República de Panamá
Superintendencia de Bancos

ACUERDO No. 007-2011
(de 20 de diciembre de 2011)

"Por el cual se establecen las normas sobre Riesgo Operativo"

LA JUNTA DIRECTIVA
En uso de sus facultades legales, y

CONSIDERANDO:

Que a raíz de la emisión del Decreto Ley 2 de 22 de febrero de 2008, el Órgano Ejecutivo elaboró una ordenación sistemática en forma de texto único del Decreto Ley 9 de 1998 y todas sus modificaciones, la cual fue aprobada mediante Decreto Ejecutivo 52 de 30 de abril de 2008, en adelante la Ley Bancaria;

Que de conformidad con lo establecido en el numeral 1 del artículo 5 de la Ley Bancaria, es objetivo de la Superintendencia velar por la solidez y eficiencia del sistema bancario;

Que de conformidad con el artículo 6 de la Ley Bancaria, son funciones de la Superintendencia de Bancos velar porque los bancos mantengan coeficientes de solvencia y liquidez apropiados para atender sus obligaciones;

Que de conformidad con la facultad de carácter técnico que se establece en el Artículo 11, Literal I, numeral 5 de la Ley Bancaria, corresponde a la Junta Directiva fijar en el ámbito administrativo la interpretación y alcance de las disposiciones legales o reglamentarias en materia bancaria;

Que de conformidad con la facultad de carácter técnico que se establece en el Artículo 11 Literal I, numeral 3 de la Ley Bancaria, corresponde a la Junta Directiva aprobar los criterios generales de clasificación de los activos de riesgos y las pautas para la constitución de reservas para cobertura de riesgos;

Que de conformidad con lo establecido en el artículo 72 de la Ley Bancaria, sobre valoración de otros riesgos, se establece que para la determinación del índice de adecuación de capital la Superintendencia podrá tomar en cuenta la existencia de otros riesgos, tales como riesgo de mercado, riego operacional y el riesgo país;

Que de conformidad con lo establecido en el artículo 16, literal I, numeral 22, son atribuciones del Superintendente, evaluar los indicadores financieros de los bancos y de los grupos bancarios que permitan dar seguimiento a los principales riesgos bancarios, tales como adecuación de capital, crédito, liquidez, operacional, mercado y otros que la Superintendencia estime conveniente.

Que el Principio No. 7 para una supervisión bancaria efectiva del Comité de Basilea, establece que los bancos deben contar con un proceso integral de gestión de riesgo, que incluya la vigilancia por la junta directiva y la gerencia superior, para identificar, evaluar, vigilar y controlar o mitigar todos los riesgos sustanciales y evaluar su suficiencia de capital global con respecto a su perfil de riesgo;

Que las entidades bancarias, según sus características, operaciones y productos que ofrece asumen riesgos operativos, razón por la cual, dentro de su proceso de gestión de riesgos deben evaluar este riesgo;

Que en sesiones de trabajo de esta Junta Directiva se ha puesto de manifiesto la necesidad y conveniencia de elaborar una norma que establezca el marco general de gestión del riesgo operativo.

ACUERDA:

NORMA DE GESTIÓN DE RIESGO OPERATIVO

CAPÍTULO I
CONSIDERACIONES GENERALES

ARTÍCULO 1.- OBJETIVO Y CRITERIOS. El presente Acuerdo establece los principios, criterios generales y parámetros mínimos que los bancos deben observar en el diseño, desarrollo y aplicación de su gestión de riesgo operativo, el cual debe incluir la identificación, medición, mitigación, monitoreo y control, e información.

ARTÍCULO 2.- ÁMBITO DE APLICACIÓN. Las disposiciones del presente Acuerdo son aplicables a:

1. Los bancos oficiales.
2. Los bancos de licencia general.
3. Los bancos de licencia internacional de los cuales la Superintendencia de Bancos ejerza la supervisión de origen.

En el caso de los bancos de licencia internacional de los cuales la Superintendencia ejerza la supervisión de destino, éstos deberán establecer bajo sus mecanismos internos una adecuada gestión del riesgo operacional, la cual estará sujeta a revisión de esta Superintendencia. No obstante lo anterior, el Superintendente podrá requerir a la gerencia local, cuando así lo considere conveniente, las exigencias de gestión de riesgo operacional establecidas en el presente Acuerdo.

ARTÍCULO 3.- DEFINICIONES Y TÉRMINOS. Para efecto de la aplicación de las disposiciones contenidas en el presente Acuerdo, se entenderá por:

1. **Junta Directiva.** Órgano responsable de la dirección y control del banco, que vela por el logro de los mejores intereses de la entidad sin participar por ningún motivo en la gestión directa de las actividades de negocio del banco.

2. **Gerencia superior o alta dirección:** Es la máxima autoridad ejecutiva (llámese gerente general, vicepresidente ejecutivo, presidente ejecutivo, u otra denominación), así como al segundo ejecutivo de más alto rango (llámese subgerente general, o cualquier otra denominación) y a los otros gerentes y colaboradores que ejecuten funciones claves que deban reportar directamente a los anteriores.

3. **Gestión Integral de Riesgos.** Es el proceso por medio del cual el banco identifica, mide, monitorea, controla, mitiga e informa a las áreas operativas dentro del banco, los distintos tipos de riesgo a los que se encuentra expuesto de acuerdo al tamaño y complejidad de sus operaciones, productos y servicios.

4. **Riesgo operativo:** Es la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones del recurso humano, de los procesos, de la tecnología, de la infraestructura o por la ocurrencia de acontecimientos externos. Esta definición incluye el riesgo legal asociado a tales factores.

5. **Riesgo legal:** Es la posibilidad de incurrir en pérdidas como resultado del incumplimiento de normas, regulaciones, o procedimientos con posibles consecuencias legales, así como por efecto de estipulaciones contractuales. El riesgo legal surge también de actuaciones malintencionadas, negligentes o involuntarias que afectan la formalización, efectividad o ejecución de contratos o transacciones.

6. **Evento de riesgo operativo:** Es un suceso o serie de sucesos potenciales, de origen interno o externo, que de producirse puedan ocasionarle pérdidas financieras al banco.

7. **Incidencia de riesgo operativo**. Es un suceso o serie de sucesos acontecidos, de origen interno o externo, que pueden ocasionarle al banco pérdidas financieras.

8. **Factor de riesgo operativo.** Es la causa primaria o el origen de un evento de riesgo operativo. Los factores pueden ser **internos** (recursos humanos, los procesos, la tecnología y la infraestructura, sobre los cuales la organización puede tener un control directo) y **externos (**acontecimientos cuyas causas y origen escapan al control de la organización).

9. **Proceso**. Es el conjunto de actividades que transforman insumos en productos o servicios con valor para el usuario, sea interno o externo.

10. **Línea de negocio.** Es una especialización del negocio que agrupa procesos encaminados a generar productos y servicios especializados para atender un segmento del mercado objetivo.

CAPÍTULO II
AMBIENTE APROPIADO PARA LA GESTIÓN DEL RIESGO OPERATIVO

ARTÍCULO 4.- ORGANIZACIÓN. Los bancos, de conformidad a la complejidad de sus operaciones y a su perfil de riesgo, deben contar con una estructura organizativa que promueva la administración adecuada del riesgo operativo. Asimismo deben definir claramente las responsabilidades y el grado de dependencia e interrelación entre las diferentes áreas del banco.

Tal como se establece en el Acuerdo de Gestión Integral de Riesgo, la estructura organizativa debe incorporar una unidad de administración de riesgos, que debe ser independiente. Dicha unidad, debe tener dentro de sus funciones la gestión del riesgo operativo.

Asimismo, el comité de riesgos debe velar por una adecuada gestión del riesgo operativo.

ARTÍCULO 5.- ESTRATEGIA DE GESTIÓN. Los bancos deben definir la estrategia para gestionar el riesgo operativo. Para ello, deben establecer una metodología que permita llevar a cabo la identificación, medición, mitigación, monitoreo y control e información de dicho riesgo.

Considerando que todas las áreas del banco generan eventos potenciales de riesgo operativo, la estrategia debe contar con el apoyo de la junta directiva e involucrar a todo el personal.

La estrategia utilizada debe ser actualizada periódicamente en función a la tolerancia al riesgo y a los cambios en el mercado y en el entorno económico que puedan afectar la operatividad del banco. Además, es importante que la estrategia defina o identifique los recursos adecuados en términos de personal capacitado, procesos, sistemas de información y todo el ambiente necesario para la gestión del riesgo operativo.

ARTÍCULO 6.- POLÍTICAS. Los bancos deberán diseñar políticas de riesgo operativo, que incluyan como mínimo lo siguiente:

1. Las funciones y responsabilidades de la junta directiva, gerencia superior, comité de riesgos, de la unidad administración de riesgos.
2. La forma y periodicidad con la que se debe informar a la junta directiva y a la gerencia superior, entre otros, sobre la exposición al riesgo operativo del banco y de cada unidad de negocio.
3. El nivel de riesgo aceptable por el banco, en función de frecuencia y severidad.
4. El proceso que se debe cumplir para la aprobación de propuestas de nuevas operaciones, productos y servicios, entre otros aspectos.
5. Los indicadores de riesgo operativo que defina el banco.

CAPÍTULO III
GESTIÓN DEL RIESGO OPERATIVO

ARTÍCULO 7.- FACTORES O CATEGORÍAS DE RIESGO OPERATIVO. Los bancos deberán considerar los siguientes factores de riesgo operativo:

1. **Recursos Humanos.** Los bancos deben gestionar el capital humano de forma adecuada, e identificar apropiadamente las fallas o insuficiencias asociadas al factor "personas", tales como: falta de personal adecuado, negligencia, error humano, sabotaje, fraude, hurto, apropiación de información sensible, nepotismo, relaciones interpersonales inapropiadas y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal, entre otros.

2. **Procesos Internos.** Con el objeto de garantizar la optimización de los recursos y la estandarización de las actividades, los bancos deben contar con procesos documentados, definidos, y actualizados permanentemente.

   Los bancos deben gestionar apropiadamente los riesgos asociados a procesos que permiten la realización de sus operaciones y servicios, dado que su diseño inadecuado puede tener como consecuencia el desarrollo deficiente de las operaciones.

3. **Tecnología.** Los bancos deben contar con la tecnología de información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; que evite interrupciones del negocio, y que logre 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.

   Además de lo anterior, deben cumplir con los requerimientos establecidos en las normas que sobre esta materia emita la Superintendencia de Bancos.

4. **Eventos Externos.** Los bancos deben gestionar los riesgos de pérdidas derivadas de la ocurrencia de eventos ajenos al control de la institución que pudieran alterar el desarrollo de sus actividades. Se deben tomar en consideración los riesgos que implican las contingencias legales, las fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, así como las fallas en servicios críticos provistos por terceros.

ARTÍCULO 8.- GESTIÓN. El proceso de gestión de riesgo operativo comprende las etapas de identificar, medir, mitigar, monitorear y controlar, e informar sobre los eventos de riesgo operativo.

ARTÍCULO 9.- IDENTIFICACIÓN. Como parte de la gestión de riesgo operativo, el banco deberá identificar los eventos o incidencias de riesgo operativo agrupándolos de la siguiente manera:

1. **Fraude interno**. Pérdidas derivadas de algún tipo de actuación, en la que se encuentran implicados empleados del banco, encaminada a defraudar, apropiarse de bienes indebidamente o incumplir regulaciones, leyes o políticas internas.

2. **Fraude externo**. Pérdidas derivadas de algún tipo de actuación por parte de un tercero encaminada a defraudar, apropiarse de un activo indebidamente o incumplir la legislación.

3. **Relaciones laborales y seguridad en el puesto de trabajo**. Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, con la seguridad e higiene en el trabajo, con el pago de reclamos por daños personales o con casos relacionados con la discriminación así como incumplimiento del código de ética.

4. **Prácticas relacionadas con los clientes, los productos y el negocio**. Pérdidas causadas por el incumplimiento de una obligación frente a clientes o derivadas de la naturaleza y el diseño de un producto o servicio. Además, se consideran prácticas relacionadas con los clientes el abuso de confianza, abuso de información confidencial sobre el cliente, negociación fraudulenta en las cuentas del banco, blanqueo de capitales, venta de productos no autorizados.

5. **Daños a activos físicos**. Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos.

6. **Interrupción del negocio por fallas en la tecnología de información**. Pérdidas derivadas de interrupciones en el negocio y de fallas en los sistemas.

7. **Deficiencia en la ejecución, entrega y gestión de procesos**. Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes (proveedores, clientes, depositantes, etc.)

La identificación de los eventos o incidencias de riesgo operativo deberá agruparse por tipos de riesgo, de conformidad a lo establecido en el Anexo 1. Asimismo, es conveniente que la identificación de los eventos de pérdida, puedan agruparse adicionalmente de acuerdo a las líneas de negocio que el banco mantiene, tal como se amplía en el Anexo 2.

ARTÍCULO 10.- MEDICIÓN. Como parte de la gestión del riesgo operativo, el banco deberá evaluar los eventos y las incidencias de riesgo operativo. Esto implica la medición de las pérdidas potenciales en términos de probabilidad de ocurrencia (frecuencia) e impacto (severidad).

La evaluación o medición de los eventos y las incidencias de riesgo operativo es importante para el banco porque en base a ello podrán establecerse mecanismos de cobertura como requerimiento de capital. Adicionalmente, es importante porque en función a dicha evaluación o medición deberán establecerse las medidas de mitigación que busquen minimizar pérdidas.

ARTÍCULO 11.- MITIGACIÓN. Como parte de la gestión del riesgo operativo, una vez identificados los eventos y las incidencias de riesgo operativo y las fallas o vulnerabilidades en relación con los factores de este riesgo y su incidencia para la institución, la gerencia superior deberá decidir si el riesgo se debe asumir, compartir, evitar o transferir, reduciendo sus consecuencias y efectos.

Asimismo, la gerencia superior tendrá una visión clara de los diferentes tipos de exposición al riesgo operativo y su prioridad, con el objeto de tomar decisiones y acciones. Éstas pueden ser, entre otras: revisar estrategias y políticas; actualizar o modificar procesos y procedimientos establecidos; implantar o modificar límites de riesgo; constituir, incrementar o modificar controles; implantar planes de contingencias; revisar términos de pólizas de seguro contratadas; contratar servicios provistos por terceros; u otros, según corresponda.

La gerencia superior debe establecer un plan de acción para implementar las medidas que busquen mitigar los eventos de riesgo identificados. Este plan debe detallar las acciones a implementar, el plazo estimado de ejecución y los responsables directos de dicha ejecución.

ARTICULO 12.- MONITOREO Y CONTROL. Como parte de la gestión del riesgo operativo, el banco deberá llevar a cabo el monitoreo para asegurar que todas las acciones implementadas para mitigar un evento de riesgo se cumplan en los plazos establecidos y que las medidas implementadas efectivamente hayan contribuido a reducir el riesgo por evento en particular y para toda la institución en general.

ARTÍCULO 13.- INFORMAR. Como parte de la gestión de riesgo operativo, el banco deberá asegurarse que la junta directiva y la gerencia superior reciban oportunamente la información sobre toda la gestión de riesgo que se está realizando y del nivel de riesgo operativo al que se encuentra expuesto el banco.

Esta etapa también involucra que las áreas operativas reciban periódicamente información respecto a los eventos y las incidencias de manera que tomen acciones respecto a las mismas.

ARTÍCULO 14.- METODOLOGÍA. Los bancos establecerán en base a su perfil de riesgo y complejidad de sus operaciones, una metodología que incorpore todas las etapas de la gestión de riesgo operativo y que cumpla con los siguientes requisitos:

1. Estar debidamente documentada.
2. Ser implementada en todas las áreas del banco.
3. Permitir una mejora continua de la gestión del riesgo operativo.
4. Estar integrada a todos los procesos de gestión de riesgos de la institución.
5. Establecer procedimientos que aseguren su cumplimiento.
6. Estar aprobada por el comité de riesgos.

ARTICULO 15.- MANUAL DE GESTIÓN. Los bancos contarán con un manual de gestión de riesgo operativo que agrupe las políticas de gestión de este riesgo, las funciones y responsabilidades de las áreas involucradas, la metodología y la periodicidad con la que se debe informar a la junta directiva y a la gerencia superior sobre la exposición al riesgo operativo.

Dado que en la gestión de riesgo operativo participan todos los empleados del banco, se recomienda que el manual de gestión de riesgo operativo esté a su disposición mediante el mecanismo de difusión que el banco considere conveniente.

Los bancos deberán remitir a la Superintendencia, a más tardar el 1 de enero de 2013, el manual de gestión de riesgo operativo que se menciona en el presente artículo. Asimismo, deberán remitir oportunamente las actualizaciones o cambios que realicen al mismo.

CAPÍTULO IV
RESPONSABILIDADES

ARTÍCULO 16.- DE LA JUNTA DIRECTIVA. La junta directiva del banco es responsable de asegurar un ambiente adecuado para la gestión de riesgo operativo, así como de propiciar un ambiente interno que facilite su desarrollo. Entre sus responsabilidades específicas están:

1. Aprobar la política de gestión de riesgo operativo, que comprende también la metodología correspondiente.
2. Aprobar los recursos necesarios para el adecuado desarrollo de la gestión de riesgo operativo, a fin de contar con la infraestructura, metodología y personal apropiado.
3. Vigilar que el comité de riesgos cumpla con las funciones que le han sido asignadas respecto a la labor de riesgo operativo.
4. Requerir a la gerencia superior para su evaluación, reportes periódicos sobre los niveles de exposición al riesgo operativo, sus implicaciones y las actividades relevantes para su mitigación y/o adecuada administración.
5. Conocer los principales riesgos operativos asumidos por el banco, y asegurarse de una efectiva gestión y criterios adecuados que permitan establecer el nivel de tolerancia al riesgo en cuanto a consecuencias y efectos.
6. Asegurarse que el banco cuenta con una efectiva gestión del riesgo operativo y que la misma se encuentra dentro del límite de tolerancia establecido.

ARTÍCULO 17.- DEL COMITÉ DE RIESGOS. El comité de riesgos establecido de conformidad al Acuerdo de Gestión Integral de Riesgos emitido por esta Superintendencia, es el encargado de velar por una sana gestión de los riesgos del banco y desempeñará como mínimo las siguientes funciones:

1. Considerar y proponer para aprobación de la Junta Directiva la metodología de gestión de riesgo operativo.
2. Evaluar, revisar y proponer para aprobación de la Junta Directiva las políticas de gestión de riesgos operativos.
3. Asegurar que se mantiene un proceso de administración de riesgos operativos adecuado y mantener informada a la junta directiva sobre su efectividad.
4. Supervisar que los riesgos operativos sean efectiva y consistentemente identificados, medidos, mitigados, monitoreados y controlados.
5. Proponer los mecanismos para la implementación de las acciones correctivas requeridas en caso de que existan desviaciones con respecto al nivel de tolerancia al riesgo operativo.
6. Apoyar la labor de la unidad de administración de riesgos, en la implementación de la gestión de riesgo operativo.

ARTÍCULO 18.- DE LA GERENCIA SUPERIOR. La gerencia superior tiene a su cargo implementar la gestión de riesgo conforme a lo aprobado por la junta directiva y sus responsabilidades incluyen lo siguiente:

1. Crear y fomentar una cultura organizacional de gestión del riesgo operativo y establecer prácticas adecuadas de controles internos, incluyendo estándares de conducta, integridad y ética para todos los empleados.
2. Administrar el proceso de gestión de riesgo operativo y asegurar su integridad de acuerdo a los lineamientos establecidos por la junta directiva.
3. Proporcionar los recursos necesarios para permitir la implementación de la gestión del riesgo operativo.
4. Asegurar que se cumpla con las estrategias y objetivos de la gestión del riesgo operativo.

ARTÍCULO 19.- DE LA UNIDAD DE ADMINISTRACIÓN DE RIESGOS. De conformidad con lo establecido en el Acuerdo de Gestión Integral de Riesgos, la unidad de administración de riesgos tiene dentro de sus funciones gestionar el riesgo operativo. Adicionalmente a las responsabilidades establecidas en el citado Acuerdo, deberá:

1. Diseñar y someter a aprobación de la junta directiva, a través del comité de riesgos, las políticas para la gestión del riesgo operativo.
2. Diseñar y someter a aprobación del comité de riesgos, la metodología para la gestión del riesgo operativo.
3. Presentar a la junta directiva a través del comité de riesgos la estructura idónea para la gestión del riesgo operativo, designando los responsables o coordinadores de las diferentes unidades funcionales para las actividades de administración de riesgos operativos.
4. Implementar la metodología de gestión de riesgo operativo.
5. Apoyar y asistir a las áreas operativas y de negocio en la implementación de la metodología del riesgo operativo.
6. Elaborar una opinión sobre posibles riesgos operativos vinculados con nuevos productos o servicios, previo a su lanzamiento.
7. Reportar oportunamente y de forma completa y detallada las fallas en los diferentes factores de riesgo operativo a la junta directiva a través del comité de riesgos.

ARTÍCULO 20.- DE LA UNIDAD DE AUDITORÍA INTERNA. La unidad de auditoría interna evaluará el cumplimiento de los procedimientos utilizados para la gestión del riesgo operativo elaborados de conformidad a lo dispuesto en el presente Acuerdo, así como la efectividad en los controles establecidos en el marco de gestión de riesgo operativo.

CAPÍTULO V
OTRAS DISPOSICIONES SOBRE LA GESTIÓN

ARTÍCULO 21.- PLAN DE CONTINUIDAD DE NEGOCIO Y SEGURIDAD DE LA INFORMACIÓN. Como parte de una adecuada gestión del riesgo operativo, los bancos deben implementar un plan de continuidad del negocio que tendrá como objetivo principal brindar respuestas efectivas que garanticen la continuidad en las actividades de servicios y del negocio bancario, ante la ocurrencia de eventos que puedan crear una interrupción o inestabilidad en sus operaciones. Este plan de continuidad debe estar incluido en el manual de riesgo operativo.

Asimismo, deben contar con un sistema de gestión de la seguridad de la información, orientado a garantizar la integridad, confidencialidad y disponibilidad de la información.

ARTÍCULO 22.- AUTOEVALUACIONES. Los bancos realizarán por lo menos una (1) vez al año, autoevaluaciones que detecten las fortalezas y debilidades del entorno de control en las operaciones y actividades de servicios en el negocio bancario, según el listado de potenciales riesgos operativos identificados a los que está expuesto.

ARTÍCULO 23.- BASES DE DATOS. La administración del riesgo operativo constituye un proceso continuo y permanente. Para esto será necesario que los bancos diseñen e implementen las bases de datos en las cuales se recopilen los eventos e incidencias para cumplir con los siguientes criterios:

1. Deben registrarse los eventos de pérdida originados en todo el banco, para lo cual se diseñarán políticas, procedimientos de captura y entrenamiento al personal que interviene en el proceso; y,

2. Debe registrarse, como mínimo, la siguiente información referida a cada evento y/o incidencia:

    a. Categoría: evento o incidencia.
    b. Código de identificación (asignado por el banco).
    c. Tipo de riesgo (según el nivel 1 del Anexo 1 del presente Acuerdo).

d. Línea de negocio asociada, según Anexo 2
e. Causa de riesgo (según el nivel 2 del Anexo 1 del presente Acuerdo)
f. Descripción del hecho. (Según ejemplos descritos en el Anexo 1)
g. Proceso o área a la que pertenece.
h. Fecha de ocurrencia o de inicio.
i. Fecha de descubrimiento.
j. Fecha de registro contable.
k. Monto(s) bruto(s) de la(s) pérdida(s).
l. Monto(s) recuperado(s) mediante coberturas existentes de forma previa al evento (Si aplica).
m. Monto total recuperado (Si aplica).
n. Cuenta(s) contable(s) asociadas (Si aplica).

En el caso de incidencias con pérdidas múltiples, los bancos deben registrar la información mínima requerida por cada pérdida y establecer una forma de agrupar dicha información por el evento que las originó.

En caso que sea un evento y dado que en esta categoría las pérdidas son estimadas, podrá inicialmente registrarse información parcial para luego completarla si se convierte en un incidente. Por ejemplo, podrá registrarse primero el monto de la pérdida, para posteriormente añadir las recuperaciones asociadas.

Los bancos crearán bases de datos donde se registren los eventos de riesgo que, aunque no se hayan convertido en pérdidas, se constituyen en eventos potenciales que requieren, ser evaluados, medidos, controlados y monitoreados desde el enfoque de una adecuada administración de riesgos. Dichas bases de datos pueden ser utilizadas como referencia en las autoevaluaciones señaladas en el artículo 22 del presente Acuerdo.

ARTÍCULO 24.- AUDITORÍA EXTERNA. Cada banco solicitará a sus auditores externos que remitan anualmente al banco un informe sobre el cumplimiento de este Acuerdo y la gestión de riesgo operativo que aplica el banco con base a las disposiciones del presente Acuerdo. Dicho informe deberá ser a su vez presentado por el banco a la Superintendencia en conjunto con los estados financieros auditados. Estos informes serán aplicables a partir de los estados financieros correspondientes a periodos fiscales que cierren en 2013.

ARTÍCULO 25.- CALIFICADORAS DE RIESGO. Los bancos solicitarán a sus calificadoras de riesgo que incorporen en sus metodologías la gestión de riesgo operativo que aplica el banco en el curso de sus operaciones.

ARTÍCULO 26.- RESPALDO POR PÉRDIDAS POTENCIALES. La Superintendencia podrá establecer requerimientos de capital para cubrir el riesgo operativo en base a los estándares internacionales y de acuerdo a la realidad del centro bancario o de un banco en particular.

ARTÍCULO 27.- TRANSPARENCIA. Los bancos deben revelar en su memoria anual, página web, o cualquier otro medio de dominio público, los aspectos fundamentales de la gestión de riesgo operativo que desarrolla la institución, incorporando los objetivos y logros alcanzados.

CAPÍTULO VI
DISPOSICIONES FINALES Y TRANSITORIAS

ARTÍCULO 28.- REQUERIMIENTOS DE INFORMACIÓN. Los bancos deberán remitir a la Superintendencia un informe anual que contenga los principales aspectos y resultados de la gestión de riesgo operativo, a más tardar el 31 de enero de cada año,

debiendo remitir el primer informe correspondiente a la gestión del año 2012, a más tardar el 31 de enero de 2013.

Asimismo, los bancos deberán remitir anualmente y por medios electrónicos en la forma que esta Superintendencia establezca, los eventos y las incidencias que están contenidos en la "bases de datos" a que hace mención el artículo 23 del presente Acuerdo, comenzando con la base de datos del 2013 que se remitirá a más tardar el 31 de enero de 2014.

ARTÍCULO 29.- REQUERIMIENTOS ADICIONALES. Los bancos deberán tener a disposición de esta Superintendencia toda la información, bases de datos, políticas, procesos, procedimientos, sistemas de gestión, estrategias, planes y otros a que hace mención el presente Acuerdo, así como las revisiones de auditoría o de la casa matriz, en caso de las instituciones cuya matriz no se encuentre en el país.

Asimismo, la Superintendencia podrá requerir a cualquier banco toda información adicional que considere necesaria, para una adecuada supervisión del riesgo operativo.

ARTÍCULO 30.- SANCIONES. En caso de incumplimiento de las disposiciones contenidas en el presente Acuerdo, la Superintendencia aplicará las sanciones establecidas en el Título IV de la Ley Bancaria.

ARTÍCULO 31.- VIGENCIA. El presente Acuerdo entrará en vigencia a partir del 1 de julio de 2012.

Dado en la ciudad de Panamá, a los veinte (20) días del mes de diciembre de dos mil once (2011).

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE.

EL PRESIDENTE	**EL SECRETARIO**
Arturo Gerbaud De La Guardia	Félix B. Maduro

ANEXO N° 1

TIPOS DE RIESGO POR PÉRDIDA OPERACIONAL

Tipo de riesgo (Nivel 1)	Causa del riesgo (Nivel 2)	Ejemplos
Fraude interno	Actividades no autorizadas	Operaciones no reveladas (intencionalmente), operaciones no autorizadas (con pérdidas pecuniarias), valoración errónea de posiciones (intencional).
	Hurto y fraude	Robo, malversación, falsificación, soborno, apropiación de cuentas, contrabando, evasión de impuestos (intencional).
Fraude externo	Robo, Hurto y fraude	Robo, falsificación.
	Seguridad de los sistemas	Daños por ataques informáticos, robo de información.
Relaciones laborales y seguridad en el puesto de trabajo	Relaciones laborales	Cuestiones relativas a remuneración, prestaciones sociales, extinción de contratos.
	Higiene y seguridad en el trabajo	Casos relacionados con las normas de higiene y seguridad en el trabajo; indemnización a los trabajadores.
	Diversidad y discriminación	Todo tipo de discriminación.
Clientes, productos y prácticas empresariales	Adecuación, divulgación de información y confianza	Abusos de confianza / incumplimiento de pautas, aspectos de adecuación / divulgación de información (conocimiento del cliente, etc.), quebrantamiento de la privacidad de información sobre clientes minoristas, quebrantamiento de privacidad, ventas agresivas, abuso de información confidencial.
	Prácticas de mercado improcedentes	Prácticas restrictivas de la competencia, prácticas comerciales / de mercado improcedentes, manipulación del mercado, abuso de información privilegiada (en favor de la empresa), lavado de dinero.
	Productos defectuosos	Defectos del producto (no autorizado, etc.), error de los modelos.
	Selección, patrocinio y riesgos	Ausencia de investigación a clientes conforme a las directrices, exceso de los límites de riesgo frente a clientes.
	Actividades de asesoramiento	Litigios sobre resultados de las actividades de asesoramiento.
Daños a activos materiales	Desastres y otros acontecimientos	Pérdidas por desastres naturales, pérdidas humanas por causas externas (terrorismo, vandalismo).
Interrupción del negocio y fallos en los sistemas	Sistemas	Pérdidas por fallas en equipos de hardware, software o telecomunicaciones; falla en energía eléctrica.
Ejecución, entrega y gestión de	Recepción, ejecución y mantenimiento de	Errores de introducción de datos, mantenimiento o descarga, incumplimiento de plazos o de responsabilidades, ejecución errónea de modelos /

Tipo de riesgo (Nivel 1)	Causa del riesgo (Nivel 2)	Ejemplos
procesos	operaciones	sistemas, errores contables. Errores en el proceso de compensación de valores y liquidación de efectivo.
	Seguimiento y presentación de informes	Incumplimiento de la obligación de informar, inexactitud de informes externos (con generación de pérdidas).
	Aceptación de clientes y documentación	Inexistencia de autorizaciones / rechazos de clientes, documentos jurídicos inexistentes / incompletos.
	Gestión de cuentas de clientes	Acceso no autorizado a cuentas, registros incorrectos de clientes (con generación de pérdidas), pérdida o daño de activos de clientes por negligencia.
	Contrapartes comerciales	Fallos de contrapartes distintas de clientes, otros litigios con contrapartes distintas de clientes.
	Distribuidores y proveedores	Subcontratación, litigios con proveedores.
Legal		Pérdidas que surgen por las sanciones impuestas por el incumplimiento de leyes y regulaciones. También como consecuencias de demandas contra la entidad bancaria, que traigan como consecuencia para el banco, reconocer la devolución a tercero de sumas de dinero.

ANEXO N° 2

LINEAS DE NEGOCIO GENÉRICAS PARA EMPRESAS DEL SISTEMA FINANCIERO

Nivel 1	Nivel 2	Definición
Finanzas corporativas	Finanzas corporativas	Realización de operaciones de financiamiento estructurado y participación en procesos de titulización; underwriting; asesoramiento financiero a empresas corporativas, grandes y medianas empresas, así como al gobierno central y entidades del sector público; entre otras actividades de naturaleza similar.
	Finanzas de administraciones públicas	
	Banca de inversión	
	Servicios de asesoramiento	
Negociación y ventas	Ventas	Operaciones de tesorería; compra y venta de títulos, monedas y commodities por cuenta propia; entre otras actividades de naturaleza similar.
	Creación de mercado	
	Posiciones propias	
	Tesorería	
Banca minorista	Banca minorista	Préstamos y depósitos de clientes minoristas, servicios bancarios, fideicomisos y testamentarias.
	Banca Privada	Préstamos y depósitos de particulares, servicios bancarios, fidecomisos y testamentarias y asesoramiento de inversión.
	Servicios de Tarjetas	Tarjetas de empresas /comerciales de marca privada y minoristas.
Banca comercial	Banca comercial	Financiamiento a clientes no minoristas, incluyendo: bienes raíces, financiación de exportaciones, financiación comercial, préstamo, garantías, letras de cambio, factoring, arrendamiento financiero, entre otros.
Pago y Liquidación	Clientes externos	Actividades relacionadas con pagos y cobranzas, transferencia interbancaria de fondos, compensación y liquidación, entre otras actividades de naturaleza similar.
Otros servicios	Custodia	Servicios de custodia, fideicomisos,
	Agencia para empresas	Agentes de emisores y pagos
	Fidecomisos de empresas	
	Otros servicios	
Administración de activos	Administración discrecional de fondos	Agrupados, segregados, minoristas, institucionales, cerrados, abiertos, participaciones accionariales
	Administración no discrecional de fondos	Agrupados, segregados, minoristas, institucionales, de capital fijo, de capital variable.
Intermediación minorista	Intermediación minorista	Ejecución y servicio completo