República de Panamá
Superintendencia de Bancos

ACUERDO No. 011-2018
(de 11 de septiembre de 2018)

"Por medio del cual se dictan nuevas disposiciones sobre Riesgo Operativo"

LA JUNTA DIRECTIVA
En uso de sus facultades legales, y

CONSIDERANDO:

Que a raíz de la emisión del Decreto Ley No. 2 de 22 de febrero de 2008, el Órgano Ejecutivo elaboró una ordenación sistemática en forma de texto único del Decreto Ley No. 9 de 1998 y todas sus modificaciones, la cual fue aprobada mediante Decreto Ejecutivo No. 52 de 30 de abril de 2008, en adelante la Ley Bancaria;

Que en atención a lo dispuesto en los numerales 1 y 2 del artículo 5 de la Ley Bancaria, son objetivos de la Superintendencia de Bancos velar porque se mantenga la solidez y eficiencia del sistema bancario; así como fortalecer y fomentar las condiciones propicias para el desarrollo de la República de Panamá como centro financiero internacional;

Que de conformidad con los numerales 3 y 5 del artículo 11 de la Ley Bancaria, son atribuciones de carácter técnico de la Junta Directiva, aprobar los criterios generales de clasificación de los activos de riesgo y las pautas para la constitución de reservas para cobertura de riesgos, y fijar en el ámbito administrativo, la interpretación y alcance de las disposiciones legales o reglamentarias en materia bancaria;

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 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 los Principios de Basilea 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, cuantificar, evaluar, vigilar, informar y controlar o mitigar todos los riesgos significativos en el momento oportuno, así como para evaluar su suficiencia de capital y liquidez en relación con su perfil de riesgo;

Que dada la evolución de la regulación prudencial, de las buenas prácticas bancarias y de las normas contables y de auditoría, se hace necesario actualizar el marco general regulatorio que rige al centro bancario internacional;

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

Que a través del Acuerdo No. 007-2011 de 20 de diciembre de 2011 se establecen las normas sobre Riesgo Operativo;

Que en sesiones de trabajo de esta Junta Directiva se ha puesto de manifiesto la necesidad y conveniencia de actualizar las disposiciones sobre la gestión del riesgo operativo conforme a los estándares internacionales.

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 se aplicarán a las entidades bancarias según lo establecido en el artículo 1 del Acuerdo sobre Adecuación de Capital emitido por esta Superintendencia.

No obstante, los aspectos relacionados a la gestión de riesgo operativo contemplados en el presente Acuerdo, solo le serán aplicables a todos los bancos de licencia general, y a 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, 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 de los distintos tipos de riesgo a los que se encuentra expuesto.

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, de información de gestión, de los modelos utilizados, o por la ocurrencia de acontecimientos externos. Esta definición incluye el riesgo legal asociado a tales factores; pero excluye las pérdidas por lucro cesante, el riesgo reputacional y el riesgo estratégico.

5. **Riesgo legal.** Es la posibilidad de incurrir en pérdidas como resultado del incumplimiento de normas, leyes, regulaciones o procedimientos con posibles consecuencias legales, así como de instrucciones provenientes de la autoridad competente; de resoluciones judiciales o administrativas adversas, acuerdos judiciales o extrajudiciales, laudos arbitrales, así como por efecto de la redacción deficiente de los textos, que afecten la instrumentación, formalización o ejecución de actos, contratos o transacciones, inclusive distintos a los de su giro ordinario de negocio, o porque los derechos y obligaciones de las partes contratantes no han sido correctamente estipulados.

6. **Evento de riesgo operativo.** Acontecimiento de origen interno o externo, que pudo o puede causar pérdidas a la entidad.

7. **Incidente de riesgo operativo.** Acontecimiento de origen interno o externo, que causó pérdidas al banco.

8. **Categorías de riesgo operativo.** Se refiere a los factores en los que se clasifica el riesgo operativo, dependiendo de la naturaleza de la amenaza.

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.

11. **Apetito al riesgo operativo.** Es el nivel de riesgo operativo que una entidad está dispuesta a asumir. La determinación del apetito al riesgo forma parte del desarrollo de los sistemas de gestión del riesgo y se establece mediante un conjunto de indicadores y parámetros de riesgo.

12. **Tolerancia al riesgo.** Es la máxima desviación que el banco puede soportar con respecto al apetito al riesgo establecido.

13. **Límites de riesgo.** Es la máxima desviación permitida respecto a los valores establecidos de tolerancia al riesgo.

14. **Marco de apetito al riesgo.** Se trata de un sistema general que incluye las políticas, la organización, los procesos, los controles y sistemas de información, mediante los cuales se gestiona el riesgo en la entidad. Deberá incluir los indicadores que permitan definir el apetito al riesgo, los niveles de tolerancia y los límites de riesgo.

15. **Perfil de riesgo.** Se define a partir de la evaluación de la cantidad y magnitud de las exposiciones del riesgo residual a las actividades de negocio y administrativas del banco.

16. **Riesgos operativos identificados.** Amenazas de origen interno o externo que, de realizarse, podrían causar pérdidas contables a la entidad.

17. **Frecuencia.** Número de veces que ocurre un evento o incidente.

18. **Exposición.** Monto de la posible pérdida máxima por la realización de un evento o incidente de riesgo operativo, sin considerar la reducción originada por coberturas o recuperaciones.

19. **Severidad.** Diferencia entre la exposición y el monto recuperado por coberturas y otros.

20. **Riesgo inherente.** Es el riesgo propio de un proceso o actividad, tomando en consideración la frecuencia y el impacto, previo a la acción de control.

21. **Riesgo residual.** Es el resultado de la evaluación de los riesgos propios de la actividad o proceso, después de aplicar los controles para reducir la posibilidad de que ocurran los riesgos operativos identificados.

22. **Límite global.** Es el valor máximo que el banco puede soportar por riesgo operativo, distribuido en rangos según los niveles de criticidad establecidos por la entidad.

23. **Niveles de criticidad.** Es el nivel de riesgo con el que se evalúa la frecuencia, la exposición y la severidad de los eventos e incidentes, de acuerdo con los límites establecidos.

24. **Límites específicos.** Es el componente del límite global asignado a cada tipo de riesgo operativo, distribuido en rangos según los niveles de criticidad establecidos por la entidad.

25. **Mapa de riesgo.** Es la representación gráfica de la concentración de los riesgos operativos por tipo de riesgo, contenidos en las matrices de riesgos y en la base de datos.

26. **Base de datos de riesgo operativo.** Es un repositorio donde se registran los eventos e incidentes de riesgo operativo, con el detalle suficiente y la profundidad histórica necesaria que contribuya a la gestión de estos riesgos.

27. **Indicadores de riesgo operativo (IRO).** Es una forma de medición con la finalidad de servir de alerta temprana sobre el comportamiento de los riesgos operativos ocurridos.

28. **Mitigación.** Consiste en la reducción de la exposición a los riesgos operativos significativos, haciendo más robustos los controles o utilizando programas y coberturas de riesgo como complementos de las medidas de control interno.

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. 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.

Para ello, el banco debe establecer una metodología que permita llevar a cabo la identificación, medición, mitigación, monitoreo, control e información de dicho riesgo.

Considerando que los posibles cambios del mercado afectan el entorno económico y la operatividad del banco, además que todas las áreas de la entidad financiera generan amenazas potenciales de riesgo operativo, la estrategia y en consecuencia la metodología, debe ser revisada anualmente, y debe contar con la aprobación y el apoyo de la junta directiva.

La gerencia superior deberá establecer procedimientos que aseguren un apropiado flujo, calidad y oportunidad de la información entre las unidades de negocios y para todo aquel involucrado en las operaciones que impliquen riesgo para el banco.

ARTÍCULO 6. POLÍTICAS. Los bancos deberán diseñar las políticas, los manuales y los procedimientos de riesgo operativo, que incluyan como mínimo lo siguiente:

1. Las funciones y responsabilidades de la junta directiva, gerencia superior, comité de riesgos y de la unidad de administración de riesgos.

2. Detalle pormenorizado del proceso de gestión (identificación, medición, mitigación, monitoreo, control e información) de los riesgos operativos.

3. Detalle de las herramientas de medición, incluyendo:
   a. El perfil de riesgo operativo,
   b. Matrices de riesgo operativo
   c. Límite global y límites específicos,
   d. Indicadores de riesgo operativo (IRO),

e. Mapas de riesgo inherente y residual por tipo de riesgo,
f. Base de datos de riesgo operativo.

4. El proceso que se debe cumplir para la aprobación de propuestas de nuevas operaciones, productos y servicios, entre otros aspectos.

5. La forma y la periodicidad con la que se debe informar a la junta directiva, comité de riesgos y a la gerencia superior sobre el resultado de la gestión del riesgo operativo.

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. **Amenazas Externas.** Los bancos deben gestionar los riesgos de pérdidas derivadas de la ocurrencia de las amenazas ajenas 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.

5. **Información de gestión.** Todas las decisiones del banco se basan en supuestos, datos, informes y análisis que están expuestos a errores. Desde los análisis sobre el entorno competitivo, los análisis de los mercados en los que la entidad se desenvuelve, la información recogida para las decisiones de riesgo, el grado de satisfacción de los clientes, hasta los sistemas de información específicos para evaluar la liquidez, solvencia y rentabilidad de la entidad. El banco debe revisar periódicamente la veracidad de los supuestos, datos, informes y análisis que utiliza, y dedicar recursos para mejorarlos, tanto de la realidad externa a la entidad como de su propia realidad.

6. **Riesgo de modelo.** La utilización de modelos, especialmente para la valoración de los instrumentos financieros a valor razonable, el diseño de los sistemas de rating, la estimación de provisiones de pérdidas de crédito en base a pérdidas esperadas y, en general, para la medición de los diferentes tipos de riesgos, es una fuente relevante de

riesgo operativo. El contraste de los modelos debe ser parte integrante de la gestión del riesgo operativo.

ARTÍCULO 8. GESTIÓN. El proceso de gestión de riesgo operativo comprende las etapas de identificación, medición, mitigación, monitoreo, control e información sobre los eventos o incidentes de riesgo operativo.

ARTÍCULO 9. IDENTIFICACIÓN. Como parte de la gestión de riesgo operativo, la unidad de administración de riesgos junto con el dueño del proceso, deberán identificar las amenazas que pueden causar pérdidas y que son inherentes a sus procesos, productos, servicios y/o áreas de negocio y administración, agrupándolos de la siguiente manera:

1. **Fraude interno**. Pérdidas potenciales 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 potenciales 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 potenciales 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 potenciales 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 potenciales derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos.

6. **Interrupción del negocio y fallas en la tecnología de información**. Pérdidas potenciales derivadas de las interrupciones en el negocio y de las fallas ocurridas en la tecnología de la información.

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

8. **Deficiencias de índole legal.** Pérdidas potenciales provenientes de sanciones impuestas por el incumplimiento de leyes y regulaciones. También como consecuencia de las demandas en contra de la entidad bancaria, y por defectos en el diseño o formalización de los contratos de los diferentes instrumentos financieros.

9. **Deficiencias de los sistemas de información de gestión.** Pérdidas potenciales derivadas de la discrepancia entre los análisis que sirven de soporte a la toma de decisiones y la realidad subyacente.

10. **Deficiencias en los modelos.** Pérdidas potenciales que surgen por la no idoneidad de determinados modelos, en los ámbitos de la valoración de los instrumentos financieros y la identificación y medición de los riesgos, originadas por hipótesis no adecuadas, estimación sesgada de determinados parámetros, no inclusión de variables relevantes, errores en las bases de datos utilizadas e incluso manipulación de los modelos.

Los riesgos operativos identificados por la entidad en sus procesos, productos, servicios, áreas de servicio y soporte, información de gestión y modelos, serán documentados en matrices de riesgo operativo, las cuales deberán contener como mínimo:

1. El proceso o actividad.
2. Detalle del riesgo identificado.
3. Tipo de riesgo.
4. La causa.
5. La valoración de la frecuencia e impacto.
6. Valoración del riesgo inherente.
7. Descripción del control.
8. Valoración cuantitativa del control.
9. Valoración del riesgo residual.

La(s) matriz(ces) deberán ser revisadas anualmente conforme a los cambios en los procesos, a las actividades de negocio y soporte o el comportamiento de los riesgos operativos.

ARTÍCULO 10. MEDICIÓN. Como parte de la gestión del riesgo operativo, el banco deberá evaluar los eventos y las incidencias de forma continua, mediante el uso de las siguientes herramientas:

1. Perfil de riesgo.
2. Mapas de riesgos.
3. Límite global y límites específicos.
4. Indicadores de riesgo operativo (IRO).
5. Bases de datos de riesgo operativo.

Esto implica al menos:

1. La medición de las exposiciones (frecuencia e impacto) y las pérdidas por tipo de riesgo; y su comparación contra el límite global y límites específicos establecidos por la entidad.
2. Medir y analizar el comportamiento histórico de los riesgos operativos, para establecer e implementar las acciones correctivas encaminadas a fortalecer el control interno en caso de aumentos de las exposiciones o las pérdidas asumidas entre los periodos evaluados, o cuando se produzcan desviaciones a los límites establecidos.

En los casos que sea posible, estimar la probabilidad de los eventos por tipo de riesgo operativo, incluyendo los niveles de confianza de tales estimaciones, para establecer mayores medidas de mitigación o cobertura en caso necesario.

ARTÍCULO 11. MITIGACIÓN. Como parte de la gestión del riesgo operativo, una vez identificadas las amenazas y las fallas o vulnerabilidades ocurridas en la entidad, el comité de riesgos y la gerencia superior deberán decidir si el riesgo se debe asumir, compartir, evitar o transferir, reduciendo sus consecuencias y efectos, para tener una visión clara de los diferentes tipos de exposición al riesgo operativo y su prioridad, con la finalidad de establecer un plan de acción para incrementar las medidas que busquen mitigar estos riesgos.

Este plan debe detallar como mínimo lo siguiente:

1. La descripción del riesgo.
2. Las acciones a implementar.
3. La unidad administrativa responsable de la ejecución.
4. La fecha de aprobación de la medida.
5. La fecha estimada de ejecución.
6. La fecha real de implementación.

La efectividad del plan y la acción de mitigación serán evaluados por el banco a través de las tareas de monitoreo de los riesgos operativos.

ARTÍCULO 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 riesgo (identificado u ocurrido) se cumplan en los plazos establecidos y que estas medidas efectivamente hayan contribuido a reducir la posibilidad de que hechos similares ocurran en el futuro.

Las tareas de monitoreo deberán documentarse y realizarse conforme a la estrategia definida por el banco y en un período no mayor a un año.

ARTÍCULO 13. INFORMAR. La unidad de administración de riesgos deberá asegurarse que el comité de riesgos, la gerencia superior y la junta directiva reciban oportunamente la información sobre el resultado de la gestión de riesgo operativo efectuada, y el nivel de riesgo operativo al que se encuentra expuesto el banco.

Para ello, la unidad de administración de riesgos deberá incluir como mínimo en sus informes lo siguiente:

1. La exposición al riesgo del banco por tipo de riesgo y el resultado de la comparación frente al límite global y límites específicos.
2. El comportamiento histórico de las exposiciones y de las pérdidas asumidas.
3. Las sugerencias respecto a las acciones correctivas que pueden implementarse como resultado de una desviación a los límites establecidos.
4. Resultado del requerimiento de capital por riesgo operativo y su comportamiento histórico,
5. El comportamiento de los indicadores de riesgos operativos y legales.
6. Resultado de las tareas de monitoreo para asegurarse que todas las acciones estén implementadas.

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 (identificación, medición, mitigación, monitoreo, control e información) 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, para lo cual deberá ser actualizada al menos una vez al año.
4. Estar integrada a todos los procesos de gestión de riesgos de la institución.
5. Establecer procedimientos que aseguren su cumplimiento.
6. Estar revisada por el comité de riesgos y aprobada por la junta directiva.

ARTÍCULO 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, el manual de gestión de riesgo operativo debe estar a disposición de los colaboradores mediante el mecanismo de difusión que el banco considere más eficiente.

Los bancos deberán remitir a la Superintendencia, a más tardar el 31 de enero de cada año, este manual por el medio electrónico y en la forma que esta Superintendencia establezca. Asimismo, deberán remitir oportunamente las actualizaciones o cambios que realicen al manual, utilizando el mismo medio electrónico.

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 las políticas y el manual de gestión de riesgo operativo, que comprenden la metodología correspondiente.
2. Aprobar planes de continuidad de negocio que permitan a la entidad reaccionar de manera eficaz frente a situaciones adversas.
3. 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.
4. Vigilar que el comité de riesgos cumpla con las funciones que le han sido asignadas respecto a la labor de riesgo operativo.
5. Conocer las exposiciones y los principales riesgos operativos asumidos por el banco.
6. Conocer sobre el requerimiento de capital regulatorio para riesgo operativo y su efecto en el banco.
7. Asegurarse que el banco cuenta con una efectiva gestión del riesgo operativo y que la misma se encuentra dentro del límite de tolerancia establecido.
8. Requerir al comité de riesgos, los reportes periódicos sobre los niveles de exposición al riesgo operativo, sus implicaciones y los planes de mitigación.
9. Asegurarse que se documente fielmente en las actas de la junta directiva, los asuntos discutidos y las decisiones tomadas sobre la gestión de riesgo operativo.

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. Evaluar y proponer para aprobación de la junta directiva, el manual, las políticas, procedimientos y metodología para la gestión de riesgos operativos.
2. Asegurar que se mantiene un proceso de administración de riesgos operativos adecuado y mantener informada a la junta directiva sobre su efectividad.
3. Supervisar que los riesgos operativos sean efectiva y consistentemente identificados, medidos, mitigados, monitoreados y controlados. El resultado de esta labor quedará documentado en las actas de las sesiones del comité de riesgos, cuando se traten los asuntos de riesgo operativo.
4. Dar seguimiento a las exposiciones a riesgos y comparar dichas exposiciones frente a los límites de tolerancia aprobados por la junta directiva.
5. Definir los escenarios y el horizonte temporal para los análisis sobre el comportamiento de los riesgos operativos.
6. Informar a la junta directiva sobre las exposiciones frente a los límites establecidos y los principales riesgos operativos asumidos, además del comportamiento histórico de estos riesgos. Para tal propósito, requerirá a la unidad de administración de riesgos los informes periódicos correspondientes.
7. Informar a la junta directiva sobre cambios en el perfil de riesgo de la entidad y los resultados de los indicadores de riesgo operativo, asuntos legales o regulatorios.
8. Revisar el requerimiento de capital regulatorio para riesgo operativo y su efecto en el banco.
9. Evaluar y aprobar los planes de acción para implementar las acciones correctivas requeridas en caso de que existan desviaciones a los límites establecidos.
10. Proponer a la junta directiva para su aprobación, el plan de continuidad de negocios para hacer frente de manera eficaz a las situaciones de interrupción o que puedan crear inestabilidad en las operaciones o servicios del banco.
11. Apoyar la labor de la unidad de administración de riesgos, en la implementación de la gestión de riesgo operativo.
12. Documentar fielmente en las actas del comité de riesgos, los asuntos discutidos y las decisiones tomadas sobre la gestión de riesgo operativo.
13. Las funciones y requerimientos que le establezca la junta directiva.

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. Asegurar la consistencia entre las operaciones y los niveles de tolerancia al riesgo.
2. Establecer programas de revisión por parte de la unidad de administración de riesgos y de las unidades de negocios, con respecto al cumplimiento de objetivos, procedimientos y controles en la realización de operaciones, así como de los límites de exposición y niveles de tolerancia al riesgo operativo.

3. Asegurarse que la unidad de administración de riesgos cuenta con el presupuesto suficiente para el desempeño de sus funciones.
4. Asegurarse de la existencia de adecuados sistemas de almacenamiento, procesamiento y manejo de información.
5. Asegurarse que se establezcan programas de capacitación y actualización para el personal de la unidad de administración de riesgos y todo aquel involucrado en las operaciones que impliquen riesgo operativo para el banco.
6. Establecer procedimientos que aseguren un apropiado flujo, calidad y oportunidad de la información entre las unidades de negocio y la de gestión integral de riesgos, y para todo aquel involucrado en las operaciones que impliquen riesgo operativo para el banco.
7. 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.

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. 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.
2. Diseñar e implementar los métodos y las herramientas para la medición del riesgo operativo, congruentes con el grado de complejidad y el volumen de sus operaciones.
3. Coordinar con las áreas operativas y administrativas la identificación, medición, monitoreo, control, mitigación e información de los riesgos operativos que son relevantes y a los cuales está expuesto el banco.
4. Asegurar que las áreas responsables suministren la información necesaria que será utilizada en los métodos y las herramientas para la medición de los riesgos operativos.
5. Reportar toda deficiencia detectada respecto a la calidad, oportunidad e integridad de la información empleada por la unidad de administración de riesgos a las áreas responsables de su elaboración y control.
6. Evaluar permanentemente los modelos y las herramientas para la medición de los riesgos operativos, cuyos resultados deberán presentarse al comité de riesgos.
7. Dar seguimiento a las exposiciones de los riesgos operativos y comparar dichas exposiciones frente a los límites aprobados por la junta directiva.
8. Proporcionar al comité de riesgos o a la instancia responsable al menos trimestralmente, la información relativa a:

    a. Las exposiciones y las desviaciones por tipo de riesgo operativos (Anexo 1) y líneas de negocio (Anexo 2) que se presenten con respecto a los límites establecidos para riesgo operativo.
    b. El impacto sobre la suficiencia del capital regulatorio para riesgo operativo, considerando los análisis de sensibilidad bajo diferentes escenarios (stress testing), incluyendo acontecimientos externos.
    c. Sugerencias respecto a acciones correctivas que pueden implementarse como resultado de una desviación respecto a los límites de tolerancia establecidos.
    d. La evolución histórica de los riesgos operativos asumidos por la entidad con respecto a los límites de tolerancia establecidos.
    e. Comportamiento del perfil, los indicadores y los mapas de riesgo operativo.
    f. Opinión sobre los riesgos operativos identificados en nuevos productos o servicios del banco, previo a su lanzamiento.
    g. Resultado de las tareas de monitoreo.
    h. Grado de avance de las tareas programadas de acuerdo al plan anual de trabajo.

9. Investigar y documentar las causas que originen desviaciones a los límites establecidos, e informar oportunamente al comité de riesgos, al gerente o administrador y al responsable de las funciones de auditoría interna.
10. Requerir a los dueños de los procesos, las acciones correctivas para disminuir las exposiciones o las pérdidas producidas por los riesgos operativos. Además de los planes de acción para fortalecer el control interno y la cultura de la organización hacia una adecuada gestión de los riesgos operativos.

11. Enviar con la periodicidad establecida en este Acuerdo, el resultado del requerimiento de capital para riesgo operativo, asegurando la calidad de los datos utilizados.
12. Coordinar y evaluar con las áreas administrativas y de negocio, la realización de la prueba del plan de continuidad de negocio, y remitir a la junta directiva a través del comité de riesgos, el informe con el resultado de dicha prueba.
13. Las funciones y requerimientos que le establezca el 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, además, de la efectividad en los controles según la lista de los riesgos operativos identificados y a solicitud de la unidad de administración de riesgos, aquellos donde el comportamiento de los eventos e incidentes requiera de una evaluación del control.

Además, a más tardar el 31 de enero de cada año, la unidad de auditoría interna remitirá a la Superintendencia de Bancos, utilizando el medio electrónico y el formato que esta establezca, un informe anual que detalle por fecha, unidad administrativa o de negocio, los hallazgos (condición, causa, efecto y recomendaciones) relacionados a riesgo operativo, en los cuales la unidad de auditoría los haya clasificado con nivel de riesgo medio o alto o que hayan producido pérdidas al banco.

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 deberá ser probado al menos una vez al año. Además, el plan 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. Para ello, el banco deberá documentar el trabajo realizado.

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 centralizadas y de calidad, que permitan registrar, ordenar, clasificar y disponer de información sobre los eventos e incidencias, además de garantizar el entrenamiento al personal que interviene en estos procesos.

Las bases de datos deberán cumplir con los siguientes criterios:

1. Deben registrarse los riesgos operativos (eventos o incidentes) originados en todo el banco, para lo cual se diseñarán políticas, procedimientos de captura y comunicación de estos riesgos.
2. Debe registrarse como mínimo, la siguiente información referida a cada evento y/o incidencia:

    a. Categoría: evento o incidencia.
    b. Modalidad de la ocurrencia.
    c. Código de identificación del evento o incidencia.

d. Línea de negocio, según Anexo 2 del presente Acuerdo.
e. Otra línea de negocio, según Anexo 2 del presente Acuerdo.
f. Origen.
g. Producto afectado.
h. Proceso o área a la que pertenece.
i. Tipo de riesgo (según el nivel uno del Anexo 1 del presente Acuerdo).
j. Causas de riesgo (según el nivel dos del Anexo 1 del presente Acuerdo).
k. Descripción del hecho (según ejemplos descritos en el Anexo 1 del presente Acuerdo).
l. Fecha de ocurrencia o de inicio.
m. Fecha de descubrimiento.
n. Fecha de registro contable.
o. Monto de exposición o monto involucrado.
p. Recuperaciones por seguros.
q. Otras recuperaciones.
r. Monto total recuperado.
s. Cuenta(s) contable(s) asociadas.
t. Estatus.
u. Frecuencia previa estimada.
v. Frecuencia desde.
w. Frecuencia hasta.
x. Criticidad de la Frecuencia.
y. Severidad desde.
z. Severidad hasta.
aa. Nivel de la severidad.
bb. Valor de la frecuencia.
cc. Valor de la severidad.

Todos los eventos e incidentes deberán mantener registrado un monto de exposición o involucrado. En caso de eventos en donde su cuantificación se le dificulte al banco, la entidad deberá estimar la posible pérdida de acuerdo con la situación ocurrida.

En caso de los registros de los eventos de riesgo, aunque no se hayan convertido en pérdidas, se constituyen en acontecimientos 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. 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 25. 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 con la realidad del centro bancario o de un banco en particular.

CAPÍTULO VI
REQUERIMIENTOS DE CAPITAL Y DE INFORMACIÓN

ARTÍCULO 26. DETERMINACIÓN DE LOS ACTIVOS PONDERADOS POR RIESGO OPERATIVO. Los activos ponderados por riesgo operativo se determinan multiplicando por el factor 0.75, el monto del Índice de Negocio (IN) según se define este concepto en el Anexo Técnico del presente Acuerdo.

ARTÍCULO 27. REQUERIMIENTOS DE CAPITAL POR RIESGO OPERATIVO. Los requerimientos mínimos de capital por riesgo operativo se determinan multiplicando los activos ponderados por riesgo operativo según se establece en el artículo anterior, por el coeficiente de capital vigente en la fecha de cumplimiento. La frecuencia del cálculo es trimestral, siguiendo las reglas operativas establecidas por la Superintendencia.

ARTÍCULO 28. REQUERIMIENTOS DE INFORMACIÓN. Los bancos deberán remitir a través del medio electrónico y el formato que la Superintendencia establezca, 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.

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. 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 VII
SANCIONES

ARTÍCULO 31. 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.

CAPÍTULO VIII
DISPOSICIONES FINALES

ARTÍCULO 32. DEROGATORIA. Con su entrada en vigor, el presente Acuerdo derogará en todas sus partes el Acuerdo No. 007-2011 de 20 de diciembre de 2011 y todas sus modificaciones.

ARTÍCULO 33. VIGENCIA. El presente Acuerdo entrará en vigor a partir del 31 de diciembre de 2019, correspondiendo la entrega de los informes pertinentes a más tardar el 30 de enero de 2020.

Dado en la ciudad de Panamá, a los once (11) días del mes de septiembre de dos mil dieciocho (2018).

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE.

EL PRESIDENTE **EL SECRETARIO**

Luis Alberto La Rocca Joseph Fidanque III

ANEXO TÉCNICO

El índice de negocio, IN, se define del modo siguiente:

$$IN = CIAD + CS + CF$$

CIAD, componente de intereses, arrendamientos y dividendos
CS, componente de servicios
CF, componente financiera

A su vez cada una de estas componentes se define del modo siguiente:

$$CIAD = Min\ (ABS(IINT-GINT);0.0225 \times SACD) + DIV$$

ABS(x-y) es el valor absoluto de la diferencia x – y que está dentro del paréntesis
Min (x ; y) es el menor valor de las dos cantidades x e y.
Max(x ; y) es el mayor valor de las dos cantidades x e y.
IINT, monto de los ingresos por intereses
GINT, monto de los pagos por intereses
SACD, monto del saldo de créditos y deuda registrados en el activo
DIV, monto de dividendos cobrados

$$CS = Max\ (OIO;OGO) + Max\ (IHC;GHC)$$

OIO, otros ingresos operativos
OGO, otros gastos operativos
IHC, ingresos por honorarios y comisiones
GHC, gastos por honorarios y comisiones

$$CF = ABS(G_{CN} – P_{CN}) + ABS(G_{LB} – P_{LB})$$

G_{CN} , ganancias de la cartera de negociación

P_{CN} , pérdidas de la cartera de negociación

G_{LB} , ganancias de la cartera del libro bancario

P_{LB} , pérdidas del libro bancario

El detalle de la composición de las variables es el siguiente,

SACD, monto del saldo de créditos y deuda registrados en el activo
SACD = SD + SCR + SIV + SR
SD, saldo de depósitos en bancos y otras instituciones financieras
SCR, saldo de créditos otorgados
SIV, saldo de inversión en títulos de deuda
SR, saldo de reportos de activo

Para el cálculo del Índice de Negocio de un determinado trimestre se realizarán los cálculos siguientes:

- En el caso de las variables que forman parte de Resultados se sumarán los tres valores correspondientes a cada mes del trimestre y se multiplicarán por cuatro para anualizar el valor
- En el caso de las variables que son cuentas del Balance y que forman la variable SACD se calculará la media aritmética de los tres meses que componen el trimestre.

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.).
	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.
Deficiencia en la Ejecución, entrega y	Recepción, ejecución y mantenimiento de	Mantenimiento o descarga, incumplimiento de plazos o de responsabilidades, sistemas. Errores en el proceso de compensación de valores y

Tipo de riesgo (Nivel 1)	Causa del riesgo (Nivel 2)	Ejemplos
gestión de procesos	operaciones	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 normas, leyes y regulaciones. También como consecuencias de demandas contra la entidad bancaria, que traigan como consecuencia para el banco, reconocer la devolución a terceros de sumas de dinero.
Deficiencias en la información de gestión	Supuestos incorrectos	Optimismo exagerado sobre el crecimiento de la economía. Cualquier otra suposición incorrecta que haya afectado decisiones del banco.
	Indicadores sesgados	Indicador de liquidez. Cualquier otro indicador utilizado por el banco.
	Información deficiente	Desconocimiento de la rentabilidad por cliente. Cualquier información incompleta o incorrecta.
	Análisis no contrastados	Opiniones no contrastadas sobre los competidores. Cualquier falta de comparación o verificación.
Deficiencias en los modelos	Supuestos incorrectos	Utilizar modelos obtenidos en otros contextos.
	Deficiencias de los datos	Falta de actualización del valor de las garantías. Cualquier información incompleta o incorrecta.
	Estimaciones sesgadas	Estimación de probabilidades sin disponer de la muestra adecuada y sin previamente disponer de un sistema de calificación contrastado.
	Ausencia de contrastes	Modelos de coberturas sin evaluar la eficacia.

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