

El Consejo conocerá y resolverá sobre las propuestas de actualización del manual para la administración del riesgo operacional y autorizará las modificaciones al mismo, las que deberán ser comunicadas a la Superintendencia de Bancos, dentro de los diez (10) días hábiles siguientes a su aprobación.

Las nuevas instituciones que se constituyan y aquellas a las que se les autorice su establecimiento o su funcionamiento deberán remitir una copia del manual referido en este artículo a la Superintendencia de Bancos antes del inicio de sus operaciones. Asimismo, las instituciones a las que se les autorice la incorporación a un grupo financiero deberán remitir dicho manual durante los treinta (30) días hábiles posteriores a su autorización. La Superintendencia de Bancos, a solicitud justificada de los interesados, podrá prorrogar el plazo indicado hasta por treinta (30) días adicionales, por una sola vez.

CAPÍTULO III
FACTORES DE RIESGO OPERACIONAL

Artículo 9. Factores de riesgo operacional. Las instituciones como parte de sus políticas, procedimientos y sistemas para la administración del riesgo operacional deben determinar los factores de riesgo operacional a los cuales se encuentran expuestas, considerando los relativos a recursos humanos, procesos internos, tecnología de la información y factores externos.

Artículo 10. Recursos humanos. Las instituciones deberán gestionar los eventos de riesgo operacional asociados a los recursos humanos, para lo cual deberán contar con políticas, procedimientos y sistemas que incluyan los perfiles de puestos y procedimientos de selección, contratación, inducción, capacitación y monitoreo permanente de su personal.

Artículo 11. Procesos internos. Las instituciones deberán gestionar los eventos de riesgo asociados a los procesos internos, para lo cual deberán definir, documentar, estandarizar y actualizar los procesos necesarios para la realización de sus operaciones y la prestación de sus servicios.

Artículo 12. Tecnología de la información. Las instituciones deberán gestionar los eventos de riesgo asociados a la tecnología de la información, relacionados con la interrupción, alteración o falla de la infraestructura de tecnología de la información, sistemas de información, bases de datos y procesos de tecnología de la información, conforme lo dispuesto en el Reglamento para la Administración del Riesgo Tecnológico.

Artículo 13. Factores externos. Las instituciones deberán gestionar su exposición a los eventos ajenos al control de la institución, que pueden alterar el desarrollo de sus actividades, para lo cual deberán tomar en consideración, entre otros, las fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, las fallas en servicios críticos provistos por terceros y las contingencias legales.

Con la finalidad de mitigar la comisión de atentados y actos delictivos en contra de la institución, de sus empleados en el ejercicio de sus funciones o de sus usuarios cuando hagan uso de los servicios que brinda, las instituciones deberán implementar las políticas, los procedimientos y las medidas de mitigación correspondientes, que permitan una adecuada administración de la seguridad bancaria. Dichas políticas y procedimientos deberán estar contenidos en el manual a que se refiere el artículo 8 de este reglamento.

CAPÍTULO IV
ADMINISTRACIÓN DEL RIESGO OPERACIONAL

Artículo 14. Proceso para la administración del riesgo operacional. Para la adecuada administración del riesgo operacional, las instituciones deberán contar con un proceso integral que debe contener la identificación, medición, monitoreo, control, prevención y mitigación.

Artículo 15. Identificación. Para efectos de lo dispuesto en este reglamento, las instituciones deberán establecer un proceso de identificación de los eventos de riesgo operacional, agrupándolos en las categorías y clasificándolos de acuerdo a las líneas de negocio, conforme a las instrucciones generales que emita la Superintendencia de Bancos.

Artículo 16. Medición. Las instituciones deberán implementar metodologías que les permitan estimar las pérdidas en términos de frecuencias y severidades para evaluar o medir los eventos de riesgo operacional.

Artículo 17. Monitoreo. Para llevar a cabo el seguimiento y control de los eventos de riesgo operacional, así como del nivel de exposición al mismo, las instituciones deberán desarrollar procesos de seguimiento periódico que permitan la rápida detección y corrección de las deficiencias; establecer indicadores de riesgo operacional; y, contar con sistemas de información que permitan la generación de reportes en forma oportuna para apoyar la toma de decisiones.

Artículo 18. Control, prevención y mitigación. Las instituciones deberán establecer mecanismos de control que permitan verificar el cumplimiento de las políticas y procedimientos establecidos en este reglamento y prevenir la ocurrencia de eventos de riesgo operacional; así como implementar medidas que busquen mitigar los eventos de riesgo identificados. Para la implementación de dichas medidas, deberán contar con controles auxiliares internos, en los cuales se describan las acciones a ejecutar, su plazo estimado y los responsables directos de cada acción.

Artículo 19. Contratación de servicios con terceros. En el caso de servicios relacionados con sus operaciones, contratados con terceros, las instituciones deberán velar por la observancia de lo dispuesto en este reglamento, así como establecer políticas y procedimientos para la contratación de dichos servicios, considerando lo siguiente:

a) Criterios para determinar qué actividades pueden ser contratadas;

b) Lineamientos y condiciones para prevenir y, cuando esto no sea posible, gestionar los conflictos de interés que puedan surgir con los miembros del Consejo, gerentes, funcionarios y empleados de la institución;

c) Procedimientos para la debida diligencia en la selección del proveedor;

d) Lineamientos y procedimientos para la formalización, autorización y finalización de la contratación, incluyendo la delimitación de responsabilidades entre las partes, así como la confidencialidad y seguridad de la información;

e) Procedimientos para el seguimiento y control de la prestación de los servicios;

f) Evaluación y monitoreo de los riesgos asociados con el acuerdo de contratación y con la capacidad del proveedor de continuar prestando el servicio; y,

g) Planes de contingencia ante posibles eventualidades derivadas del incumplimiento del proveedor.

En los contratos de servicios que suscriban deberá hacerse constar expresamente que la Superintendencia de Bancos tendrá libre acceso a las instalaciones de la sociedad, empresa o persona particular contratada por las instituciones y podrá requerir cualquier información y documentación relacionada con la contratación de servicios, para efectos de supervisión.

Artículo 20. Plan de continuidad del negocio. Las instituciones deberán implementar un plan de continuidad del negocio, considerando las mejores prácticas internacionales, que tendrá como objetivo principal brindar respuestas efectivas para que la operatividad del negocio continúe de una manera normal, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en sus operaciones. El plan debe contemplar lo siguiente:

a) La identificación de eventos que ponen en riesgo la continuidad del negocio, las actividades a realizar para superarlos, las alternativas de operación, y el retorno a las actividades normales;

b) La asignación de roles y responsabilidades para la continuidad del negocio; así como las acciones a ejecutar durante y una vez ocurrido el evento que ponga en riesgo la continuidad del negocio;

c) Capacitación del personal clave para activar el plan de continuidad del negocio;

d) La realización de las pruebas necesarias para confirmar su eficacia y eficiencia; y,

e) La divulgación del plan a los miembros de la institución que corresponda.

El plan de continuidad deberá ser consistente y podrá estar integrado con el sistema de gestión de la seguridad de la información establecido en el Reglamento para la Administración del Riesgo Tecnológico.

Artículo 21. Base de datos. Las instituciones deberán conformar una base de datos de eventos de riesgo operacional, considerando la información siguiente:

1. Código de identificación del evento;
2. Tipo de evento;
3. Factor de riesgo;
4. Línea de negocio asociada;
5. Descripción del evento;
6. Proceso o área con la que guarda relación el evento;
7. Fecha de ocurrencia o de inicio del evento;
8. Fecha de descubrimiento del evento;
9. Fecha de registro contable del evento, cuando corresponda;
10. Monto bruto de la pérdida incurrida;
11. Monto recuperado mediante coberturas contratadas;
12. Monto total recuperado;
13. Cuentas contables asociadas, cuando corresponda; y,
14. Identificación del riesgo a que está asociado el evento.

Artículo 22. Envío de información a la Superintendencia de Bancos. Las instituciones deberán enviar a la Superintendencia de Bancos información sobre los eventos contenidos en la base de datos a que hace referencia el artículo 21 de este reglamento, a más tardar el 31 de marzo de cada año, con información referida a diciembre del año anterior, conforme a las instrucciones generales que emita el órgano supervisor.

CAPÍTULO V
DISPOSICIONES TRANSITORIAS Y FINALES

Artículo 23. Plazos de implementación. Las instituciones deberán ajustarse a las disposiciones establecidas en este reglamento, con excepción de lo establecido en el artículo 16, y enviar el manual para la administración del riesgo operacional y el plan de continuidad del negocio, a que se refieren los artículos 8 y 20 respectivamente, a más tardar el 31 de enero de 2017.

Asimismo, a más tardar el 30 de junio de 2018, deberán implementar las metodologías a que se refiere el artículo 16 de este reglamento y enviar la información a que se refiere el artículo 21 correspondiente al año 2017.

La Superintendencia de Bancos, a solicitud justificada de los interesados, podrá prorrogar cada uno de los plazos indicados hasta por doce (12) meses, por una sola vez.

Artículo 24. Casos no previstos. Los casos no previstos en este reglamento serán resueltos por la Junta Monetaria, previo informe de la Superintendencia de Bancos.