Comité de Basilea sobre supervisión bancaria

Documento consultivo

Revisiones a la principios para buenas prácticas de la administración de Riesgo operacional

Publicado para comentarios antes del 6 de noviembre de 2020

Agosto 2020

BANK FOR INTERNATIONAL SETTLEMENTS

Esta publicación está disponible en el sitio web de BIS (www.bis.org).

ISBN 978-92-9259-417-6 (en línea)

Contenido

Revisiones de los Principios para la administración del riesgo operacional

1. Introducción

El Comité de Supervisión Bancaria de Basilea ("el Comité") presentó sus Principios para la Administración del Riesgo Operacional ("los Principios") en 2003, y posteriormente los revisó en 2011 para incorporar las lecciones de la crisis financiera. En 2014, el Comité realizó una revisión de la implementación de los Principios.[1] El propósito de esta revisión fue (i) evaluar el grado en que los bancos habían implementado los Principios; (ii) identificar brechas significativas en la implementación; y (iii) destacar las prácticas emergentes y notables de gestión del riesgo operacional en bancos que actualmente no se abordan en los Principios.

La revisión de 2014 identificó que varios principios no se habían implementado adecuadamente, y se necesitaría más orientación para facilitar su implementación en las siguientes áreas:

a) herramientas de identificación y evaluación de riesgos, incluidas las autoevaluaciones de riesgo y control (RCSA), indicadores clave de riesgo, datos de pérdidas externas, mapeo de procesos de negocios, análisis comparativo y monitoreo de planes de acción generados a partir de diversas herramientas de gestión de riesgos operativos;

b) programas y procesos de gestión del cambio (y su monitoreo efectivo);

c) implementación de las tres líneas de defensa, especialmente refinando la asignación de roles y responsabilidades;

d) Directorio y supervisión de la Alta Gerencia;

e) articulación de apetito de riesgo operacional y declaraciones de tolerancia; y

f) divulgaciones de riesgo.

El Comité también reconoció que los Principios de 2011 no captaron suficientemente ciertas fuentes importantes de riesgo operativo, como las derivadas del riesgo de las tecnologías de la información y la comunicación (TIC),[2] garantizando así la introducción de un principio específico sobre la gestión del riesgo de las TIC. Se realizaron otras revisiones para garantizar la coherencia con el nuevo marco de riesgo operacional en las reformas de Basilea III.[3]

Reconociendo el mayor potencial de interrupciones significativas en las operaciones bancarias debido a pandemias, desastres naturales, incidentes destructivos de seguridad cibernética o fallas tecnológicas, el Comité también ha desarrollado principios para la resiliencia operativa,[4] que reflejan varios de los principios contenidos

Comité de Basilea sobre Supervisión Bancaria, Revisión de los Principios para la Gestión Racional del Riesgo Operacional, 6 de octubre de 2014, https://www.bis.org/publ/bcbs292.pdf.

[1] Los riesgos legales y de conducta (incluidos los riesgos asociados con el lavado de dinero o el financiamiento del terrorismo) siguen siendo preocupaciones importantes. En este contexto, las instituciones financieras deberían continuar mejorando su

[2] capacidad para gestionar el riesgo operativo.

Comité de Basilea sobre Supervisión Bancaria, Basilea III: Finalización de las reformas posteriores a la crisis, 7 de diciembre de

[3] 2017, https://www.bis.org/bcbs/publ/d424.pdf

Según lo propuesto, la resiliencia operativa se define como la capacidad de un banco para realizar operaciones críticas en un contexto

[4] de interrupción. Esta capacidad permite a un banco identificarse y protegerse de amenazas y posibles fallas, responder y adaptarse, así como recuperarse y aprender de eventos disruptivos para minimizar su impacto en la entrega de operaciones críticas a través de la interrupción. Al considerar su capacidad de recuperación operativa, un banco debe tener en cuenta su apetito de riesgo general, capacidad de riesgo y perfil de riesgo. por

Para más detalles, consulte el Comité Consultivo de Basilea sobre Supervisión Bancaria, Documento Consultivo - Principios para la resiliencia operativa ", 6 de agosto de 2020, https://www.bis.org/bcbs/publ/d509.htm.

en este documento Para facilitar el proceso de consulta pública, el Comité ha optado por consultar sobre las revisiones de los Principios para la administración del riesgo operativo y los principios para la resiliencia operativa al mismo tiempo, pero por separado.

El Comité agradece los comentarios sobre este documento de todas las partes interesadas. Más específicamente, el Comité desea obtener comentarios sobre las siguientes preguntas:

Q1. ¿Ha incorporado el Comité las revisiones apropiadas a los Principios? ¿Tiene algún comentario específico sobre las revisiones de los Principios y los párrafos de apoyo?
Q2 ¿Hay algún aspecto que el Comité debería considerar más a fondo?

Los comentarios a este documento consultivo deben enviarse antes del 6 de noviembre de 2020 utilizando el siguiente enlace: www.bis.org/bcbs/commentupload.htm. Todos los comentarios pueden publicarse en el sitio web del Banco de Pagos Internacionales a menos que el demandado solicite específicamente un tratamiento confidencial.

2. Componentes de la gestión del riesgo operacional.

Los Principios en este documento para bancos abarcan la gobernanza, el ambiente de la gestión de riesgos, la tecnología de la información y la comunicación, la planificación de la continuidad del negocio y el papel de la divulgación. Estos elementos no deben verse de forma aislada; más bien, son componentes integrados del marco de gestión de riesgos operativos (ORMF) y el marco general de gestión de riesgos (incluida la capacidad de recuperación operativa) del grupo.

Mediante la publicación de este documento, el Comité desea promover la efectividad de la gestión del riesgo operacional en todo el sistema bancario. El Comité cree que los Principios reflejan buenas prácticas relevantes para todos los bancos. Aun así, el Comité recomienda que los bancos tengan en cuenta la naturaleza, el tamaño, la complejidad y el perfil de riesgo de sus actividades al implementar los Principios.

3. Administración del riesgo operacional

1. El riesgo operacional se define en el marco de capital como el riesgo de pérdida resultante de procesos internos, personas y sistemas inadecuados o fallidos o de eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación.
2. El riesgo operacional es inherente a todos los productos, actividades, procesos y sistemas bancarios, y la gestión eficaz del riesgo operacional es un elemento fundamental del programa de gestión de riesgos de un banco. La sólida gestión del riesgo operacional es un reflejo de la eficacia del Directorio y la Alta Dirección en la administración de su cartera de productos, actividades, procesos y sistemas. Para fines de gestión, las categorías de riesgo estratégico y de reputación están fuertemente vinculadas al programa de gestión de riesgos del banco.
3. La gestión de riesgos abarca identificar riesgos para el banco, medir y evaluar las exposiciones a esos riesgos (cuando sea posible), monitorear las exposiciones y las necesidades de capital correspondientes de forma continua, tomar medidas para controlar o mitigar las exposiciones e informar al Directorio y a la Alta Dirección sobre las exposiciones al riesgo y las posiciones de capital del banco. Los controles internos suelen estar integrados en el negocio diario de un banco y están diseñados para garantizar, en la medida de lo posible, que las actividades del banco sean eficientes y efectivas; y que esa información es confiable, oportuna y completa;

y que el banco cumple con las leyes y regulaciones aplicables.

4. La buena gobernanza interna forma la base de un ORMF efectivo. La gobernanza de la gestión del riesgo operacional tiene similitudes, pero también diferencias en relación con la gestión del riesgo crediticio o de mercado. La función de gobernanza del riesgo operacional de los bancos debe integrarse completamente en su estructura general de gobernanza de gestión de riesgos.

5. Los bancos suelen confiar en tres líneas de defensa: (i) gestión de unidades de negocio, [5] (ii) una función independiente de gestión del riesgo operacional corporativo (CORF) y (iii) auditoría independiente. [6] Dependiendo de la naturaleza, tamaño y complejidad del banco, y del perfil de riesgo de las actividades de un banco, el grado de formalidad de cómo se implementan estas tres líneas de defensa variará.

6. Los bancos deben asegurarse de que cada línea de defensa:

   a) Cuenta con los recursos adecuados en términos de presupuesto, herramientas y personal;

   b) Tiene funciones y responsabilidades claramente definidas;

   c) Está continuamente y adecuadamente entrenado;

   d) Promueve una sólida cultura de gestión de riesgos en toda la organización;

   e) Se comunica con las otras líneas de defensa para reforzar el ORMF.

   Si en una unidad de negocios hay funciones de la primera y segunda línea de defensa, entonces los bancos deben documentar y distinguir las responsabilidades de tales funciones en la primera y segunda línea de defensa, enfatizando la independencia de la segunda línea de defensa.

7. El Comité destacó recientemente que, a pesar de que los bancos adoptan ampliamente el modelo de tres líneas de defensa, la confusión en torno a los roles y responsabilidades a veces dificulta su efectividad. [7] Por lo tanto, la revisión de los Principios también es la oportunidad de enfatizar que este modelo debe ser utilizado de manera adecuada y proporcional por las instituciones financieras para gestionar todo tipo de subcategoría de riesgo operativo, incluido el riesgo de las TIC.

8. En la práctica de la industria, la primera línea de defensa es la gestión de la unidad de negocios. Una buena práctica del riesgo operacional reconoce que la administración de la unidad de negocios es responsable de identificar y gestionar los riesgos inherentes a los productos, actividades, procesos y sistemas por los cuales es responsable. Los bancos deben tener una política que defina funciones y responsabilidades claras en los asuntos relevantes.

[5] El término "unidad de negocio" se entiende en términos generales para incluir todas las funciones de soporte, corporativas y / o servicios compartidos asociados, como por ejemplo: Finanzas, Cumplimiento, Legal, Recursos Humanos, Operaciones y Tecnología, etc. La gestión de riesgos y la auditoría interna no están incluidos a menos que se indique lo contrario.

[6] La Auditoría independiente incluye verificación y validación: la verificación del ORMF se realiza de forma periódica y generalmente se realiza mediante la auditoría interna y / o externa del banco, pero puede involucrar a otros terceros independientes adecuadamente calificados de fuentes externas. Las actividades de verificación prueban la efectividad del ORMF general, de acuerdo con las políticas aprobadas por la junta directiva, y también prueban los procesos de validación para garantizar que sean independientes y se implementen de manera consistente con las políticas bancarias establecidas. La validación asegura que los sistemas de cuantificación utilizados por el banco sean lo suficientemente robustos y garanticen la integridad de los insumos, supuestos, metodologías, procesos y productos. La validación es crítica para un ORMF que funcione bien.

[7] Ver BCBS, *Ciber resiliencia: gama de prácticas*, Diciembre de 2018, disponible en https://www.bis.org/bcbs/publ/d454.pdf,

Unidades de negocios.[8] Las responsabilidades de una primera línea de defensa efectiva en la promoción de una cultura de gestión del riesgo operacional deben incluir:

a) Identificar y evaluar la materialidad de los riesgos operacionales inherentes a sus respectivas unidades de negocio mediante el uso de herramientas de gestión de riesgos;
b) Establecer controles apropiados para mitigar los riesgos operacionales inherentes y evaluar el diseño y la efectividad de estos controles mediante el uso de herramientas de gestión de riesgos operacionales;
c) Informar si las unidades de negocio carecen de recursos, herramientas y capacitación adecuados para garantizar la identificación y evaluación de riesgos operacionales;
d) Monitorear y reportar los perfiles de riesgo operacional de las unidades de negocios,[9] y asegurar su adhesión al apetito de riesgo operacional establecido y la declaración de tolerancia;
e) Informar riesgos operacionales residuales no mitigados por los controles, incluidos los eventos de pérdidas operativas, deficiencias de control, deficiencias de procesos y el incumplimiento de las tolerancias de riesgos operativos.

9. Una función de riesgo operacional corporativo (CORF) funcionalmente independiente es típicamente la segunda línea de defensa. Las responsabilidades de una segunda línea de defensa efectiva deben incluir:

a) Desarrollar una visión independiente con respecto a las unidades de negocio (i) identificaron riesgos operacionales importantes, (ii) diseño y efectividad de controles clave y (iii) tolerancia al riesgo;
b) Revisar/desafiar la relevancia y la coherencia de la implementación de la unidad de negocios de las herramientas de gestión del riesgo operacional, actividades de medición y sistemas de informes a través de un programa de garantía de calidad,[10] y proporcionar evidencia de este desafío efectivo;
c) Desarrollar y mantener políticas, estándares y directrices de gestión y medición de riesgos operacionales;
d) Revisar y contribuir al monitoreo y reporte del perfil de riesgo operacional;
e) Diseñando y brindando capacitación y concientización sobre riesgos operacional;

10. El grado de independencia del CORF puede diferir entre los bancos. En los bancos pequeños, la independencia puede lograrse mediante la separación de funciones y la revisión independiente de los procesos y funciones. En los bancos más grandes, el CORF debe tener una estructura de informes independiente de las unidades de negocio generadoras de riesgo y ser responsable del diseño, mantenimiento y desarrollo continuo del ORMF dentro del banco. CORF normalmente contrata grupos de control corporativo relevantes (por ejemplo, cumplimiento, legal, finanzas y TI) para respaldar su evaluación de los riesgos y controles operativos. Los bancos deben tener una política que defina funciones y responsabilidades claras del CORF, que reflejen el tamaño y la complejidad de la organización.

11. La tercera línea de defensa proporciona al Directorio una garantía independiente de la idoneidad del marco de gestión de riesgos operacionales del banco. El personal de esta función no debe participar en el desarrollo, implementación y operación de los procesos de gestión de riesgos operacional.

En las estructuras bancarias complejas, las "unidades de negocios relevantes" probablemente incluyen funciones de apoyo tales como departamentos de sistemas de información.

[8] Los perfiles de riesgo operativo describen las exposiciones al riesgo operativo y las evaluaciones del entorno de control de las unidades de negocios y consideran el rango de posibles impactos que podrían surgir de las estimaciones de pérdidas esperadas a severas. Los perfiles generalmente brindan a la gerencia y al consejo de administración una representación de las exposiciones al riesgo operativo a un nivel que respalda sus responsabilidades de toma de decisiones y supervisión.

[9]

[10] El aseguramiento de la calidad no siempre es una función de segunda línea; en muchas empresas se considera que es "línea 1.5" e informa a través de la jerarquía empresarial.

por las otras dos líneas de defensa. Las revisiones de la tercera línea de defensa generalmente son realizadas por la auditoría interna y/o externa del banco, pero también pueden involucrar a otros terceros independientes adecuadamente calificados. El alcance y la frecuencia de las revisiones deberían ser suficientes para cubrir todas las actividades y entidades legales de un banco. Una revisión independiente efectiva debería:

a) Revisar el diseño y la implementación de los sistemas de gestión de riesgos operacionales y los procesos de gobernanza asociados a través de la primera y segunda línea de defensa (incluida la independencia de la segunda línea de defensa);

b) Revisar los procesos de validación para garantizar que sean independientes y se implementen de manera coherente con las políticas bancarias establecidas;

c) Asegúrese de que los sistemas de cuantificación utilizados por el banco sean lo suficientemente sólidos como (i) brinden seguridad de la integridad de los insumos, supuestos, procesos y metodología y
(ii) dar lugar a evaluaciones del riesgo operacional que reflejen de manera creíble el perfil de riesgo operativo del banco;

d) Asegúrese de que la gerencia de las unidades de negocios responda de manera rápida, precisa y adecuada a los problemas planteados, e informe periódicamente al Directorio o sus comités relevantes sobre asuntos pendientes y cerrados;

e) Opine sobre la adecuación y adecuación general del ORMF y los procesos de gobierno asociados en todo el banco. Más allá de verificar el cumplimiento de las políticas y procedimientos aprobados por el Directorio, la revisión independiente también debe evaluar si el ORMF cumple con las necesidades y expectativas de la organización (como el respeto del apetito y la tolerancia al riesgo corporativo y el ajuste del marco a las cambiantes circunstancias operativas) y cumple con las disposiciones legales y legislativas, acuerdos contractuales, normas internas y conducta ética.

12. Debido a que la gestión del riesgo operacional está evolucionando y el entorno empresarial cambia constantemente, la alta dirección debe asegurarse de que las políticas, los procesos y los sistemas de ORMF sigan siendo lo suficientemente sólidos como para gestionar y garantizar que las pérdidas operativas se aborden adecuadamente de manera oportuna. Las mejoras en la gestión del riesgo operacional dependen en gran medida de la disposición de la alta dirección para ser proactivo y también actuar de manera rápida y adecuada para abordar las preocupaciones de los gerentes de riesgo operativo.

4. Principios para la gestión racional del riesgo operacional.

Principio 1: El Directorio debe liderar el establecimiento de una fuerte cultura de gestión de riesgos, implementada por la alta dirección.[11] *El Directorio y la alta dirección deben establecer una cultura corporativa guiada por una sólida gestión de riesgos, establecer estándares e incentivos para un comportamiento profesional y responsable, y garantizar que el personal reciba entrenamiento adecuado en gestión de riesgos y la formación ética.*

11 Este documento se refiere a una estructura administrativa compuesta por una junta directiva y la alta gerencia. El Comité es consciente de que existen diferencias significativas en los marcos legislativos y regulatorios entre países con respecto a las funciones de la junta directiva y la alta gerencia. En algunos países, la junta tiene la función principal, si no exclusiva, de supervisar al cuerpo ejecutivo (alta gerencia, gerencia general) para asegurar que este último cumpla con sus tareas. Por esta razón, en algunos casos, se conoce como una junta de supervisión. Esto significa que la junta no tiene funciones ejecutivas. En otros países, el consejo tiene una competencia más amplia, ya que establece el marco general para la gestión del banco. Debido a estas diferencias,

13. Los bancos con una fuerte cultura de gestión de riesgos y prácticas comerciales éticas tienen menos probabilidades de experimentar eventos de riesgo operacional dañinos y están en mejores condiciones para enfrentar de manera efectiva los eventos que ocurren. Las acciones del Directorio y la alta dirección, así como las políticas, procesos y sistemas de gestión de riesgos del banco proporcionan la base para una sólida cultura de gestión de riesgos.

14. El Directorio debe establecer un código de conducta o una política de ética para abordar el riesgo de conducta. Este código o política debe aplicarse tanto al personal como a los miembros del Directorio, establecer expectativas claras de integridad y valores éticos del más alto nivel, identificar prácticas comerciales aceptables y prohibir conflictos de intereses o la provisión inapropiada de servicios financieros (ya sea intencional o negligente) . El código o la política deben ser revisados y aprobados regularmente por el Directorio y atestiguados por los empleados; su implementación debe ser supervisada por un comité de ética de alto nivel u otro comité a nivel de Directorio, y debe estar a disposición del público (por ejemplo, en el sitio web del banco). Se puede establecer un código de conducta separado para puestos específicos en el banco (por ejemplo, agentes de tesorería, alta gerencia).

15. La gerencia debe establecer expectativas y responsabilidades claras para garantizar que el personal del banco comprenda sus roles y responsabilidades para la gestión de riesgos, así como su autoridad para actuar.

16. Las políticas de compensación deben estar alineadas con la declaración de apetito y tolerancia al riesgo del banco, así como con la seguridad y solidez en general, y equilibrar adecuadamente el riesgo y la recompensa.12

17. La alta dirección debe garantizar que haya un nivel adecuado de capacitación en riesgos operacionales en todos los niveles de la organización y que los programas de capacitación personalizados sean obligatorios para roles específicos, como jefes de unidades de negocios, jefes de controles internos y gerentes. La capacitación brindada debe reflejar la antigüedad, el rol y las responsabilidades de las personas a quienes está destinada.

18. Contar con un Directorio sólido y consistente y el apoyo de la alta dirección para la gestión del riesgo operacional y el comportamiento ético refuerzan de manera convincente los códigos de conducta y ética, las estrategias de compensación y los programas de capacitación.

Principio 2: Los bancos deben desarrollar, implementar y mantener un marco de gestión de riesgos operativos (ORMF) que esté completamente integrado en los procesos generales de gestión de riesgos del banco. El ORMF adoptado por un banco individual dependerá de una variedad de factores, que incluyen la naturaleza, tamaño, complejidad y perfil de riesgo del banco.

19. El Directorio y la alta dirección del Banco deben comprender la naturaleza y la complejidad de los riesgos inherentes a la cartera de productos, servicios, actividades y sistemas bancarios, lo cual es una premisa fundamental de la buena gestión de riesgos. Esto es particularmente importante para el riesgo operacional, dado que el riesgo operacional es inherente a todos los productos, actividades, procesos y sistemas comerciales.

20. Los componentes del ORMF deben estar completamente integrados en los procesos generales de gestión de riesgos del banco por la primera línea de defensa, revisados y cuestionados adecuadamente por la segunda línea de defensa, y revisados independientemente por la tercera línea de defensa. El ORMF debe integrarse en todos los niveles de la organización, incluidas las unidades de grupo y de negocio como

12 Véanse también el Informe del Comité sobre la gama de metodologías para la alineación de riesgo y desempeño de la remuneración, mayo de 2011; Principios del Foro de Estabilidad Financiera para prácticas sólidas de compensación, abril de 2009; los principios del FSB de la Junta de Estabilidad Financiera para prácticas sólidas de compensación - estándares de implementación, septiembre de 2009 y el conjunto de herramientas de la Junta de Estabilidad Financiera "Fortalecimiento de los marcos de gobernanza para mitigar el riesgo de mala conducta", abril de 2018.

así como productos, actividades, procesos y sistemas de nuevas iniciativas empresariales. Además, los resultados de la evaluación del riesgo operativo del banco deben incorporarse en el proceso general de desarrollo de la estrategia comercial del banco.

21. El ORMF debe documentarse de manera integral y apropiada en las políticas aprobadas por el Directorio e incluir definiciones de riesgo operacional y pérdida operativa. Los bancos que no describen y clasifican adecuadamente el riesgo operacional y la exposición a pérdidas pueden reducir significativamente la efectividad de su ORMF.

22. La documentación de ORMF debe claramente:

a) Identificar las estructuras de gobernanza utilizadas para gestionar el riesgo operacional, incluidas las líneas de presentación de informes y las responsabilidades, y los mandatos y miembros de los comités de gobernanza del riesgo operativo;

b) Hacer referencia a las políticas y procedimientos relevantes de gestión de riesgos operacionales;

c) Describa las herramientas para la identificación y evaluación de riesgos y controles y el papel y las responsabilidades de las tres líneas de defensa en su uso;

d) Describa el apetito y la tolerancia aceptados por el riesgo operacional del banco; los umbrales, disparadores de actividad o límites para el riesgo inherente y residual; y las estrategias e instrumentos de mitigación de riesgos aprobados;

e) Describir el enfoque del banco para garantizar que los controles se diseñen, implementen y operen de manera efectiva;

f) Describa el enfoque del banco para establecer y monitorear umbrales o límites de exposición al riesgo inherente y residual;

g) Riesgos de inventario y controles implementados por todas las unidades de negocio (por ejemplo, en una biblioteca de control);

h) Establecer informes de riesgos y sistemas de información de gestión (MIS) que produzcan datos precisos y oportunos;

i) Proporcione una taxonomía común de términos de riesgo operacional para garantizar la coherencia de la identificación del riesgo, la calificación de exposición y los objetivos de gestión del riesgo en todas las unidades de negocios.[13]La taxonomía puede distinguir las exposiciones al riesgo operacional por tipo de evento, causas, materialidad y unidades de negocio donde ocurren; también puede marcar aquellas exposiciones operativas que representan parcial o totalmente riesgos legales (incluida la conducta), modelo y TIC (incluidos los cibernéticos), así como exposiciones en el límite de riesgo de crédito o de mercado;

j) Proporcionar una revisión independiente apropiada y el desafío de los resultados del proceso de gestión de riesgos; y

k) Exigir que las políticas sean revisadas y revisadas según corresponda en función de la evaluación continua de la calidad del entorno de control que aborde los cambios ambientales internos y externos o cuando ocurra un cambio importante en el perfil de riesgo operativo del banco.

13 Una taxonomía inconsistente de los términos de riesgo operacional puede aumentar la probabilidad de que no se identifiquen y clasifiquen los riesgos, o que no se asigne la responsabilidad de la evaluación, monitoreo, control y mitigación de riesgos. Para el caso particular de riesgo cibernético, el Ciber Léxico del Consejo de Estabilidad Financiera publicado en noviembre de 2018 debe usarse como punto de partida.

Gobernancia[14]

El Directorio

Principio 3: El Directorio debe supervisar los riesgos operacionales importantes y la eficacia de los controles clave, y garantizar que la alta dirección implemente las políticas, procesos y sistemas del ORMF de manera efectiva en todos los niveles de decisión.

23. El Directorio debe:

    a) Asegúrese de que el banco tenga procesos adecuados para comprender la naturaleza y el alcance del riesgo operacional inherente a las estrategias y actividades actuales y planificadas del banco;

    b) Asegurarse de que los procesos de gestión de riesgos operacionales estén sujetos a una supervisión integral y dinámica y que estén completamente integrados o coordinados con el marco general para gestionar todos los riesgos en toda la empresa;

    c) Brindar a la alta dirección una orientación clara sobre los principios subyacentes de la ORMF y garantizar que las políticas correspondientes desarrolladas por la alta dirección estén alineadas con estos principios;

    d) Desafíe regularmente a la alta gerencia sobre el diseño y la efectividad del ORMF del banco y apruebe y revise el ORMF para asegurarse de que el banco haya identificado y esté gestionando el riesgo operacional derivado de los cambios externos del mercado y otros factores ambientales, así como los riesgos operacionales asociados con nuevos productos, actividades, procesos o sistemas, incluidos cambios en los perfiles y prioridades de riesgo (por ejemplo, cambios en los volúmenes de negocios);

    e) Asegúrese de que el ORMF del banco esté sujeto a una revisión independiente efectiva por una tercera línea de defensa (auditoría u otros terceros independientes debidamente capacitados de fuentes externas); y

    f) Asegúrese de que, a medida que evolucionan las mejores prácticas, la administración esté aprovechando estos avances.[15]

24. Los controles internos fuertes son un aspecto crítico de la gestión del riesgo operacional. El Directorio debe establecer líneas claras de responsabilidad de gestión y responsabilidad para implementar un entorno de control sólido. Los controles deben ser revisados, monitoreados y probados regularmente para asegurar la efectividad continua. El entorno de control debe proporcionar la independencia/separación adecuada de funciones entre las funciones de gestión de riesgos operacional, las unidades de negocio y las funciones de soporte.

Principio 4: El Directorio debe aprobar y revisar periódicamente una declaración de apetito de riesgo y tolerancia para el riesgo operacional que articula la naturaleza, los tipos y los niveles de riesgo operacional que el banco está dispuesto a asumir.

25. El apetito por el riesgo y la declaración de tolerancia para el riesgo operacional deben desarrollarse bajo la autoridad del directorio y vincularse a la estrategia estratégica y a corto y largo plazo del banco.

14 Véanse también los Principios del Comité para mejorar el gobierno corporativo, octubre de 2010.

15 Véanse la Convergencia internacional de medidas y estándares de capital de 2006 del Comité: un marco revisado - Versión completa; párrafo 718 (xci).

16 Véanse las pautas de gobierno corporativo de 2015 del Comité, que utilizan la definición de "Principios para un marco de apetito de riesgo efectivo" del FSB de 2013: el nivel agregado y los tipos de riesgo que un banco está dispuesto a asumir, decidido de antemano y dentro de su capacidad de riesgo, para lograr sus objetivos estratégicos y plan de negocios. La "tolerancia al riesgo" es la variación en torno al apetito de riesgo prescrito que el banco está dispuesto a tolerar.

planes financieros Teniendo en cuenta los intereses de los clientes y accionistas del banco, así como los requisitos reglamentarios, una declaración efectiva de apetito de riesgo y tolerancia debería:

a) Ser fácil de comunicar y, por lo tanto, fácil de entender para todos los interesados;
b) Incluya información de antecedentes clave y suposiciones que informaron los planes comerciales del banco en el momento en que fue aprobado;
c) Incluya declaraciones que articulen claramente las motivaciones para asumir o evitar ciertos tipos de riesgo, y establezca límites o indicadores (que pueden ser cuantitativos o no) para permitir el monitoreo de estos riesgos;
d) Asegurar que la estrategia y los límites de riesgo de cada unidad de negocio y entidad legal, según corresponda, se alineen con la declaración de apetito de riesgo a nivel bancario
e) Sea prospectivo y, cuando corresponda, esté sujeto a pruebas de escenarios y estrés para asegurarse de que el banco comprenda qué eventos podrían empujarlo fuera de su declaración de apetito de riesgo y tolerancia

26. El Directorio debe aprobar y revisar periódicamente la idoneidad de los límites y la declaración general de apetito y tolerancia al riesgo operacional. Esta revisión debe considerar los cambios actuales y esperados en el entorno externo (incluido el contexto normativo en todas las jurisdicciones donde la institución proporciona servicios); aumentos continuos o futuros del material en los volúmenes de negocios o actividades; la calidad del ambiente de control; la efectividad de la gestión de riesgos o estrategias de mitigación; experiencia de pérdida; y la frecuencia, volumen o naturaleza de las infracciones de límite. El directorio debe monitorear la adherencia de la gerencia a la declaración de apetito de riesgo y tolerancia y proporcionar detección oportuna y remediación de infracciones.

Alta Gerencia

Principio 5: La alta gerencia debe desarrollar para la aprobación del Directorio una estructura de gobierno clara, efectiva y sólida con líneas de responsabilidad bien definidas, transparentes y consistentes. La alta gerencia es responsable de implementar y mantener consistentemente en toda la organización políticas, procesos y sistemas para administrar el riesgo operacional en todos los productos, actividades, procesos y sistemas materiales del banco de acuerdo con la declaración de tolerancia y apetito de riesgo del banco.

27. La alta gerencia es responsable de establecer y mantener mecanismos sólidos de revisión y procesos efectivos de resolución de problemas. Estos deben incluir sistemas para informar, rastrear y, cuando sea necesario, escalar problemas para garantizar la resolución. Los bancos deben poder demostrar que el enfoque de tres líneas de defensa está funcionando satisfactoriamente y explicar cómo el directorio, la auditoría independiente del directorio y la alta gerencia se aseguran de que este enfoque se implemente y opere de manera adecuada.
28. La alta gerencia debe traducir el ORMF aprobado por el directorio en políticas y procedimientos específicos que puedan implementarse y verificarse dentro de las diferentes unidades de negocios. La alta gerencia debe asignar claramente las relaciones de autoridad, responsabilidad y presentación de informes para alentar y mantener la rendición de cuentas, y para garantizar que los recursos necesarios estén disponibles para gestionar el riesgo operativo de acuerdo con el apetito de riesgo y la declaración de tolerancia del banco. Además, la alta gerencia debe asegurarse de que el proceso de supervisión de la administración sea apropiado para los riesgos inherentes a la actividad de una unidad de negocios.
29. La alta gerencia debe garantizar que el personal responsable de administrar el riesgo operativo se coordine y se comunique de manera efectiva con el personal responsable de administrar el crédito, el mercado y otros riesgos, así como con aquellos que en el Banco que son responsables de la adquisición de servicios externos

como transferencia de riesgo de seguro y otros acuerdos de terceros (incluida la contratación externa). De lo contrario, podrían producirse lagunas o superposiciones significativas en el programa general de gestión de riesgos de un banco.

30. Los gerentes del CORF deben tener la estatura suficiente dentro del banco para desempeñar sus funciones de manera efectiva, idealmente evidenciadas por un título que sea acorde con otras funciones de gestión de riesgos como el riesgo de crédito, mercadas y liquidez.

31. La alta gerencia debe garantizar que las actividades bancarias sean realizadas por personal con la experiencia necesaria, las capacidades técnicas y el acceso a los recursos. El personal responsable de supervisar y hacer cumplir el cumplimiento de la política de riesgos de la institución debe tener autoridad independiente de las unidades que supervisan.

32. La estructura de gobierno de un banco debe ser acorde con la naturaleza, el tamaño, la complejidad y el perfil de riesgo de sus actividades. Al diseñar la estructura de gobernanza del riesgo operativo, un banco debe tener en cuenta lo siguiente:

a) Estructura del comité: la práctica sólida de la industria es para organizaciones más grandes y complejas con una función de grupo central y unidades de negocio separadas para utilizar un comité de riesgo de nivel empresarial creado por el directorio para supervisar todos los riesgos, al que reporta un comité de riesgo operativo de nivel gerencial. Dependiendo de la naturaleza, tamaño y complejidad del banco, el comité de riesgo a nivel de empresa puede recibir aportes de los comités de riesgo operacional por país, negocio o área funcional. Las organizaciones más pequeñas y menos complejas pueden utilizar una estructura organizativa más plana que supervise el riesgo operacional directamente dentro del comité de gestión de riesgos del Directorio;

b) Composición del comité: una buena práctica de la industria es que los comités de riesgo operacional (o el comité de riesgo en bancos más pequeños) incluyan miembros con una variedad de experiencia, que deben cubrir actividades financieras, asuntos legales, tecnológicos y regulatorios, y gestión de riesgos; y

c) Operación del comité: las reuniones del comité deben celebrarse en las frecuencias apropiadas con tiempo y recursos adecuados para permitir una discusión productiva y la toma de decisiones. Los registros de las operaciones del comité deben ser adecuados para permitir la revisión y evaluación de la efectividad del comité.

Ambiente de gestión de riesgos

Identificación y evaluación

Principio 6: La alta gerencia debe garantizar la identificación y evaluación integrales del riesgo operacional inherente a todos los productos, actividades, procesos y sistemas materiales para asegurarse de que los riesgos e incentivos inherentes se entiendan bien.

33. La identificación y evaluación de riesgos son características fundamentales de un sistema efectivo de gestión de riesgos operacionales. La identificación efectiva de riesgos considera tanto factores internos como factores externos.

17 Consulte los principios de Gobierno Corporativo 2015 del Comité para bancos para conocer los requisitos adicionales sobre la composición del Comité.

Una evaluación de riesgos sólida le permite al banco comprender mejor su perfil de riesgos y asignar recursos y estrategias de gestión de riesgos de la manera más efectiva.

34. Los ejemplos de herramientas utilizadas para identificar y evaluar el riesgo operacional incluyen:

a) Datos de eventos de riesgo operacional: los bancos a menudo mantienen un conjunto completo de datos de eventos de riesgo operacional que recopila toda la experiencia de eventos materiales del banco y sirve como base para las evaluaciones de riesgos operacionales. El conjunto de datos de eventos generalmente incluye datos de pérdidas internas, casi errores y, cuando sea factible, datos de eventos de pérdidas operativas externas (ya que los datos externos son informativos de los riesgos comunes en toda la industria). Los datos de eventos generalmente se clasifican de acuerdo con una taxonomía definida en las políticas de ORMF y se aplican consistentemente en todo el banco. Los datos de eventos generalmente incluyen la fecha del evento (fecha de ocurrencia, fecha de descubrimiento y fecha contable) y, en el caso de eventos de pérdida, impacto financiero. Cuando está disponible otra información de causa raíz para eventos, idealmente también se puede incluir en el conjunto de datos de riesgo operativo. Cuando sea factible,

b) Autoevaluaciones: los bancos a menudo realizan autoevaluaciones de sus riesgos operacional y controles en varios niveles diferentes. Las evaluaciones generalmente evalúan el riesgo inherente (el riesgo antes de considerar los controles), la efectividad del entorno de control y el riesgo residual (la exposición al riesgo después de considerar los controles) y contienen elementos tanto cuantitativos como cualitativos. El elemento cualitativo refleja la consideración tanto de la probabilidad como de la consecuencia del evento de riesgo en la determinación del banco de sus calificaciones de riesgo inherente y residual. Las evaluaciones pueden utilizar el mapeo de procesos comerciales para identificar los pasos clave en los procesos comerciales, actividades y funciones organizacionales, así como los riesgos asociados y las áreas de debilidad de control. Las evaluaciones contienen información suficientemente detallada sobre el entorno comercial, riesgos operativos, causas subyacentes, controles y evaluación de la efectividad del control para permitir que un revisor independiente determine cómo el banco alcanzó sus calificaciones. Se puede mantener un registro de riesgos para recopilar esta información para formar una visión significativa de la efectividad general de los controles y facilitar la supervisión por parte de la alta gerencia, los comités de riesgos y la junta directiva.

c) Gestión de eventos: cuando los bancos experimentan un evento de riesgo operativo, el proceso de identificación, análisis, gestión de end-to-end e informes del evento sigue un conjunto predeterminado de protocolos. Un enfoque sólido de gestión de eventos generalmente incluye el análisis de eventos para identificar nuevos riesgos operativos, comprender las causas subyacentes y controlar las debilidades, y formular una respuesta adecuada para evitar la recurrencia de eventos similares. Esta información es un insumo para la autoevaluación y, en particular, para la evaluación de la efectividad del control.

d) Monitoreo del control y marco de aseguramiento: la incorporación de un monitoreo del control y garantía de control adecuado facilita un enfoque estructurado para la evaluación, revisión y monitoreo y prueba continuos de los controles clave. El análisis de los controles garantiza que estos estén diseñados adecuadamente para los riesgos identificados y que funcionen de manera efectiva. El análisis también debe considerar la suficiencia de la cobertura de control, incluidas las estrategias adecuadas de prevención, detección y respuesta. El monitoreo y las pruebas de control deben ser apropiados para los diferentes riesgos operativos y controles clave en todas las áreas de negocio.

e) Métricas: utilizando datos de eventos de riesgo operacional y evaluaciones de riesgo y control, los bancos a menudo desarrollan métricas para evaluar y monitorear su exposición al riesgo operacional. Estas métricas pueden ser indicadores simples, como el recuento de

18 Esta lista no es exhaustiva y no refleja la diversidad completa de sofisticación de los posibles análisis. Debe ser visto como indicativo (y no limitativo).

eventos, o el resultado de modelos de exposición más sofisticados cuando sea apropiado. Las métricas proporcionan información de advertencia temprana para monitorear el desempeño continuo del negocio y el entorno de control, y para informar el perfil de riesgo operativo. Las métricas efectivas se vinculan claramente con los riesgos y controles operativos asociados. Monitorear las métricas y las tendencias relacionadas a lo largo del tiempo contra los umbrales o límites acordados proporciona información valiosa para la gestión de riesgos y los informes.

f) Análisis de escenarios: el análisis de escenarios es un método para identificar, analizar y medir una variedad de escenarios, incluidos los eventos de baja probabilidad y alta gravedad, algunos de los cuales podrían provocar graves pérdidas de riesgo operativo. El análisis de escenarios generalmente implica reuniones de taller de expertos en la materia, incluida la alta gerencia, la gestión comercial y el personal de riesgo operacional y otras áreas funcionales como cumplimiento, recursos humanos y gestión de riesgos de TI, para desarrollar y analizar los impulsores y el rango de consecuencias de eventos potenciales. Los aportes al análisis de escenarios típicamente incluirían datos relevantes de pérdidas internas y externas, información de autoevaluaciones, el marco de monitoreo y garantía de control, métricas prospectivas, análisis de causa raíz y el marco del proceso, cuando se utiliza. El proceso de análisis de escenarios podría usarse para desarrollar una gama de consecuencias de eventos potenciales, incluidas las evaluaciones de impacto para fines de gestión de riesgos, que complementan otras herramientas basadas en datos históricos o evaluaciones de riesgos actuales. También podría integrarse con la recuperación ante desastres y los planes de continuidad del negocio, para su uso dentro de las pruebas de resistencia operativa. Dada la subjetividad del proceso del escenario, un marco de gobernanza sólido y una revisión independiente son importantes para garantizar la integridad y la coherencia del proceso. para su uso en pruebas de resistencia operativa. Dada la subjetividad del proceso del escenario, un marco de gobernanza sólido y una revisión independiente son importantes para garantizar la integridad y la coherencia del proceso. para su uso en pruebas de resistencia operativa. Dada la subjetividad del proceso del escenario, un marco de gobernanza sólido y una revisión independiente son importantes para garantizar la integridad y la coherencia del proceso.

g) Análisis comparativo: los análisis comparativos son comparaciones de los resultados de diferentes herramientas de medición y gestión de riesgos implementadas dentro del banco, así como comparaciones de métricas del banco con otras empresas de la industria. Dichas comparaciones se pueden realizar para mejorar la comprensión del perfil de riesgo operacional del banco. Por ejemplo, comparar la frecuencia y la gravedad de las pérdidas internas con las autoevaluaciones puede ayudar al banco a determinar si sus procesos de autoevaluación funcionan de manera efectiva. Los datos del escenario se pueden comparar con los datos de pérdidas internas y externas para obtener una mejor comprensión de la gravedad de la exposición del banco a posibles eventos de riesgo.

35. Los bancos deben asegurarse de que los resultados de las herramientas de evaluación de riesgos operativos sean:

a) Basado en datos precisos, cuya integridad está garantizada por un gobierno sólido y procedimientos sólidos de verificación y validación;

b) Tomado en cuenta adecuadamente en los mecanismos internos de medición de tasas y desempeño, así como para las evaluaciones de oportunidades de negocios;

c) Sujeto a los planes de acción monitoreados por el CORF cuando sea necesario.

<u>Principio 7</u>: La alta gerencia debe garantizar que el proceso de gestión de cambios del banco sea integral, que cuente con los recursos adecuados e incluya evaluaciones continuas de riesgo y control, articuladas adecuadamente entre las líneas de defensa relevantes.

36. En general, la exposición al riesgo operacional de un banco evoluciona cuando un banco inicia un cambio, como participar en nuevas actividades o desarrollar nuevos productos o servicios; entrar en mercados o jurisdicciones desconocidas; implementar procesos comerciales o sistemas tecnológicos nuevos o modificativos; y/o participar en negocios que están geográficamente distantes de la oficina central.

La gestión del cambio debe evaluar la evolución de los riesgos asociados a lo largo del tiempo, desde el inicio hasta la finalización (es decir, durante todo el ciclo de vida de un producto). 19

37. Un banco debe tener políticas y procedimientos que definan el proceso para identificar, administrar, desafiar, aprobar y monitorear el cambio sobre la base de criterios objetivos acordados. La implementación del cambio debe ser monitoreada por controles de supervisión específicos. Las políticas y procedimientos de gestión del cambio deben estar sujetos a una revisión y actualización independiente y regular, y asignar claramente roles y responsabilidades de acuerdo con el modelo de tres líneas de defensa, en particular:

    a) La primera línea de defensa debe realizar evaluaciones de riesgo operacional y control de nuevos productos e iniciativas.

    b) La segunda línea de defensa (CORF) debe desafiar las evaluaciones de riesgo operacional y control de la primera línea de defensa, así como monitorear la implementación de controles apropiados o acciones correctivas. CORF debe cubrir todas las fases de este proceso, desde la identificación y evaluación del cambio requerido, pasando por las fases de toma de decisiones y planificación, hasta la implementación y la revisión posterior a la implementación. Además, CORF debe garantizar que todos los grupos de control relevantes (por ejemplo, finanzas, cumplimiento, legal, negocios, TIC, gestión de riesgos) participen según corresponda.

38. Un banco debe tener políticas y procedimientos para la revisión y aprobación de nuevos productos, actividades, procesos y sistemas. El proceso de revisión y aprobación debe considerar:

    a) Riesgos inherentes, incluidos riesgos legales, TIC y modelo, en el lanzamiento de nuevos productos, servicios, actividades, operaciones en mercados desconocidos y en la implementación de nuevos procesos, personas y sistemas (especialmente cuando se subcontratan);

    b) Cambios en el perfil de riesgo operativo, el apetito y la tolerancia del banco, incluidos los cambios en el riesgo de productos o actividades existentes;

    c) Los controles necesarios, los procesos de gestión de riesgos y las estrategias de mitigación de riesgos;

    d) El riesgo residual;

    e) Cambios en los umbrales o límites de riesgo relevantes; y

    f) Los procedimientos y las métricas para evaluar, monitorear y administrar el riesgo de nuevos productos, servicios, actividades, mercados, jurisdicciones, procesos y sistemas.

39. El proceso de revisión y aprobación debe incluir garantizar que se haya realizado una inversión adecuada para los recursos humanos y la infraestructura tecnológica antes de introducir cambios. Los cambios deben ser monitoreados, durante y después de su implementación, para identificar cualquier diferencia material con respecto al perfil de riesgo operativo esperado y gestionar cualquier riesgo inesperado.

40. Los bancos deben mantener un registro central de sus productos y servicios en la medida de lo posible (incluidos los subcontratados) para facilitar el seguimiento de los cambios.

Monitoreo e informes

Principio 8: La alta gerencia debe implementar un proceso para monitorear regularmente los perfiles de riesgo operacional y las exposiciones operacionales materiales. Deben establecerse mecanismos de notificación adecuados.

19 El ciclo de vida de un producto o servicio abarca varias etapas desde el desarrollo, los cambios continuos, el abuelo y el cierre. De hecho, el nivel de riesgo puede aumentar, por ejemplo, cuando nuevos productos, actividades, procesos o sistemas pasan de un nivel introductorio a un nivel que representa fuentes materiales de ingresos u operaciones críticas para el negocio.

en los niveles del Directorio, la alta gerencia y las unidades de negocios para respaldar la gestión proactiva del riesgo operativo.

41. Los bancos deberían mejorar continuamente la calidad de los informes de riesgo operacional. Un banco debe asegurarse de que sus informes sean completos, precisos, consistentes y procesables en todas las unidades de negocios y productos. Con este fin, la primera línea de defensa debe garantizar la presentación de informes sobre los riesgos operativos residuales, incluidos los eventos de riesgo operativo, las deficiencias de control, las deficiencias del proceso y el incumplimiento de las tolerancias de riesgo operativo. Los informes deben ser manejables en alcance y volumen proporcionando una perspectiva sobre el perfil de riesgo operacional del banco y la adhesión al apetito de riesgo operacional y la declaración de tolerancia; la toma de decisiones efectiva se ve obstaculizada por cantidades excesivas y escasez de datos.

42. La presentación de informes debe ser oportuna y un banco debe ser capaz de producir informes en condiciones de mercado normales y estresadas. La frecuencia de los informes debe reflejar los riesgos involucrados y el ritmo y la naturaleza de los cambios en el entorno operativo. Los resultados de las actividades de monitoreo deben incluirse en los informes regulares de la gerencia y de la junta, al igual que las evaluaciones del ORMF realizadas por las funciones de auditoría interna/externa y/o gestión de riesgos. Los informes generados por o para las autoridades de supervisión también se deben informar internamente a la alta gerencia y al consejo de administración, cuando corresponda.

43. Los informes de riesgo operacional deben describir el perfil de riesgo operacional del banco al proporcionar indicadores financieros, operativos y de cumplimiento internos, así como información externa del mercado o ambiental sobre eventos y condiciones que son relevantes para la toma de decisiones. Los informes de riesgo operativo deben incluir:
    a) Incumplimientos del apetito de riesgo del banco y la declaración de tolerancia, así como umbrales, límites o requisitos cualitativos;
    b) Una discusión sobre el riesgo clave y emergente evaluado y monitoreado por métricas;
    c) Detalles de recientes eventos significativos internos de riesgo operacional y pérdidas (incluyendo análisis de causa raíz);
    d) Eventos externos relevantes o cambios regulatorios y cualquier impacto potencial en el banco.

44. Los procesos de captura de datos e informes de riesgos deben analizarse periódicamente con el objetivo de mejorar continuamente el rendimiento de la gestión de riesgos, así como avanzar en las políticas, procedimientos y prácticas de gestión de riesgos.

Control y Mitigación

Principio 9: Los bancos deberían tener un entorno de control sólido que utilice políticas, procesos y sistemas; controles internos apropiados; y estrategias apropiadas de mitigación y/o transferencia de riesgos.

45. Los controles internos deben estar diseñados para proporcionar una seguridad razonable de que un banco tendrá operaciones eficientes y efectivas; salvaguardar sus activos; producir informes financieros confiables; y cumplir con las leyes y regulaciones aplicables. Un programa de control interno sólido consta de cuatro componentes que son parte integral del proceso de gestión de riesgos: evaluación de riesgos, actividades de control, información y comunicación, y actividades de monitoreo.[20]

46. Los procesos y procedimientos de control deben incluir un sistema para garantizar el cumplimiento de las políticas, regulaciones y leyes. Los ejemplos de elementos principales de una evaluación de cumplimiento de políticas incluyen:

20 El documento del Comité Marco para los sistemas de control interno en las organizaciones bancarias, septiembre de 1998, analiza los controles internos con mayor detalle.

a) Revisiones de alto nivel del progreso hacia los objetivos establecidos;

b) Verificar el cumplimiento de los controles de gestión;

c) Revisión del tratamiento y resolución de instancias de incumplimiento;

d) Evaluación de las aprobaciones y autorizaciones requeridas para garantizar la rendición de cuentas a un nivel adecuado de gestión; y

e) Informes de seguimiento de excepciones aprobadas a umbrales o límites, anulaciones de gestión y otras desviaciones de políticas, regulaciones y leyes.

47. Un entorno de control efectivo también requiere una segregación de tareas adecuada. Las asignaciones que establecen deberes conflictivos para individuos o un equipo, sin controles duales u otras contramedidas, pueden resultar en la ocultación de pérdidas, errores u otras acciones inapropiadas. Por lo tanto, las áreas donde pueden surgir conflictos de interés deben identificarse, minimizarse y estar sujetas a un cuidadoso monitoreo y revisión independientes.

48. Además de la segregación de deberes y controles duales, los bancos deben asegurarse de que existan otros controles internos tradicionales, según corresponda, para abordar el riesgo operativo. Los ejemplos de estos controles incluyen:

a) Autoridades y/o procesos de aprobación claramente establecidos;

b) Vigilancia estrecha de la adherencia a los umbrales o límites de riesgo asignados;

c) Salvaguardas para el acceso y uso de los activos y registros bancarios;

d) Nivel adecuado de personal y capacitación para mantener la experiencia técnica;

e) Procesos en curso para identificar unidades de negocios o productos donde los retornos parecen estar fuera de línea con expectativas razonables;[21]

f) Verificación y conciliación periódica de transacciones y cuentas; y

g) Política de vacaciones que prevé que los funcionarios y empleados estén ausentes de sus funciones por un período no menor de dos semanas consecutivas.

49. El uso efectivo y la implementación sólida de la tecnología pueden contribuir al entorno de control. Por ejemplo, los procesos automatizados son menos propensos a errores que los procesos manuales. Sin embargo, los procesos automatizados introducen riesgos que deben abordarse a través de programas sólidos de gobernanza tecnológica y gestión de riesgos de infraestructura.

50. El uso de productos, actividades, procesos y canales de entrega relacionados con la tecnología expone a un banco a riesgos operacionales, estratégicos y de reputación y la posibilidad de pérdidas financieras importantes. En consecuencia, un banco debe tener un enfoque integrado para identificar, medir, monitorear y administrar los riesgos tecnológicos siguiendo los mismos preceptos que la administración del riesgo operacional.

51. Si bien recurrir a entidades tales como, entre otros, los proveedores de servicios de terceros pueden ayudar a administrar los costos, proporcionar experiencia, ampliar las ofertas de productos y mejorar los servicios, también presenta riesgos que la administración debería abordar. El directorio y la alta gerencia son responsables de comprender los riesgos operativos asociados con los acuerdos de subcontratación y de garantizar que existan políticas y prácticas eficaces de gestión de riesgos para gestionar el riesgo en las actividades de subcontratación. Entre otros, la concentración de riesgo y la

21 Por ejemplo, donde una actividad comercial supuestamente de bajo riesgo y bajo margen genera altos retornos que podrían cuestionar si dichos retornos se han logrado como resultado de una violación del control interno.

La complejidad de la subcontratación debe tenerse en cuenta. Políticas de riesgo de terceros y actividades de gestión de riesgos.22 debe abarcar:

a) procedimientos para determinar si las actividades se pueden externalizar y cómo;

b) procesos para llevar a cabo la debida diligencia en la selección de posibles proveedores de servicios;

c) estructuración sólida del acuerdo de subcontratación, incluida la propiedad y confidencialidad de los datos, así como los derechos de terminación;

d) programas para administrar y monitorear los riesgos asociados con el acuerdo de subcontratación, incluida la condición financiera del proveedor de servicios;

e) establecimiento de un entorno de control efectivo en el banco y el proveedor de servicios (lo que debe incluir un registro de actividades tercerizadas);

f) desarrollo de planes de contingencia viables;

g) ejecución de contratos integrales y / o acuerdos de nivel de servicio con una clara asignación de responsabilidades entre el proveedor de outsourcing y el banco.

52. En aquellas circunstancias en las que los controles internos no abordan adecuadamente el riesgo y salir del riesgo no es una opción razonable, la administración puede complementar los controles buscando transferir el riesgo a otra parte, como a través de un seguro. El consejo de administración debe determinar la exposición máxima a pérdidas que el banco está dispuesto y tiene la capacidad financiera para asumir, y debe realizar una revisión anual del programa de gestión de riesgos y seguros del banco. Si bien las necesidades específicas de seguro o transferencia de riesgos de un banco deben determinarse de manera individual, muchas jurisdicciones tienen requisitos reglamentarios que deben considerarse.

53. Debido a que la transferencia de riesgos es un sustituto imperfecto de controles sólidos y programas de gestión de riesgos, los bancos deberían ver las herramientas de transferencia de riesgos como un complemento, en lugar de un reemplazo, para un control interno exhaustivo del riesgo operacional. Tener mecanismos para identificar, reconocer y rectificar rápidamente los distintos errores de riesgo operacional, o la exposición específica al riesgo legal, puede reducir en gran medida las exposiciones. También se debe considerar cuidadosamente la medida en que las herramientas de mitigación de riesgos, como los seguros, realmente reducen el riesgo, transfieren el riesgo a otro sector o área comercial, o crean un nuevo riesgo (por ejemplo, riesgo de contraparte).

54. Los bancos deben tener una clasificación unificada, metodología, procedimientos de gestión del riesgo operacional establecidos por el CORF.

Tecnología de la información y la comunicación

Principio 10: Los bancos deberían implementar una gobernanza solida de TIC[23] que sea coherente con su apetito por el riesgo y la declaración de tolerancia para el riesgo operacional y garantice que sus TIC respalden y faciliten completamente sus operaciones. Las TIC deben estar sujetas a los programas apropiados de identificación, protección, detección, respuesta y recuperación de riesgos que se prueban regularmente, incorporan una conciencia situacional adecuada y transmiten información relevante a los usuarios de manera oportuna.

55. El desempeño y la seguridad efectivos de las TIC son primordiales para que un banco realice sus negocios adecuadamente. El uso apropiado y la implementación de un marco sólido de TIC

22 Estas políticas de riesgo y actividades de gestión de riesgos deben ser coherentes y llevadas a cabo junto con la gestión de operaciones críticas y la gestión de dependencia para la resiliencia operativa. Comité de Basilea sobre Supervisión Bancaria, Documento Consultivo - Principios para la resiliencia operativa", 6 de agosto de 2020, https://www.bis.org/bcbs/publ/d509.htm.

23 La tecnología de la información y la comunicación se refiere al diseño físico y lógico subyacente de la tecnología de la información y los sistemas de comunicación, los componentes individuales de hardware y software, los datos y los entornos operativos.

contribuyen a la efectividad del entorno de control y son fundamentales para el logro de los objetivos estratégicos de un banco. El marco de las TIC debería reducir la exposición al riesgo de un banco a pérdidas directas, reclamos legales, daños a la reputación, interrupción de las TIC y mal uso de la tecnología en línea con su apetito de riesgo y declaración de tolerancia.

56. Para garantizar la confidencialidad, integridad y disponibilidad de los datos y los sistemas, el directorio y la alta gerencia deben evaluar de forma rutinaria el diseño, la implementación y la eficacia del marco de las TIC. Esto requiere una alineación regular de las estrategias de negocios, gestión de riesgos y TIC para ser coherente con el apetito de riesgo y la declaración de tolerancia del banco, así como con la privacidad y otras leyes aplicables. Los bancos deben monitorear continuamente sus TIC e informar periódicamente a la alta gerencia sobre los riesgos, controles y eventos de las TIC.

57. El marco de las TIC junto con los procesos complementarios establecidos por los bancos deberían:

a) Ser revisado periódicamente para verificar su integridad con respecto a los estándares y las mejores prácticas relevantes de la industria, así como contra las amenazas en evolución (por ejemplo, cibernéticas) y las tecnologías nuevas o en evolución;
b) Ser probado regularmente como parte de un programa para identificar brechas contra los objetivos establecidos de tolerancia al riesgo y facilitar la mejora de la identificación, protección, detección y gestión de eventos de riesgos de las TIC;
c) Utilice la inteligencia procesable para mejorar continuamente su conciencia situacional de las vulnerabilidades a los sistemas, redes y aplicaciones de las TIC y facilitar la toma de decisiones efectiva en la gestión de riesgos o cambios.

Planificación de la Continuidad del Negocio

Principio 11: Los bancos deben tener planes de continuidad del negocio establecidos para garantizar su capacidad de operar de manera continua y limitar las pérdidas en caso de una interrupción grave del negocio.[24]

58. Gobierno sólido y efectivo de la política de continuidad del negocio de los bancos[25] requiere:

a) La validación y revisión periódica por parte del Directorio;
b) La fuerte participación de la gerencia general y los líderes de las unidades de negocios en su implementación;
c) El compromiso de primera y segunda línea de defensa con su diseño.
d) Revisión periódica por la tercera línea de defensa.

59. Los bancos deben preparar planes de continuidad del negocio (BCP) con visión de futuro con análisis de escenarios asociados con evaluaciones de impacto relevantes y procedimientos de recuperación.

a) Un banco debe basar su política de continuidad del negocio en análisis de escenarios de posibles interrupciones que identifiquen y clasifiquen las operaciones comerciales críticas y las dependencias internas o externas clave. Al hacerlo, los bancos deben cubrir todas sus unidades de negocio, así como los proveedores críticos y los principales terceros (por ejemplo, bancos centrales, cámaras de compensación).

24 El documento del Comité, Principios de alto nivel para la continuidad del negocio, agosto de 2006, analiza los principios de continuidad de sonido con mayor detalle.

25 La planificación de la continuidad del negocio debe ser coherente y llevarse a cabo junto con la planificación de la continuidad del negocio y las pruebas de las operaciones críticas, tal como se especifica en los principios de resistencia operativa. Comité de Basilea sobre Supervisión Bancaria, Documento Consultivo - Principios para la resiliencia operativa, agosto de 2020

b) Cada escenario debe estar sujeto a una evaluación de impacto cuantitativa y cualitativa o análisis de impacto empresarial (BIA) con respecto a sus consecuencias financieras, operativas, legales y de reputación.

c) Cada escenario de interrupción debe estar sujeto a umbrales o límites (como la interrupción máxima tolerable) para la activación de un procedimiento de continuidad. El procedimiento debe abordar aspectos de reanudación, establecer objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO), así como pautas de comunicación para informar a la administración, empleados, autoridades reguladoras, clientes, proveedores y, cuando corresponda, autoridades civiles.

60. Un banco debe revisar periódicamente todos los componentes de su política de continuidad del negocio para garantizar que las estrategias de contingencia permanezcan consistentes con las operaciones, riesgos y amenazas actuales. Los programas de capacitación y sensibilización deben personalizarse en función de roles específicos para garantizar que el personal pueda ejecutar con eficacia los planes de contingencia. Los procedimientos de continuidad del negocio deben probarse periódicamente para garantizar que se puedan cumplir los objetivos y plazos de recuperación y reanudación. Siempre que sea posible, un banco debe participar en las pruebas de continuidad del negocio con proveedores de servicios clave. Los resultados de las pruebas formales y las actividades de revisión deben informarse a la alta gerencia y al directorio.

Rol de Divulgación

Principio 12: Las divulgaciones públicas de un banco deberían permitir a las partes interesadas evaluar su enfoque para la gestión del riesgo operacional y su exposición al riesgo operacional.

61. La divulgación pública de un banco de información relevante de gestión de riesgos operacionales puede conducir a la transparencia y al desarrollo de mejores prácticas de la industria a través de la disciplina de mercado. La cantidad y el tipo de divulgación deben ser proporcionales al tamaño, el perfil de riesgo y la complejidad de las operaciones de un banco y la evolución de la práctica de la industria.

62. Los bancos deben divulgar información relevante sobre la exposición al riesgo operacional a sus partes interesadas (incluidos los eventos de pérdida operacional significativos), sin crear riesgos operacionales a través de esta divulgación (por ejemplo, descripción de vulnerabilidades de control no abordadas). Un banco debe divulgar su ORMF de manera que permita a las partes interesadas determinar si el banco identifica, evalúa, monitorea y controla/mitiga el riesgo operativo de manera efectiva.

63. Los bancos deben tener una política de divulgación formal que esté sujeta a una revisión periódica e independiente y a la aprobación del directorio y la alta gerencia. La política debe abordar el enfoque del banco para determinar qué divulgaciones de riesgo operacional realizará y los controles internos sobre el proceso de divulgación. Además, los bancos deben implementar un proceso para evaluar la idoneidad de sus divulgaciones y su política de divulgación.

Rol de los supervisores

64. Los supervisores deben evaluar regularmente el ORMF de los bancos evaluando las políticas, procesos y sistemas de los bancos relacionados con el riesgo operativo. Los supervisores deben asegurarse de que existan mecanismos apropiados que les permitan estar al tanto de la evolución del riesgo operativo de los bancos.

65. Las evaluaciones de supervisión del riesgo operacional deben incluir todas las áreas descritas en los principios para la gestión racional del riesgo operacional. Cuando los bancos forman parte de un grupo financiero, los supervisores deben asegurarse de que existan procesos para garantizar que el riesgo

Operacional se gestione de forma adecuada e integrada en todo el grupo. Al evaluar el ORMF de los bancos, puede ser necesaria la cooperación y el intercambio de información con otros supervisores, de acuerdo con los procedimientos establecidos.27 En ciertas circunstancias, los supervisores pueden optar por utilizar auditores externos en estos procesos de evaluación.28

66. Los supervisores deben tomar medidas para garantizar que los bancos aborden las deficiencias identificadas a través de la revisión supervisora del ORMF de los bancos. Los supervisores deben usar las herramientas más adecuadas para las circunstancias particulares de los bancos y su entorno operativo. Para garantizar que los supervisores reciban información actualizada sobre el riesgo operativo, los supervisores pueden desear establecer mecanismos de informes directamente con los bancos y auditores externos (por ejemplo, los informes internos de gestión bancaria sobre el riesgo operativo podrían ponerse a disposición de los supervisores de forma rutinaria)

67. Los supervisores deben alentar los esfuerzos continuos de desarrollo interno de los bancos al monitorear, comparar y evaluar las mejoras y planes recientes de los bancos para futuros desarrollos.

27 Consulte los documentos del Comité Principios de alto nivel para la implementación transfronteriza del Nuevo Acuerdo, agosto de 2003, y Principios para la cooperación y mecanismos de asignación de supervisión en el hogar anfitrión en el contexto de Enfoques de medición avanzada (AMA), noviembre de 2007.

28 Para mayor discusión, ver el documento del Comité: La relación entre los supervisores bancarios y los auditores externos del banco, enero de 2002.