PROYECTO DE REFORMAS A LA NORMA DE GESTIÓN DE RIESGO OPERATIVO

CAPÍTULO I
DISPOSICIONES GENERALES

ARTÍCULO 1.- OBJETO

La presente Norma tiene por objeto establecer los principios, criterios generales, responsabilidades y lineamientos mínimos que deben observar las instituciones supervisadas en el diseño, desarrollo y aplicación de su gestión de riesgo operativo, el cual debe incluir su identificación, evaluación, mitigación, monitoreo y comunicación.

ARTÍCULO 2.- ALCANCE

La presente Norma es aplicable a todas las instituciones supervisadas por la Comisión Nacional de Bancos y Seguros (CNBS), en función del tamaño, naturaleza y complejidad de sus operaciones.

ARTÍCULO 3.- DEFINICIONES

Para efectos de la presente Norma, en adición a las definiciones establecidas en la Norma sobre Gestión Integral de Riesgos, serán aplicables las siguientes definiciones:

a) **Comisión o CNBS:** Comisión Nacional de Bancos y Seguros.
b) **Institución(es):** Instituciones Supervisadas por la Comisión.
c) **Evento de Riesgo Operativo:** Suceso o serie de sucesos, de origen interno o externo, que han ocurrido o pueden ocurrir y generar o no pérdidas financieras para la institución.
d) **Factor de Riesgo Operativo:** Causa primaria o el origen de un evento de riesgo operativo. Éstos pueden ser internos como ser recursos humanos, los procesos, la tecnología y la infraestructura, sobre los cuales la organización puede tener un control directo y externos, los cuales son acontecimientos cuyas causas y origen escapan al control de la organización.
e) **Proceso:** Conjunto de actividades secuenciales que describen las acciones llevadas a cabo por personas y sistemas, que transforma insumos en productos o servicios finales para usuarios internos o externos. Todo proceso tiene: a) un dueño o responsable, b) uno o varios insumos, c) uno o varios productos o servicios finales con valor, d) uno o varios usuarios internos o externos; e) riesgos inherentes; f) elementos de mitigación; y g) riesgos residuales.

f) **Infraestructura:** Conjunto de elementos de apoyo para el funcionamiento de una organización, entre otros se incluyen: edificios, espacios de trabajo, almacenamiento y transporte.

g) **Línea de Negocio:** Especialización que agrupa procesos encaminados a generar productos y servicios para atender un segmento del mercado objetivo, definido en la planificación estratégica de la institución.

h) **Matriz de Riesgos Operativos:** Herramienta de control y de gestión que permite realizar un diagnóstico de la situación del riesgo operativo de una institución.

i) **Periodo Máximo Tolerable de Interrupción (RPO) por sus siglas en inglés:** Período de tiempo luego del cual la viabilidad de la institución sería afectada seriamente, si un producto o servicio en particular no es reanudado.

j) **Plan de Continuidad de Negocio:** Plan orientado a asegurar la continuidad del negocio, la satisfacción del cliente y la productividad a pesar de eventos inesperados, el cual se ejecuta permanentemente como parte de la administración de riesgos. Dicho plan debe contener procedimientos que se ajusten a la realidad del negocio de cada institución.

k) **Tiempo Objetivo de Recuperación (RTO) por sus siglas en inglés:** Tiempo establecido por la institución para reanudar un proceso, en caso de ocurrencia de un evento de interrupción de operaciones. El RTO es menor al periodo máximo tolerable de interrupción (RPO).

l) **Tercerización:** Modalidad en la que se contrata a un tercero para que éste desarrolle o suministre un determinado producto o servicio, de forma permanente, temporal o intermitente.

CAPÍTULO II
DE LAS RESPONSABILIDADES DE LA ADMINISTRACIÓN EN LA GESTIÓN DEL RIESGO OPERATIVO

ARTÍCULO 4.- ORGANIZACIÓN

La Unidad de Riesgos es la responsable de la gestión del riesgo operativo, tal como lo establece la Norma sobre Gestión Integral de Riesgo y el Reglamento de Gobierno Corporativo para las Instituciones Supervisadas. Asimismo, el Comité de Riesgos debe velar por una adecuada gestión de este riesgo.

ARTÍCULO 5.- ESTRATEGIA

Las instituciones deben definir la estrategia para gestionar el riesgo operativo, para ello deben establecer una metodología que permita llevar a cabo la identificación, evaluación, mitigación, monitoreo y comunicación de los eventos de riesgo operativo, tanto internos como externos que se hayan producido (incidencias) o que se puedan producir (eventos potenciales).

En virtud que todas las áreas de la institución generan eventos potenciales de riesgo operativo, la estrategia debe ser aprobada por el Directorio e involucrar a todo el personal. Asimismo, dicha estrategia debe ser actualizada periódicamente en función a la tolerancia al riesgo y a los cambios en los procesos internos, en el mercado y en el entorno económico que puedan afectar la operatividad de la institución. Es importante señalar que la estrategia debe establecer los recursos adecuados en términos de personal capacitado, sistemas de información y todo el ambiente necesario para la gestión de este riesgo.

ARTÍCULO 6.- RESPONSABILIDADES DEL DIRECTORIO

En adición a las funciones y responsabilidades establecidas en el marco normativo aplicable sobre la gestión integral de riesgos, corresponde al Directorio asegurar un ambiente adecuado para la gestión del riesgo operativo, dentro de las cuales se señalan las siguientes:

a) Crear una cultura organizacional con principios y valores de comportamiento ético que priorice la gestión eficaz del riesgo operativo;
b) Aprobar las políticas y procedimientos, así como la metodología y el manual para la gestión de riesgo operativo; cuya periodicidad mínima de revisión será anual o cada vez que se produzcan a juicio de la institución, hechos o situaciones de relevancia vinculadas con este riesgo;
c) Aprobar el plan y los recursos necesarios para la administración y el adecuado desarrollo de la gestión de la continuidad del negocio y de seguridad de la información, a fin de contar con la infraestructura, metodología y personal calificado;
d) Tener conocimiento de los principales riesgos operativos, niveles de exposición, sus implicaciones y actividades relevantes para su mitigación, para lo cual deberá recibir por parte del comité de riesgos información periódica y suficiente que le permita analizar el perfil de riesgo de la institución;

e) Definir en términos cuantitativos, su apetito y nivel de tolerancia al riesgo operativo;
f) Asegurar que la gestión del riesgo operativo se encuentra dentro de los límites establecidos; y,
g) Asegurar que la gestión del riesgo operativo este sujeto a un proceso de auditoría interna que contemple una adecuada cobertura y profundidad de las revisiones y adopción oportuna de medidas correctivas por parte de las áreas auditadas.

ARTÍCULO 7.- RESPONSABILIDADES DE LA ALTA GERENCIA

En adición a las funciones y responsabilidades establecidas en el marco normativo aplicable sobre la gestión integral de riesgos, la Alta Gerencia es responsable de implementar la gestión de riesgo operativo conforme a las disposiciones aprobadas por el Directorio, dentro de las cuales se encuentran las siguientes:

a) Desarrollar y promover, en coordinación con el Directorio, una cultura organizacional de gestión del riesgo operativo y de la implementación de prácticas adecuadas de controles internos, incluyendo estándares de conducta, integridad y ética para todos los empleados, asignación de recursos, incentivos ligados a la asunción de riesgos, y programas de capacitación;
b) Implementar la gestión de la continuidad del negocio conforme a las disposiciones aprobadas por el Directorio;
c) Administrar el proceso de gestión de riesgo operativo en toda la institución y asegurar su integridad de acuerdo a los lineamientos establecidos por el Directorio;
d) Asegurar que se cumpla con las estrategias y objetivos de la gestión de riesgo operativo; y,
e) Establecer claras líneas de autoridad, responsabilidad y comunicación con las distintas gerencias para fomentar y mantener la asunción de responsabilidad.

ARTÍCULO 8.- RESPONSABILIDADES DEL COMITÉ DE RIESGOS

En adición a las funciones y responsabilidades establecidas en el marco normativo aplicable sobre la gestión integral de riesgos, corresponde al Comité de Riesgos, de manera directa o a través de un sub Comité de Riesgo Operativo, desempeñar como mínimo las siguientes funciones:

a) Evaluar, revisar y proponer para aprobación del Directorio, las políticas, procedimientos, metodología y el manual de gestión del riesgo operativo;

b) Asegurar que se mantiene un proceso de gestión de riesgo operativo adecuado y mantener informado al Directorio sobre su efectividad;
c) Supervisar que el riesgo operativo sea efectivamente, identificado, evaluado, mitigado, monitoreado y comunicado a los diferentes niveles de la institución;
d) Supervisar que todas las unidades de la institución, cumplan con su labor en la implementación de la metodología de gestión del riesgo operativo;
e) Proponer los mecanismos para la implementación de las acciones correctivas requeridas en caso de que existan desviaciones con respecto al nivel de tolerancia del riesgo operativo; y,
f) Apoyar la labor de la Unidad de Riesgos.

ARTÍCULO 9.- UNIDAD DE RIESGOS

En adición a las funciones y responsabilidades establecidas en el marco normativo aplicable sobre la gestión integral de riesgos, corresponde a la Unidad de Riesgos:

a) Diseñar y someter a aprobación del Directorio, a través del Comité de Riesgos, las políticas y procedimientos para la gestión de riesgo operativo, su metodología, y la estructura idónea para su gestión;
b) Coordinar la implementación de la metodología de gestión de riesgo operativo, así como, apoyar a las demás unidades de la institución para dicha implementación;
c) Emitir informes con una periodicidad al menos bimensual, sobre los eventos de riesgo operativo, violaciones o excesos ocurridos sobre los límites establecidos, los resultados de la medición de los indicadores claves de riesgo operativo, y cualquier otra alerta que conlleve a un evento que pueda afectar severamente a la institución;
d) Elaborar una opinión sobre el riesgo operativo de los nuevos productos y servicios o modificación de los mismos, previo a su lanzamiento, así como ante cambios importantes en el ambiente operativo o tecnológico; y,
e) Asegurar que la gestión del plan de continuidad del negocio sea consistente con las políticas y procedimientos aplicados para la gestión integral de riesgos.

ARTÍCULO 10.- UNIDAD DE AUDITORÍA INTERNA

Corresponde a la Unida de Autoría Interna evaluar la efectividad y el nivel de cumplimiento de las políticas, procedimientos y metodología utilizados para la gestión de riesgo operativo. Dicha evaluación de efectividad y cumplimiento deberá estar contenida en su Plan Anual de Trabajo.

La función de auditoría interna no debe ser la de gestionar directamente el riesgo operativo, y debe proporcionar un valor agregado a la gestión de riesgo operativo que realiza la institución, ejecutando revisiones a la efectividad de este proceso en todas sus etapas y componentes.

CAPÍTULO III
DE LA GESTIÓN DE RIESGO OPERATIVO

ARTÍCULO 11.- DEFINICIÓN DE RIESGO OPERATIVO

Para efectos de la presente Norma se entiende como Riesgo Operativo la posibilidad de ocurrencia de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información, la infraestructura o eventos externos. Se incluye de éste, el riesgo legal, pero excluye el riesgo estratégico y de reputación.

ARTÍCULO 12.- FACTORES DE RIESGO OPERATIVO

Para efectos de la presente Norma se consideran factores de riesgo operativo, los siguientes:

a) Recursos Humanos: Las instituciones 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, ausencia de planes de capacitación, negligencia, error humano, sabotaje, fraude, robo, apropiación de información sensible, nepotismo, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal, entre otros.

b) Procesos Internos: Con el objeto de garantizar la optimización de los recursos y la estandarización de las actividades, las instituciones deben contar con procesos definidos, documentados y actualizados permanentemente, que pueden ser agrupados en procesos estratégicos y procesos productivos u operativos.

Las instituciones 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.

c) Tecnología de la Información: Las instituciones deben contar con la tecnología de información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; así como, evitar interrupciones del negocio y lograr 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 vigentes establecidos por la Comisión en esta materia, así como con las mejores prácticas internacionales relacionadas.

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

ARTÍCULO 13.- DE LA GESTIÓN DEL RIESGO OPERATIVO

El proceso de gestión de riesgo operativo comprende las etapas de identificación, evaluación, mitigación y monitoreo de los eventos de riesgo operativo. A dicho proceso debe añadirse un mecanismo de comunicación y retroalimentación; y, en caso de determinarse un nivel significativo de pérdidas potenciales, un respaldo patrimonial. El proceso de gestión debe estar documentado, tanto en la matriz de riesgo operativo, como en el Manual de Gestión de Riesgo correspondiente.

ARTÍCULO 14.- DE LA IDENTIFICACIÓN

Las instituciones supervisadas deben identificar los eventos de riesgo operativo, para ello deben contar con todos los procesos claramente definidos y documentados. En caso de no contar con los mismos en su totalidad, la identificación debe realizarse por áreas o unidades en tanto se definen los mismos en un período de tiempo razonable. Los eventos identificados deben agruparse de acuerdo al Anexo No.1 de la presente Norma, de la siguiente manera:

a) Fraude Interno: Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir regulaciones, leyes o políticas internas en las que se encuentra implicados empleados de la institución, y que tiene como fin obtener un beneficio ilícito.

b) Fraude Externo: Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de un activo indebidamente o incumplir la legislación, por parte de un tercero, con el fin de obtener un beneficio ilícito.

c) **Relaciones Laborales y Seguridad en el Puesto de Trabajo:** Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, el pago de reclamos por daños personales, o casos relacionados con la diversidad o discriminación.
d) **Prácticas relacionadas con los Clientes, los Productos y el Negocio:** Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación frente a clientes o de la naturaleza y el diseño de un producto o servicio.
e) **Daños a Activos Físicos:** Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos.
f) **Interrupción del Negocio por fallas en la Tecnología de Información:** Pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas.
g) **Deficiencia en la Ejecución, Entrega y Gestión de Procesos:** Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes (proveedores, clientes, depositantes, etc.).

Asimismo, la identificación de los eventos de pérdida deberá relacionarse a las líneas de negocio que la institución mantiene de acuerdo a su propia naturaleza y giro del negocio. En el Anexo No. 2 de la presente Norma, se consignan las líneas de negocio a las cuales deberán relacionarse los eventos de pérdida, de acuerdo al sector de la institución supervisada.

ARTÍCULO 15.- EVALUACIÓN

Las instituciones deben evaluar los eventos de riesgo operativo identificados, esto implica medir la pérdida o impacto que se produce si el riesgo, previamente identificado, se materializa. La medición debe hacerse considerando la probabilidad de ocurrencia (frecuencia) y el impacto (severidad) en términos monetarios.

La evaluación o medición de la pérdida por eventos de riesgo operativo será determinada, al inicio de la gestión de éste riesgo, de manera cuantitativa, lo que ayudará a establecer un orden en la que los eventos deben ser mitigados. Ante la ausencia de la información histórica, la evolución o medición de la pérdida se realizará de forma cualitativa.

Las instituciones deben evaluar o medir sus eventos de riesgo operativo porque en base a ellos podrán establecer mecanismos de cobertura, así como establecer límites

presupuestarios sobre las medidas de mitigación a implementar, que busquen minimizar las pérdidas estimadas.

ARTÍCULO 16.- MITIGACIÓN

Una vez identificados los eventos de riesgo operativo y su impacto, las instituciones están en la capacidad de decidir si el riesgo se debe asumir, compartir, evitar o transferir, reduciendo sus consecuencias y efectos. Asimismo, tendrán una visión clara de los diferentes tipos de exposición al riesgo operativo y su prioridad. En ese sentido, las instituciones deben establecer un plan de acción para implementar las medidas que busquen mitigar los eventos de riesgo identificados, detallándose las acciones a realizar, el plazo estimado de ejecución y los responsables directos de dicha ejecución. Dentro de dichas acciones, se encuentran las siguientes:

a) Revisar estrategias y políticas;
b) Actualizar o modificar procesos y procedimientos establecidos;
c) Implantar o modificar límites de riesgo;
d) Constituir, incrementar o modificar controles;
e) Implantar planes de contingencias;
f) Revisar términos de pólizas de seguro contratadas;
g) Contratar servicios provistos por terceros; y,
h) Cualquier otra acción que estime pertinente la institución.

ARTÍCULO 17.- MONITOREO

Las instituciones supervisadas deben establecer indicadores de riesgo, tanto descriptivos como prospectivos, que evidencien los potenciales riesgos operativos y su evolución, debiendo a su vez realizar un seguimiento y monitoreo oportuno a dichos indicadores, los cuales deben estar definidos en su metodología. Por medio de las acciones de monitoreo, las instituciones deben asegurar que todas las acciones implementadas para mitigar un evento de riesgo se cumplan en los plazos establecidos y que las medidas adoptadas efectivamente han contribuido a reducir el riesgo potencial por evento y para toda la institución.

ARTÍCULO 18.- COMUNICACIÓN

Las instituciones deben establecer un mecanismo de comunicación gerencial que permita al Directorio, Comité de Riesgos, Alta Gerencia y demás involucrados con nivel de decisión,

tener conocimiento periódico sobre el desarrollo de la gestión de riesgo operativo y generar alertas que permitan una toma de decisiones efectiva.

ARTÍCULO 19.- MANUAL DE GESTIÓN

Las instituciones deben contar con un manual de gestión de riesgo operativo, actualizado de forma permanente, que este de conformidad a sus estrategias y su proceso de gestión integral del riesgo. El referido manual debe tener en cuenta, como mínimo, los siguientes aspectos:

a) Políticas: Las instituciones deben diseñar las políticas de riesgo operativo, que deben incluir como mínimo:

i. Funciones y responsabilidades del Directorio, Alta Gerencia, Comité de Riesgos, Unidad de Riesgo y el resto de la institución;
ii. Las pautas generales que observará la institución en el manejo del riesgo operativo, describiendo la metodología aplicada para la gestión del mismo;
iii. La forma y periodicidad con la que se debe informar al Directorio y a la Alta Gerencia, entre otros, sobre la exposición al riesgo operativo de la institución y de cada línea de negocio;
iv. El nivel de riesgo aceptable por la institución, en función de impacto y probabilidad de ocurrencia;
v. El proceso que se debe cumplir para la aprobación de propuestas de nuevas operaciones, productos y servicios, introducción de nuevas tecnologías en sus procesos, entre otros aspectos;
vi. Indicadores de riesgo operativo que permitan monitorear la gestión del riesgo; y,
vii. Establecer procedimientos de captura de información de eventos de riesgo operativo para la base de datos, incluyendo controles de calidad que aseguren la calidad de la información registrada.

b) Metodología: Las instituciones supervisadas deben definir una metodología que incorpore todas las etapas de la gestión de riesgo operativo y debe cumplir como mínimo los siguientes requisitos:

i. Establecer procesos periódicos de autoevaluación de riesgos y controles por las áreas operativas de las instituciones supervisadas;
ii. Indicadores claves de riesgo, que indiquen alertas respecto a variaciones en la exposición de los riesgos, así como pérdidas a futuro; y,

iii. Procesos para la elaboración de escenarios que puedan identificar posibles riesgos y sus impactos;

Asimismo esta metodología debe:

i. Estar debidamente documentada y actualizada;
ii. Ser implementada en toda la institución;
iii. Fomentar el desarrollo de una cultura de gestión de riesgos, que permita una mejora continua de la gestión del riesgo operativo;
iv. Estar integrada en todo los procesos de gestión de riesgos de la institución; y,
v. Establecer procedimientos que aseguren su efectividad y cumplimiento.

ARTÍCULO 20.- MATRIZ DE RIESGO OPERATIVO

Las instituciones deben contar con una matriz de riesgo operativo, basada en los procesos de sus líneas de negocio, que considere entre otros aspectos: a) la identificación de los riesgos inherentes y factores de riesgo de cada línea de negocio; b) la medición de la efectividad de los controles internos; c) la determinación de los riesgos residuales, y se compare con el apetito y tolerancia al riesgo definido por la institución, para establecer actividades adicionales de mitigación de riesgos.

CAPÍTULO IV
DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO Y DE LA SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO 21.- GESTIÓN DE LA CONTINUIDAD DE NEGOCIO

La gestión de la continuidad del negocio requiere que el Directorio y todo el personal de la institución, implemente un proceso que brinde respuestas efectivas para que la operatividad del negocio continúe de una manera razonable, salvaguardando los intereses de sus principales grupos de interés, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en las operaciones de la institución. Esta gestión debe ser adecuada al tamaño y complejidad de las operaciones y servicios de la institución.

ARTÍCULO 22.- ETAPAS DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Para la gestión de la continuidad del negocio, las instituciones deben considerar al menos las siguientes etapas:

a) Análisis y Evaluación de la Continuidad del Negocio

Las instituciones deben identificar los riesgos que podrían causar una interrupción del negocio. Una vez identificados, se debe determinar el impacto que tendría una interrupción de los procesos que soportan los principales productos y servicios. Para ello, deben considerarse aspectos como: daños a la viabilidad financiera, daños a su reputación, incumplimiento de requerimientos regulatorios, daños al personal o al público en general. Según ello, deben establecer el período máximo tolerable de interrupción (RPO) y el tiempo objetivo de recuperación (RTO) por cada uno de estos procesos. Adicionalmente, deben definir qué procesos requieren contar con una estrategia de continuidad de negocios, considerando los resultados del análisis de impacto y de la evaluación de riesgos.

b) Definición de la Estrategia de Continuidad del Negocio

Las instituciones deben determinar la estrategia de continuidad que les permitirán mantener sus actividades y procesos de negocio, luego de ocurrido un evento de interrupción de operaciones, dentro del tiempo objetivo de recuperación definido para cada proceso. La estrategia de continuidad, dependiendo del tipo de proceso que se trate, debe considerar al menos lo siguiente: seguridad del personal, habilidades y conocimientos asociados al proceso, instalaciones alternas de trabajo, infraestructura alterna de tecnología de información que soporte el proceso, seguridad de la información y equipamiento necesario para el proceso, entre otros.

c) Desarrollo e implementación de la estrategia de continuidad

Las instituciones deberán desarrollar planes de respuesta ante los eventos analizados anteriormente, e implementar un modelo de respuesta adecuado que permita cubrir los eventos inesperados y proveer los recursos necesarios, acorde con la estrategia seleccionada, para enfrentar con éxito un evento de interrupción de operaciones. Para este fin, deben implementar un Plan de Continuidad de Negocio, el cual consiste en establecer un plan documentado que permita dotar a la institución de la capacidad de mantener, o de ser el caso recuperar, los principales procesos de negocio dentro de los parámetros previamente establecidos. Dicho Plan, debe incluir al menos lo siguiente:

a) Propósito y alcance;
b) Roles y responsabilidades;
c) Criterios de activación;
d) Planes de gestión de crisis;
    i. Roles y responsabilidades;

ii. Criterios de activación;
iii. Planes de acción;
iv. Plan de comunicación interno con medios de comunicación y grupos de interés; y,
v. Establecimiento de un centro de operaciones principal y alterno.

e) Planes de acción para reanudar los procesos conforme a la estrategia seleccionada;
f) Requerimiento de recursos;
g) Información básica y mecanismos de acceso a ella, incluyendo información de clientes, contratos, escrituras, garantías, pólizas de seguro, entre otros; y,
h) Responsable de mantener actualizado el plan.

El Plan de Continuidad de Negocio debe considerar mecanismos que tengan como objetivo salvaguardar la integridad física del personal y la recuperación de los servicios de tecnología de información. Adicionalmente, las pruebas deben realizarse con una periodicidad de al menos un (1) año o cuando existan cambios significativos en la institución o en el ambiente en que opera, y estar basadas en escenarios adecuados y planificados; cada prueba deberá tener un reporte que contenga los resultados alcanzados, recomendaciones y acciones para implementar las mejoras de forma oportuna.

ARTÍCULO 23.- GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La gestión de la seguridad de la información es un proceso, aprobado por el Directorio que busca asegurar razonablemente la integridad, confidencialidad y disponibilidad de la información que posee la institución. Para ello, debe diseñar, implementar, documentar, monitorear y actualizar un Plan de Gestión de la Seguridad de la Información, conforme a lo establecido en las normas que para tales efectos emita la Comisión, el cual debe considerar al menos los siguientes aspectos:

a) Definición de una política de seguridad de información aprobada por el Directorio;
b) Definición e implementación de una metodología de gestión de seguridad de información, que guarde consistencia con la gestión de continuidad del negocio y de riesgos operativos de la institución; y,
c) Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la institución.

CAPÍTULO V
SUBCONTRATACIÓN Y TERCERIZACIÓN

ARTÍCULO 24.- SUBCONTRATACIÓN Y TERCERIZACIÓN

Es importante que las instituciones gestionen el riesgo operativo relativo a los servicios tercerizados y subcontratados con otras personas naturales o jurídicas. Para ello, deben establecer políticas y procedimientos apropiados que permitan la gestión del riesgo operativo a través de terceros, considerando al menos los siguientes aspectos:

a) El proceso de selección del proveedor del servicio;
b) La elaboración del acuerdo de tercerización o subcontratación;
c) La gestión y monitoreo de los riesgos asociados con el acuerdo de tercerización o subcontratación;
d) La implementación de un entorno de control interno efectivo; y,
e) Establecimiento de planes de continuidad, en los casos que aplique.

Los acuerdos de tercerización o subcontratación deberán formalizarse mediante contratos escritos, los cuales deben incluir acuerdos de niveles de servicio, cuando aplique, y definir claramente las responsabilidades del proveedor y de la institución.

Para el caso de la gestión del riesgo tecnológico, adicionalmente debe considerarse lo señalado en el marco normativo que en dicha materia emita la Comisión.

Asimismo, las instituciones que formen parte de un grupo financiero o sean consideradas partes relacionadas, deberán cumplir con lo dispuesto por la Comisión en materia de contratación de bienes y servicios bajo condiciones competitivas de mercado.

ARTICULO 25. RESPONSABILIDAD

Las instituciones son responsables ante la Comisión de las funciones o procesos que puedan ser objeto de una tercerización y deben verificar que se mantengan las disposiciones contempladas en la presente Norma.

ARTICULO 26. DEBIDA DILIGENCIA SOBRE EL PROVEEDOR

Las instituciones deben ejecutar acciones de debida diligencia para seleccionar el proveedor de servicios, analizando al menos la viabilidad técnica, financiera y legal del

proveedor, de modo que alguno de estos aspectos no afecten la prestación del servicio en el futuro.

ARTICULO 27. TERCERIZACIÓN SIGNIFICATIVA

Para efectos de la presente Norma, se entenderá por tercerización significativa aquella que, en caso de falla o suspensión del servicio contratado, puede poner en riesgo importante a la institución, al afectar sus ingresos, solvencia o continuidad operativa. En toda tercerización significativa, un análisis formal de los riesgos asociados debe ser realizado y puesto en conocimiento del Directorio para su aprobación.

Los contratos suscritos con los proveedores de una tercerización significativa deben contener al menos lo siguiente:

a) Acuerdos de nivel de servicio (SLA), donde se manifiesten las expectativas de calidad del servicio esperado, tiempos de respuesta y penalizaciones, entre otros;
b) Procedimientos de monitoreo sobre el servicio contratado;
c) Disposiciones claras sobre el derecho a auditar por parte de la institución y la Comisión al proveedor, en los procesos relacionados a la prestación del servicio contratado, de acuerdo a lo estipulado en las leyes nacionales y regulación emitida por la Comisión. Este aspecto será aplicable sobre cualquier otra entidad que el proveedor subcontrate para brindar servicios a la institución;
d) Requerir que el proveedor cumpla con todos los requerimientos legales y regulatorios aplicables, incluyendo los promulgados después de la iniciación del contrato;
e) Responsabilidad del proveedor de contar con un Plan de Continuidad del Negocio, de modo que las interrupciones en la prestación del servicio contratado no afecten de manera significativa las operaciones de la institución;
f) Responsabilidad del proveedor de contar con un Marco de Gestión de Seguridad de la Información, de modo que se garantice la confidencialidad, integridad y disponibilidad de la información propiedad de la institución;
g) Acuerdos de confidencialidad;
h) Responsabilidad del proveedor para identificar todas las relaciones del subcontrato y requerir la aprobación de la institución supervisada para cambiar los subcontratistas;
i) Requerir la obligatoriedad de la prestación del servicio en regímenes especiales establecidos en la Ley del Sistema Financiero (vigilancia, intervención, resolución) determinados por la Comisión. El proveedor debe seguir brindando el servicio como

mínimo un año después de que la institución ha ingresado a un régimen especial de supervisión establecido por la Comisión.

CAPÍTULO VI
BASE DE DATOS

ARTÍCULO 28.- BASES DE DATOS

La gestión del riesgo operativo constituye un proceso continuo y permanente, para ello, será necesario que las instituciones conformen bases de datos que cumplan con los criterios que se abordan en el presente Artículo, debiendo registrarse los eventos de riesgo operativo que se hayan originado.

Las políticas y metodología establecida por la institución deben establecer los procedimientos de captura de información, así como el entrenamiento adecuado al personal que interviene en el proceso.

Las áreas operativas de la institución deben identificar y comunicar a la Unidad de Riesgos, todos aquellos eventos de riesgo operativo que ocurran, debiendo registrarse, como mínimo, la siguiente información referida al evento y a las pérdidas asociadas, en caso que las hubieren:

a) Código de identificación del evento (asignado por la institución), que permita diferenciar si es una incidencia o un evento que se ha materializado luego de haber sido identificado;
b) Tipo de evento de riesgo operativo, según los señalados en el Anexo 1 de la presente Norma;
c) Línea de negocio asociada, según Anexo 2 de la presente Norma;
d) Título del evento;
e) Descripción del evento;
f) Proceso, área y producto al cual pertenece el evento;
g) Fecha de ocurrencia o de inicio del evento (si aplica);
h) Fecha de descubrimiento del evento (si aplica);
i) Fecha de registro contable del evento (si aplica);
j) Monto bruto de la pérdida estimada por evento;

k) Monto estimado de costo de oportunidad dejado de percibir, derivado del evento de riesgo operativo, cuando no se pueda medir con precisión la pérdida;
l) Monto estimado de recuperación por evento;
m) Monto total recuperado;
n) Cuentas contables asociadas (si aplica); de conformidad al catálogo contable aprobado por la CNBS; y,
o) Identificación si el evento está asociado con algún otro riesgo específico, según el tipo de institución, de conformidad al Anexo No. 4 de la presente Norma.

En el caso de eventos con pérdidas múltiples, las instituciones pueden registrar la información mínima requerida por cada pérdida, y establecer una forma de agrupar dicha información por el evento que la originó.

Por otro lado, las instituciones podrán registrar información parcial de un evento, en tanto se obtengan los demás datos requeridos. Por ejemplo, podrá registrarse primero el monto de la pérdida, para posteriormente añadir las recuperaciones asociadas.

ARTÍCULO 29.- RESPALDO PATRIMONIAL POR PÉRDIDAS POTENCIALES

Dada la importancia que la gestión del riesgo operativo tiene en las instituciones por las pérdidas potenciales que se producen, los estándares internacionales establecen respaldos por las pérdidas potenciales que se enfrentan por este riesgo, a través de cargas de capital. Cabe destacar que una adecuada gestión del riesgo operativo permite minimizar las pérdidas potenciales por este riesgo, por lo que reduce las cargas de capital antes mencionado. La Comisión establecerá posteriormente requerimientos de capital en base a los estándares internacionales y de acuerdo a la realidad de las instituciones.

CAPÍTULO VII
DISPOSICIONES FINALES

ARTÍCULO 30.- REQUERIMIENTOS DE INFORMACIÓN

Las instituciones deberán remitir a la Comisión, un informe semestral que contenga los principales aspectos y resultados de la gestión de riesgo operativo, a más tardar el 31 de enero y 31 de julio de cada año. Dicho informe deberá contener al menos la siguiente información: a) Nivel de exposición al riesgo operativo (Inherente y residual) por cada línea

de negocio; b) estrategias adoptadas de mitigación de riesgos; c) Desviaciones a los límites previamente establecidos y acciones correctivas implementadas; d) Análisis de frecuencia y severidad de los eventos de riesgo operativo ocurridos por línea de negocio; e) Resultados del monitoreo de indicadores clave de riesgo operativo; y, f) Resultados de las pruebas del plan de continuidad de negocio, entre otros.

Todas las Instituciones deberán remitir las modificaciones o actualizaciones al Manual y Metodología de Gestión de Riesgo Operativo, cada vez que realicen cambios a los mismos, debiendo acompañar el punto de acta de aprobación por parte del Directorio. Asimismo, deberán remitir de forma trimestral, por el medio que determine la Comisión, los eventos de riesgo operativo registrados en su base de datos, de conformidad lo señalado en el Anexo No. 3 de la presente Norma.

ARTÍCULO 31.- REQUERIMIENTOS ADICIONALES

La Comisión podrá requerir a las instituciones, cualquier otra información que considere necesaria, para una adecuada supervisión del riesgo operativo.

Asimismo, las instituciones deberán tener a disposición de esta Comisión toda la información, políticas, procesos, procedimientos, sistemas de gestión, estrategias, planes y otros a que hace mención la presente Norma, así como las revisiones de auditoría interna y externa o de la casa matriz, en caso de aquellas instituciones cuya matriz no se encuentre en el país.

ARTÍCULO 32.- SANCIONES

En caso de incumplimiento de las disposiciones contenidas en la presente Norma, la Comisión aplicará las sanciones correspondientes, de conformidad con lo establecido en el marco legal aplicable y en el Reglamento de Sanciones vigente.

ARTÍCULO 33.- CASOS NO PREVISTOS

Lo no previsto en la presente Norma, será resuelto por la Comisión de conformidad al marco legal y normativo vigente.

ARTÍCULO 34.- PLAZO DE ADECUACIÓN

Para efectos de adecuación a las disposiciones contenidas en la presente Norma, las instituciones deberán sujetarse a los siguientes plazos:

Programa	Plazo	Observaciones
Instituciones del Sistema Financiero, BANHPROVI, RAP PENSIONES		
1. Plan de acción para adecuarse a las modificaciones de la presente Norma, con su respectiva aprobación por el Directorio	Treinta (30) días hábiles contados a partir de la entrada en vigencia de la Norma.	Se deberá acompañar un plan de acción con plazo límite máximo de seis (6) meses a partir de la entrada en vigencia de la Norma, para adecuar su proceso de gestión de riesgo operativo a las modificaciones de la misma. El proceso de adecuación de esta norma, no exime de responsabilidad al Directorio en velar porque se gestionen los riesgos a que se expone la institución. Este plan de acción deberá incluir al menos: Fechas de inicio y finalización de las actividades, responsables de ejecución, descripción de las actividades a realizar, entre otros.
2. Informe semestral sobre la gestión de riesgo operativo	31 de enero y 31 de julio.	El primer envío será con cifras al cierre del segundo semestre del año 2019.
3. Base de datos trimestral con eventos de pérdida	Diez (10) días hábiles después del cierre de cada trimestre.	El primer envío será a partir del cierre del tercer trimestre del año 2019.
4. Cumplimiento Artículo 10 – Unidad de Auditoria Interna	De inmediato.	
Demás Instituciones Supervisadas		
1. Plan de acción para adecuarse a los lineamientos de la presente Norma, con su respectiva aprobación por el Directorio.	Treinta (30) días hábiles contados a partir de la entrada en vigencia de la Norma.	Se deberá acompañar un plan de acción con plazo límite máximo de veinte y cuatro (24) meses a partir de la entrada en vigencia de la Norma para dar cumplimiento total a la misma. El proceso de implementación de esta norma, no exime de responsabilidad al Directorio en velar porque se gestionen los riesgos a que se expone la institución. Este plan de acción deberá incluir al menos: Fechas de inicio y finalización de las actividades, responsables de ejecución, descripción de las actividades a realizar, entre otros.

Programa	Plazo	Observaciones
2. Informe trimestral sobre los avances en la implementación de la Norma de Gestión de Riesgo Operativo.	Diez (10) días hábiles después del cierre del trimestre.	Según Anexo No. 5, a partir del cierre del tercer trimestre del año 2019.
3. Manual y Metodología de Gestión de Riesgo Operativo	Seis (6) meses contados a partir de la entrada en vigencia de la Norma.	Según fechas establecidas en Artículo 30.
4. Informe semestral sobre la gestión de riesgo operativo	31 de enero y 31 de julio.	El primer envío será a partir del cierre del primer semestre del año 2020.
5. Reporte trimestral de base de datos de eventos de pérdida	Diez (10) días hábiles después del cierre de cada trimestre.	El primer envío será a partir del cierre del tercer trimestre del año 2020.
6. Cumplimiento Artículo 10 – Unidad de Auditoria Interna	De inmediato.	

ARTÍCULO 35.- DEROGATORIA

A partir de la entrada en vigencia de la presente Norma, queda sin valor y efecto la Resolución SB No.1321/02-08-2011, contentiva de la "Norma de Gestión de Riesgo Operativo", así como cualquier otra disposición emitida sobre la materia que se oponga a la presente Norma.