CONASSIF CONSEJO NACIONAL DE SUPERVISIÓN DEL SISTEMA FINANCIERO

12 de abril del 2016
CNS-1242/05

Señor
Luis Carlos Delgado Murillo, ***Presidente***
CONSEJO NACIONAL DE SUPERVISIÓN
DEL SISTEMA FINANCIERO

Estimado señor:

El Consejo Nacional de Supervisión del Sistema Financiero en el artículo 5 del acta de la sesión 1242-2016, celebrada el 5 de abril del 2016, con base en lo propuesto por la Superintendencia General de Entidades Financieras en su oficio SGF-824-2016, del 3 de marzo del 2016,

considerando que:

consideraciones legales y reglamentarias:

de conformidad con el inciso c), artículo 131, de la Ley Orgánica del Banco Central de Costa Rica, Ley 7558, el Superintendente General de Entidades Financieras propuso al Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF) para su aprobación, el Acuerdo SUGEF 18-16 "Reglamento sobre Gestión del Riesgo Operativo", el cual establece los requerimientos mínimos que deben observar la entidades supervisadas en la gestión del riesgo operativo. Asimismo, el párrafo segundo del artículo 119 de la citada Ley, en relación con la operación propia de las entidades fiscalizadas, establece que se podrán dictar las normas generales que sean necesarias para el establecimiento de sanas prácticas bancarias, todo en salvaguarda del interés de la colectividad.

El inciso b), artículo 171 de la Ley Reguladora del Mercado de Valores, Ley 7732, dispone que son funciones del CONASSIF aprobar las normas atinentes a la autorización, regulación, supervisión, fiscalización y vigilancia que conforme a la ley, deben ejecutar la Superintendencia General de Entidades Financieras (SUGEF), la Superintendencia General de Valores (SUGEVAL) y la Superintendencia de Pensiones (SUPEN).

El párrafo segundo del artículo 28 de la Ley Reguladora del Mercado de Seguros, Ley 8653, indica que a la Superintendencia General de Seguros (*SUGESE*) le son aplicables las disposiciones establecidas, de manera genérica y de aplicación uniforme, para las demás superintendencias bajo la dirección del CONASSIF y sus respectivos superintendentes e intendentes.

Las disposiciones que se emiten son complementarias a las establecidas en los Acuerdos: SUGEF 2-10 "*Reglamento sobre Administración Integral de Riesgos*", SUGEF 16-09 "*Reglamento de Gobierno Corporativo*" y SUGEF 14-09 "*Reglamento sobre la Gestión de la Tecnología de Información*". Además, son congruentes con los principios referenciados como buenas prácticas para la gestión de riesgos, divulgados mediante la Resolución del

Superintendente R-008-2010, del 22 julio del 2010. En virtud de esta condición, a lo largo del reglamento, se introducen las respectivas referencias con el objeto de preservar su concordancia, limitar duplicidades y mejorar la integridad del marco normativo.

consideraciones prudenciales:

El Pilar 2 del documento sobre Convergencia internacional de medidas y normas de capital: marco revisado (Basilea II) y las recomendaciones del Comité de Basilea, contenidas en los "Principios Básicos para una Supervisión Bancaria Eficaz" (setiembre 2012), señalan los principios a seguir para la mejora y fortalecimiento de las prácticas de regulación y supervisión. El principio 25 indica que los supervisores deben determinar que las entidades cuentan con un marco adecuado de gestión del riesgo operativo que considere su apetito por el riesgo, su perfil de riesgo y la situación macroeconómica y de los mercados. Este marco incluye políticas y procesos prudentes para identificar, cuantificar, evaluar, vigilar, informar y controlar o mitigar el riesgo operativo en el momento oportuno.

Conforme los nuevos enfoques de gestión del riesgo, las acciones que se desarrollan, sean correctivas o preventivas, deben armonizarse con la estrategia global de la entidad; por tal razón, las autoridades de las entidades supervisadas deben velar para que el marco de gestión para el riesgo operativo esté integrado, tanto desde el aspecto formal como en la práctica, al proceso de administración integral de riesgos de la entidad; asimismo, que incorpore y atienda oportunamente las recomendaciones derivadas del proceso supervisor.

El riesgo operativo es transversal a la organización, por lo que cualquier área de la entidad es generadora potencial de eventos de riesgo operativo. Esta condición requiere que la estrategia para su gestión involucre a todo el personal. Asimismo, debido a que el entorno empresarial está en constante cambio, la Junta Directiva o autoridad equivalente y la Administración Superior deben velar porque el marco para gestionar el riesgo operativo sea robusto en relación con la idoneidad y capacitación del personal involucrado y los sistemas de información, en línea con los requerimientos planteados por el Acuerdo SUGEF 2-10, dentro de la estructura de soporte para la administración de riesgos.

La incorporación de mejores prácticas en la gestión del riesgo operativo por parte de las entidades supervisadas es imperativo para lograr una mejora en la gestión del riesgo. Con el propósito de avanzar en ese sentido, es necesario establecer un conjunto de requerimientos regulatorios que promuevan dicha gestión.

Este reglamento cubre un conjunto de tópicos que la industria financiera internacional ha reconocido como relevante en la gestión de riesgo operativo. El CONASSIF reconoce que la extensión y profundidad en la implementación de este reglamento debe ser proporcional tanto con el perfil de riesgo y tamaño de cada entidad, como con el volumen y complejidad de sus actividades; por tanto, los requerimientos han sido consignados de manera que se brinde espacio para la aplicación del juicio crítico de las autoridades de la entidad, en el diseño de su marco para gestionar el riesgo operativo. Esta condición de proporcionalidad requiere, consecuentemente, un compromiso de la entidad para realizar una evaluación rigurosa y meticulosa de su propia realidad.

Con el objeto de estimular la implementación, mejora y mantenimiento de estos marcos de gestión para el riesgo operativo, se brinda una gradualidad que permita balancear los esfuerzos requeridos por las entidades y la Superintendencia en el proceso de implementación de estas disposiciones. Asimismo, vía Lineamientos Generales la Superintendencia establece los aspectos técnicos operativos que se estiman necesarios al efecto.

El CONASSIF considera factible a futuro introducir estímulos asociados al grado de intensidad del proceso supervisor o al cargo de capital regulatorio para riesgo operativo actualmente en vigor; sin embargo, este tipo de estímulos estará sujeto a una valoración más integral sobre la evolución de los marcos de gestión, su efectividad y rigor. En ese sentido, el CONASSIF ha señalado (inciso iii del considerando c. del artículo 5 del acta de la sesión 852-2010, celebrada el 20 de mayo del 2010) que, una condición necesaria para dar este tipo de pasos, es el desarrollo de las destrezas y capacidades relacionadas con el juicio informado y criterio valorativo, en las entidades y en el órgano supervisor, aunado a la necesidad de evidenciar la consolidación de los procesos para la gestión integral de riesgos; por tanto, el reglamento que se aprueba a continuación no contempla cambios tendientes a modificar el cargo de capital por riesgo operativo.

La emisión de este reglamento propicia la creación de bases de datos sobre incidencias y eventos potenciales de riesgo operativo que permitan a las entidades, cuyo perfil de riesgo así lo amerite, evolucionar desde metodologías para valoración del riesgo operativo relativamente simples a otras más sofisticadas. Asimismo, establece requerimientos respecto a continuidad del negocio, procesos de tercerización y seguridad de la información que son aspectos inherentes a la gestión de riesgo operativo.

Mediante artículo 10, del acta de la sesión 1162-2015, del 20 de abril del 2015, el CONASSIF sometió a consulta el presente Reglamento. Asimismo, mediante artículo 17, del acta de la sesión 1171-2015, celebrada el 1° de junio del 2015, extendió el plazo otorgado a los consultados para remitir comentarios y observaciones.

Los comentarios y observaciones obtenidos fueron tomados en consideración para el texto final.

resolvió:

I. Aprobar el Acuerdo SUGEF 18-16 "*Reglamento sobre Gestión del Riesgo Operativo*"

ACUERDO SUGEF 18-16
REGLAMENTO SOBRE GESTIÓN DEL RIESGO OPERATIVO
CAPITULO I
DISPOSICIONES GENERALES

Artículo 1. Objeto
Este reglamento establece los requerimientos mínimos que deben observarse en la gestión de riesgo operativo.

Artículo 2. Ámbito de aplicación
Las disposiciones de este reglamento son de aplicación para las entidades supervisadas por la Superintendencia General de Entidades Financieras.

Artículo 3. Definiciones
Para efecto de la aplicación de las disposiciones contenidas en este reglamento se entiende como:
Acuerdo SUGEF 2-10: Reglamento sobre Administración Integral de Riesgos.
Acuerdo SUGEF 16-09: Reglamento de Gobierno Corporativo.
Acuerdo SUGEF 14-09: Reglamento sobre la Gestión de la Tecnología de Información.
Administración Superior: Cualquier persona física que, por su función, cargo o posición, ejerza o represente la máxima autoridad administrativa de una persona jurídica, así como cualquier

persona física que, por su función, cargo o posición en una entidad, intervenga o tenga la posibilidad de intervenir en la toma de decisiones importantes dentro de la entidad.

Administración Integral de Riesgos: Proceso por medio del cual una entidad financiera identifica, mide, evalúa, monitorea, controla, mitiga y comunica los distintos tipos de riesgo a que se encuentra expuesta.

Cuasipérdida: Eventos de riesgo que no resultan en pérdidas financieras, cuyo resultado no depende de la efectividad o funcionamiento de un indicador, control u otra medida preventiva, sino por cuestiones puramente circunstanciales.

Evento de riesgo: Suceso o serie de sucesos, de origen interno o externo, que pueden derivar en pérdidas financieras para la entidad. Puede ser de dos tipos: incidencias, eventos que se han producido; o eventos potenciales, aquellos que podrían producirse.

Factor de riesgo: Causa u origen de un evento de riesgo operativo. Los factores son los procesos, personas, tecnología de información y eventos externos.

Frecuencia: Número de eventos o resultados por unidad de tiempo definida.

Indicador de riesgo: medida cuantitativa o cualitativa que permite determinar prospectivamente la posibilidad de un evento, como de sus consecuencias.

Línea de negocio: Especialización que agrupa procesos encaminados a generar productos y servicios para atender un segmento del mercado objetivo definido en la planificación estratégica de la entidad.

Perfil de riesgo: Naturaleza y magnitud de las exposiciones al riesgo de la entidad.

Plan de contingencia (o Planificación de contingencias): Proceso de desarrollar acuerdos y procedimientos avanzados que permiten a una organización responder a un evento no deseado que repercute negativamente en la organización.

Plan de continuidad (o Plan de continuidad del negocio): Procedimientos documentados que guían a las organizaciones para responder, recuperar, reanudar y restaurar a un nivel predefinido de operación tras la interrupción.

Probabilidad: Medición de la posibilidad de ocurrencia, expresada como un número comprendido entre 0 y 1, donde 0 es la imposibilidad y 1 la certeza absoluta.

Proceso: Es el conjunto de actividades que transforman, bajo determinadas condiciones y plazo, insumos en productos o servicios con valor para el usuario, sea interno o externo.

Proceso crítico: Proceso indispensable para la continuidad del negocio y sus operaciones.

Riesgo inherente: es aquél intrínseco de un producto, actividad, proceso o sistema, entre otros, al que se enfrenta una entidad en ausencia de acciones o controles tendientes a modificar su probabilidad o impacto.

Riesgo legal: Es la posibilidad de pérdidas económicas debido a la inobservancia o aplicación incorrecta o inoportuna de disposiciones legales o normativas, instrucciones emanadas de los organismos de control o como consecuencia de resoluciones judiciales, extrajudiciales o administrativas adversas, o de la falta de claridad o redacción deficiente en los textos contractuales que pueden afectar la formalización o ejecución de actos, contratos o transacciones.

Riesgo operativo: Posibilidad de sufrir pérdidas económicas debido a la inadecuación o a fallos de los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos. Esta definición incluye el riesgo legal y el riesgo de tecnologías de información, pero excluye el riesgo estratégico y el de reputación.

Subprocesos: Son agrupaciones de actividades dentro de un proceso. Su identificación puede resultar útil para aislar los tratamientos específicos que pueden presentarse dentro de un mismo proceso.

Subcontratación: Modalidad de contratación en la que una empresa requiere a otra para que realice determinados servicios, asignados originalmente a la primera.

Tercerización: Modalidad en la que se contrata a un tercero para que éste desarrolle o suministre

un determinado producto o servicio, de forma permanente, temporal o intermitente.

Tolerancia al riesgo: La tolerancia es el nivel máximo de riesgo que la entidad está dispuesta a soportar.

CAPÍTULO II
MARCO GENERAL PARA LA GESTIÓN DEL RIESGO OPERATIVO

Artículo 4. Contexto de la gestión del riesgo operativo
La entidad, de conformidad con lo dispuesto en el Acuerdo SUGEF 2-10, debe contar con una estructura organizativa que le permita implementar efectivamente su estrategia para la gestión del riesgo operativo.

La Junta Directiva o autoridad equivalente, junto con la Administración Superior, deben velar por que las acciones y herramientas que desarrolle la entidad para la gestión del riesgo operativo, estén plenamente integradas a su proceso institucional de administración integral de riesgos y que sean acordes con su tamaño, complejidad, volumen de sus operaciones y perfil de riesgo. En este sentido deben asignar los recursos necesarios para su implementación, sostenibilidad y mejora a través del tiempo.

Artículo 5. Estrategia para la gestión del riesgo operativo
La entidad debe definir la estrategia para gestionar su riesgo operativo. La estrategia debe ser actualizada periódicamente en función al nivel de tolerancia al riesgo, a los cambios en el mercado y en el entorno económico que puedan afectar la operatividad de la entidad. Asimismo, debe estar debidamente aprobada por la Junta Directiva o autoridad equivalente, en línea con las responsabilidades asignadas en el Acuerdo SUGEF 2-10.
La estrategia debe considerar el establecimiento y mantenimiento de límites de tolerancia al riesgo operativo conforme al artículo 9 del Acuerdo SUGEF 2-10 y de un marco o proceso que comprenda las siguientes etapas:

- Identificación.
- Medición y evaluación.
- Control y mitigación.
- Monitoreo e información.

Artículo 6. Políticas para la gestión del riesgo operativo
La Junta Directiva o autoridad equivalente debe aprobar y mantener actualizadas las políticas sobre riesgo operativo, dichas políticas deben considerar como mínimo los siguientes aspectos:

a) Las responsabilidades de la Junta Directiva o autoridad equivalente, de la Administración Superior, del Comité de Riesgos y de la función o unidad de riesgos.
b) Las pautas generales que observará la entidad en el manejo del riesgo operativo.
c) La periodicidad con la que se debe informar a las diferentes instancias de gobierno, sobre la exposición al riesgo operativo de la entidad y de cada unidad de negocio.
d) El nivel de riesgo aceptable por la entidad, en función de probabilidad (frecuencia) e impacto.
e) El proceso que se debe cumplir para la aprobación de propuestas de nuevas operaciones, productos, servicios y sistemas de información.
f) Indicadores de riesgo operativo.

En el marco de las funciones que establece el Acuerdo SUGEF 2-10, la Junta Directiva o autoridad

equivalente y la Administración Superior deben velar por que se definan claramente las funciones que deben acometer el Comité de Riesgos y la unidad o función de riesgos en relación con el riesgo operativo.

Artículo 7. Gestión del riesgo operativo

En consonancia con el marco normativo establecido en el Acuerdo SUGEF 16-09 y el Acuerdo SUGEF 2-10, la entidad debe considerar al riesgo operativo como un riesgo relevante, inherente a la actividad financiera y objeto de gestión en su proceso de administración integral de riesgos.

La entidad debe considerar en su gestión del riesgo operativo los siguientes factores de riesgo:

a) Procesos,
b) Recursos humanos (personas),
c) Tecnología de información, y
d) Eventos externos.

Artículo 8. Identificación

La entidad debe establecer un proceso para identificar, catalogar y posteriormente documentar en su Manual de Administración Integral de Riesgos las líneas de negocio que desarrolla en su actividad comercial, junto con los procesos y subprocesos relacionados, a un nivel de detalle que le permita una adecuada identificación de los eventos de riesgo y la distinción de sus procesos críticos.

El Superintendente, mediante Lineamientos Generales, establecerá las líneas de negocio y categorías de eventos de riesgo operativo que pueden ser utilizados como referencia por la entidad.

En el proceso de identificación de riesgos, la entidad debe velar que se provea de información suficiente para determinar la exposición al riesgo operativo, la cual debe incluir lo correspondiente al riesgo legal.

A efecto de garantizar las condiciones e información necesarias para este ejercicio, la Administración Superior debe velar por que exista una comunicación efectiva entre las áreas de negocio y la unidad o función de riesgos; esta última responsable de coordinar los aspectos necesarios en torno a la identificación de los eventos de riesgo de la organización.

La entidad debe realizar una evaluación del riesgo operativo inherente a los productos, actividades, procesos y sistemas que previo análisis y clasificación, resulten relevantes para la entidad. Asimismo, la Administración Superior debe asegurar que, antes de introducir nuevos productos, se emprendan nuevas actividades o se establezcan nuevos procesos y sistemas, el riesgo operativo inherente a ellos esté sujeto a un procedimiento de evaluación. La unidad o función de riesgos, previo al lanzamiento o prestación de nuevos productos y servicios, debe rendir a la Junta Directiva o autoridad equivalente una opinión sobre la evaluación efectuada. Este requerimiento es obligatorio también cuando se trate del relanzamiento de un producto, servicio, proceso o sistema.

Artículo 9. Medición y evaluación

La entidad debe evaluar los eventos de riesgo, esto implica la medición de las pérdidas potenciales en términos de probabilidad de ocurrencia (frecuencia) e impacto.

La metodología que implemente la entidad para la medición y evaluación debe ser cualitativa y cuantitativa en función al avance que vaya teniendo en su proceso de implementación de la gestión de riesgo operativo. La evaluación cualitativa busca desarrollar los criterios para priorizar la atención de los riesgos y la periodicidad para su seguimiento. La evaluación cuantitativa debe realizarse a través de la información histórica de eventos de riesgo para el caso de las incidencias

de riesgo y en estimaciones para el caso de los eventos potenciales. La metodología utilizada debe constar en el Manual de Administración Integral de Riesgos.

Asimismo, la entidad debe considerar el establecimiento y mantenimiento de un proceso de recopilación y registro de eventos de riesgo considerando los procesos y líneas de negocio identificados. Dicho proceso debe garantizar que la información se computa oportunamente.

Artículo 10. Control y mitigación

El control y mitigación se refiere a las acciones o mecanismos de cobertura y a los controles implementados por la entidad con el propósito de modificar la probabilidad (frecuencia) de ocurrencia y/o el impacto de los eventos de riesgo operativo que conforme el análisis de riesgo excedan su apetito de riesgo operativo.

Para dichos eventos de riesgo, la entidad debe implementar y mantener un plan que establezca las acciones a efectuar, el plazo estimado de ejecución, el grado de avance y los responsables directos de dicha ejecución.

Asimismo, la entidad debe contar con un sistema de control interno que permita verificar el acatamiento de las políticas y procedimientos, incluyendo los planes de acción definidos por la entidad para la mitigación del riesgo operativo. La Administración Superior es responsable de tomar las acciones necesarias para subsanar debilidades del sistema de control interno de la entidad.

Las acciones y controles definidos deben ser proporcionales al riesgo identificado por la entidad de manera que se asegure que los costos de las acciones de mitigación y control no sean mayores a las pérdidas definidas o estimadas.

Artículo 11. Monitoreo e Información

La entidad debe establecer, en su sistema de información, los indicadores y reportes que estime necesarios para realizar un seguimiento de su perfil de riesgo operativo. La periodicidad establecida del seguimiento debe permitir una adecuada retroalimentación sobre las acciones ejecutadas y sobre los cambios del perfil de riesgo operativo, de lo cual la entidad debe mantener evidencia. Dicha periodicidad no podrá ser mayor a seis meses.

CAPÍTULO III
OTRAS DISPOSICIONES SOBRE LA GESTIÓN

Artículo 12. Continuidad del Negocio

Como parte de una adecuada gestión del riesgo operativo, la entidad debe implementar y mantener un sistema que le permita la continuidad del negocio, con el propósito de brindar respuestas efectivas, para que la operatividad de la entidad continúe de una manera razonable, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en sus operaciones.

El sistema para la continuidad del negocio debe ser congruente con el perfil de riesgo, el tamaño, la complejidad y el volumen de las operaciones de la entidad. El sistema para la continuidad del negocio, al menos, debe considerar:

a) Determinación de los procesos críticos del negocio, incluyendo procesos o servicios provistos por terceros.
b) Análisis de impacto al negocio.
c) Plan de continuidad.
d) Planes de contingencia.
e) Ejecución de pruebas periódicas y evaluación de sus resultados. La periodicidad de estas

pruebas no debe ser mayor a los 12 meses.

f) Divulgación y entrenamiento.
g) Establecimiento de un equipo de gestión de la continuidad del negocio, cuyos integrantes cuenten con el conocimiento e información del plan de continuidad, el cual evaluará el problema operativo que se está enfrentando, decidirá las acciones a seguir y monitoreará los eventos y tomará acciones correctivas cuando sea necesario. Las responsabilidades y autoridad de cada miembro del equipo deben ser establecidas de manera detallada.
h) Dentro del sistema para la continuidad del negocio, la entidad debe incorporar el plan para la continuidad de la tecnología de información.

Artículo 13. Seguridad de la información

La entidad debe contar con un sistema de gestión de la seguridad de la información, orientado a garantizar la integridad, confidencialidad y disponibilidad de la información. Para ello, debe cumplir como mínimo con los requerimientos establecidos en el Acuerdo SUGEF 14-09 "*Reglamento Sobre la Gestión de la Tecnología de Información*".

Asimismo, con el propósito de resguardar la calidad de la información, su confidencialidad, integridad y disponibilidad, la entidad debe contar con políticas y procedimientos de gestión y seguridad de la información, que consideren entre otros aspectos:

a) La autenticación para el acceso lógico a los sistemas y servicios informáticos internos y externos.
b) La conservación ordenada, completa, íntegra, oportuna de la información y documentación (registros) que soporta las operaciones de la entidad.
c) La divulgación y uso no autorizado de información confidencial o protegida por ley.

El Superintendente establecerá, mediante Lineamientos Generales, requerimientos mínimos respecto a la autenticación de clientes y autorización de transacciones en la prestación de servicios financieros, en ambientes de banca en línea.

Artículo 14. Base de Datos

La entidad debe conformar una base de datos para incidencias y una base de datos para eventos potenciales. Ambas bases deben contener, al menos, la información que establezca el Superintendente mediante Lineamientos Generales. La entidad, adicionalmente, puede incluir otros campos que requiera para su gestión; asimismo, la Junta Directiva o autoridad equivalente de la entidad debe definir en sus políticas un monto mínimo de pérdida a partir del cual se registra una incidencia o evento potencial en la base de datos. En este último caso, la entidad debe definir los criterios que le permitan imputar un valor al evento en función de la información que se disponga.

Artículo 15. Tercerización

La entidad debe, según la complejidad, naturaleza y criticidad de los servicios contratados o subcontratados, establecer las políticas, procedimientos y controles necesarios para conducir el proceso de selección y contratación de proveedores de servicios, así como para monitorear los procesos o servicios subcontratados. La entidad debe cubrir, como mínimo, los siguientes aspectos:

a) Definición de los criterios para la calificación y adecuada selección de proveedores.
b) En el proceso de contratación:
   i. Legalidad y formalidad de los contratos.
   ii. Definición de los acuerdos del nivel de servicio, brindando especial cuidado al establecimiento de cláusulas referentes a la seguridad de la información, así como cláusulas ante incumplimientos a éstas.
   iii. Definición de las responsabilidades del proveedor y de la entidad.
   iv. Establecimiento de planes de contingencia y continuidad del servicio por parte del proveedor. La entidad debe considerar la inclusión de cláusulas sobre la disponibilidad del proveedor, de ser objeto de pruebas por parte de la entidad, sobre dichos planes, principalmente para el caso de los servicios críticos que están siendo tercerizados sean o no relacionados con Tecnologías de Información (*TI*).
c) La gestión de los riesgos asociados con la subcontratación o con la tercerización.

La entidad debe aplicar la diligencia debida al seleccionar posibles proveedores de servicios. Adicionalmente, la entidad debe considerar los controles aplicables a los servicios de tecnología de información suministrados por terceros, de conformidad con lo dispuesto en el Acuerdo SUGEF 14-09.

Artículo 16. Riesgo de Tecnologías de Información (TI)
La entidad, en su gestión del riesgo operativo, debe considerar el riesgo de Tecnologías de Información (*TI*). Para ello, la Administración Superior debe velar que el marco de trabajo de administración de riesgos de TI esté alineado a su proceso de administración de riesgos. Dicho marco de trabajo debe cumplir con los requerimientos dispuestos por el respectivo proceso de conformidad con lo dispuesto en el Acuerdo SUGEF 14-09.

Artículo 17. Riesgos operativos asociados a actividades específicas
La entidad debe considerar, en el ámbito de la gestión del riesgo operativo, los riesgos operativos asociados a las actividades de titularización, fideicomiso y de toma u ofrecimiento de productos derivados. En tales casos, la entidad debe considerar las leyes y reglamentos que al respecto regulan dichas actividades.

Artículo 18. Divulgación
La entidad debe incluir, en su informe anual de riesgos, los aspectos referidos a su gestión del riesgo operativo, de conformidad con lo dispuesto por el artículo 18 del Acuerdo SUGEF 2-10.

Artículo 19. Reporte para la SUGEF
La entidad debe remitir anualmente, por el medio y en el plazo que defina la SUGEF en el Manual de Información-SICVECA, los datos sobre incidencias y eventos potenciales contenidos en las respectivas bases de datos a que hace mención este reglamento en el artículo 14.

Transitorio 1
La entidad debe presentar a la SUGEF, dentro de los seis meses siguientes a la entrada en vigencia de esta norma, un plan de actividades para la implementación de las disposiciones de este reglamento, que incluya el cronograma de ejecución y los responsables a cargo.

Transitorio 2
La entidad cuenta con dieciocho meses, contados a partir de la entrada en vigencia de este

reglamento para poner en funcionamiento las bases de datos de incidencias y de los eventos potenciales de riesgo operativo.
La primera remisión de los datos de las bases de datos, será un año posterior a su puesta en funcionamiento.

Transitorio 3
La identificación de eventos de riesgo operativo, requerida a la entidad en el artículo 8 de este reglamento, puede realizarse por áreas o unidades organizacionales por el lapso que le tome finalizar su proceso para identificar, catalogar y documentar las líneas de negocio que desarrolla en su actividad comercial.

DISPOSICIÓN FINAL ÚNICA: Entrada en vigencia.
Rige a partir de su publicación en el Diario Oficial La Gaceta.

II. Modificar el Acuerdo SUGEF 2-10 "*Reglamento sobre Administración Integral de Riesgos*", como se indica a continuación:

1. Reformar la definición de riesgo operativo, del artículo 3, conforme el siguiente texto:
Artículo 3. Definiciones
Para los propósitos de este Reglamento se entiende como:
[…]
j) **Riesgo operativo:** Posibilidad de sufrir pérdidas económicas debido a la inadecuación o a fallos de los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos. Esta definición incluye el riesgo legal y el riesgo de tecnologías de información, pero excluye el riesgo estratégico y el de reputación.
[…]

2. Reformar el artículo 11. "*Manual de Administración Integral de Riesgos*", para que se lea de la siguiente forma:

Artículo 11. Manual de Administración Integral de Riesgos
La entidad financiera supervisada por la SUGEF debe contar con un Manual de Administración Integral de Riesgos, el cual es un documento técnico que describe los elementos del proceso de Administración Integral de Riesgos, incluyendo los marcos de gestión específicos para riesgos, cuyas características así lo requieran.

Sin perjuicio de otros aspectos que a juicio de la entidad deban incluirse en su Manual de Administración Integral de Riesgos, la entidad deberá considerar lo siguiente:

a) Etapas del proceso de Administración Integral de Riesgos y de los marcos específicos para la gestión de riesgos que así lo requieran.
b) Políticas y procedimientos para los riesgos relevantes.
c) Metodologías de medición y responsable(s) de la medición para los riesgos relevantes.
d) Límites de tolerancia para cada riesgo relevante.
e) Periodicidad de monitoreo y responsables.
f) Periodicidad, finalidad y usuario final de los informes y reportes de riesgos.
g) Casos de excepción a las políticas, límites de tolerancia y responsable de su autorización.
h) Instancias y órganos que participan del proceso de Administración Integral de Riesgos.

i) Responsabilidades y deberes de funcionarios involucrados en el proceso de Administración Integral de Riesgos.
j) Estrategias de comunicación hacia lo interno de la entidad.
k) Proceso de control, revisión y reacción interna del proceso.

El Manual de Administración Integral de Riesgos puede constituirse en formato digital, para ello la entidad debe velar que los documentos y demás registros electrónicos estén aprobados y firmados digitalmente.

3. Incluir un nuevo capítulo VII. "*Informe anual de riesgos*", según el siguiente texto:

Capítulo VII
Informe anual de Riesgos

Artículo 20. Informe Anual de Riesgos
La entidad, con corte al 31 de diciembre de cada año, debe preparar y divulgar en su sitio *web* u otro medio en ausencia del primero, un informe anual de riesgos, que contenga al menos la siguiente información:

a) Enunciación de los riesgos objeto de gestión.
b) Resumen de los principios y principales políticas sobre la gestión de riesgos.
c) Acciones o avances en la implementación de mejoras en relación con la gestión de sus riesgos relevantes.
d) Breve descripción de las metodologías dispuestas para la medición y evaluación de los riesgos relevantes de la entidad.
e) Acciones de mitigación y control implementados.
f) Logros obtenidos.

El plazo máximo para divulgar el informe anual de riesgos es de tres meses posteriores al corte.

III. Las anteriores disposiciones rigen a partir de su publicación en el diario oficial La Gaceta.

Atentamente,

Documento suscrito mediante firma digital.

Jorge Monge Bonilla
Secretario del Consejo

Comunicado a: *Entidades supervisadas por SUGEF, diario oficial La Gaceta (c. a: Banco Central de Costa Rica, Superintendencias, Intendencias y Auditoría Interna CONASSIF).*