COMISIÓN PARA EL MERCADO FINANCIERO

Regulador y Supervisor Financiero de Chile

Informe Normativo

Gestión de Riesgo Operacional de Sociedades Administradoras de Sistemas de Compensación y Liquidación, Empresas de Depósito y Custodia de Valores, Bolsas de Valores, Bolsas de Productos y Administradoras Generales de Fondos.

Mayo 2024

www.CMFChile.cl

Contenido

I. INTRODUCCIÓN Y OBJETIVO DE LA PROPUESTA

El presente proyecto normativo establece los requisitos para una adecuada gestión del riesgo operacional de Administradoras Generales de Fondos (AGF), Bolsas de Valores, Bolsas de Productos, Sociedades de Compensación y Liquidación de Instrumentos Financieros y Entidades de Depósito y Custodia de Valores.

Asimismo, las entidades mencionadas deberán reportar a esta Comisión los incidentes y pérdidas operacionales oportunamente, de manera que ésta tome conocimiento y lleve a cabo las acciones pertinentes, en el uso de sus facultades, con el objetivo de que los participantes del sistema financiero local tengan una mayor capacidad de respuesta y tomen los resguardos necesarios en forma oportuna.

II. DIAGNÓSTICO Y MARCO NORMATIVO LOCAL

El proyecto normativo viene a aplicar y dar cumplimiento a un marco para la gestión de riesgo operacional que incorpore a entidades que no cuentan con uno específicamente, y por otra parte a complementar las disposiciones sobre gestión de riesgo operacional ya existentes en otras entidades.

En particular, el presente proyecto normativo busca resolver las siguientes brechas identificadas como parte del diagnóstico:

a) Establecer un marco de gestión de riesgo operacional para Bolsas de Valores, Bolsas de Productos, Sociedades de Compensación y Liquidación de Instrumentos Financieros, y Entidades de Depósito y Custodia de Valores, subsanando de esta forma la asimetría regulatoria con otras entidades que ya contaban con dicho marco (Intermediarios de Valores y AGF).
b) Actualizar las disposiciones existentes sobre la gestión de riesgo operacional de AGF.
c) Adecuar la regulación de gestión de riesgo operacional local a las mejores prácticas internacionales.
d) Adecuar la regulación de gestión de riesgo operacional local al marco dado por la reciente Ley N° 21.521 (Ley Fintec). Esta última requiere que las entidades del mercado de valores tengan la capacidad operacional para soportar el procesamiento de las transacciones que se realice mediante los sistemas o infraestructura de las entidades.

Finalmente, se establece un marco normativo que permite la supervisión de aspectos de riesgo operacional tales como seguridad de la información, continuidad operacional y externalización de servicios.

A continuación, se describe el marco normativo local existente actualmente para la gestión de riesgo operacional, para las siguientes entidades: Depósito y Custodia de Valores, Sociedades Administradoras de Sistemas de Compensación y Liquidación de Instrumentos Financieros, Compañías de Seguros y Bancos.

a) Entidades de Depósito y Custodia de Valores

Circular N° 1.939

Establece los requisitos de gestión de riesgo operacional de las Entidades de Depósito y Custodia de Valores y las Sociedades Administradoras de Sistemas de Compensación y Liquidación de Instrumentos Financieros. Los principales requisitos son los siguientes:

a) Política de Gestión de Riesgo Operacional, con definición de roles y responsabilidades y criterios para la evaluación y tratamiento de riesgos, lo que debe estar documentado en un Manual de Gestión de Riesgo Operacional.
b) Unidad responsable de la Gestión de Riesgo Operacional, responsable de la gestión y monitoreo de los riesgos operacionales y adopción de medidas de mitigación, lo que debe estar documentado en una Matriz de Riesgos.
c) Unidad responsable de evaluar el cumplimiento de las políticas de gestión de riesgo operacional, con reporte anual al Directorio.
d) La Gerencia General es responsable de aprobar, implementar y controlar el proceso de gestión de riesgo operacional, con reporte anual al Directorio.

Circular N° 2.020

Establece las instrucciones que deben cumplir las Entidades de Depósito y Custodia de Valores y las Sociedades Administradoras de Sistemas de Compensación y Liquidación sobre la comunicación y resolución de incidentes operacionales.

Se debe informar a la CMF lo antes posible y por correo electrónico todo incidente crítico, entendiéndose por tal aquel evento que provoque la falta de disponibilidad de un servicio por al menos 15 minutos, reduzca el rendimiento de un servicio por debajo del nivel establecido por la entidad, o provoque la solicitud de una Extensión Horaria al Banco Central.

Adicionalmente, todo incidente que no haya sido resuelto luego de transcurridos 30 minutos desde su ocurrencia debe comunicarse al menos a sus usuarios, a la entidad no afectada y al Banco Central, indicando el tiempo previsto para resolverlo, las recomendaciones para los usuarios y, llegado el caso, el tiempo de extensión horaria otorgado por el Banco Central. Transcurridos 20 días hábiles, debe remitirse a la CMF un informe que documente la descripción del incidente y la descripción de los procedimientos implementados para resolverlo.

b) Sociedades Administradoras de Sistemas de Compensación y Liquidación

Circular N° 2.020

Ídem anterior.

c) Compañías de Seguros

Norma de Carácter General N° 454

Establece que las compañías aseguradoras cuenten con un Marco de Gestión de Riesgo operacional, el que debe ser parte del sistema de gestión de riesgos de la compañía y estar debidamente documentado. El marco debe incluir una declaración de apetito de riesgo operacional con un enfoque basado en tres líneas de defensa: actividades del negocio, supervisión y monitoreo de riesgos, y auditoría interna. Dentro de este marco debe incluirse una estrategia de gestión de ciberseguridad y contar con un profesional responsable de la implementación de dicha estrategia.

La norma requiere la adopción de las siguientes prácticas internacionales en materia de ciberseguridad:

a) Identificar riesgos cibernéticos dentro de las funciones y procesos organizacionales. Las aseguradoras deberán mantener un inventario de activos de información. Los activos deberán ser clasificados en términos de su criticidad, considerando su confidencialidad, integridad y disponibilidad. Dentro de este mapeo se deben considerar derechos de acceso individual, dependencias y proveedores externos, así como procesos de inversión, adquisiciones y cambios.
b) Identificar las áreas operativas de la aseguradora expuestas a riesgo cibernético. Este proceso se puede organizar por medio de las siguientes categorías descritas en la norma: (1) tecnologías y tipos de conexión, (2) canales de entrega, (3) características organizacionales y (4) amenazas externas.
c) Implementar tecnologías y procesos de respaldo y almacenamiento de datos acorde con su criticidad.
d) La aseguradora deberá verificar que sus proveedores externos protejan los datos de los servicios prestados en el mismo grado que se esperaría de la aseguradora.
e) Identificar proactivamente los riesgos cibernéticos de su entorno, actualizando sus política y procesos dinámicamente.

En materia de comunicación de incidentes operacionales, estos deberán ser reportados a la Comisión por medio del módulo SEIL, tanto al inicio como al cierre de este. La compañía deberá informar a los clientes y usuarios de la aseguradora, actualizando la información hasta que el incidente sea superado. Adicionalmente, la aseguradora deberá compartir información relevante con las entidades de la industria con la finalidad de resguardar a los clientes y al sistema en su conjunto.

d) Bancos

RAN Capítulo 1-13

Establece disposiciones generales relativas a la evaluación de la Administración de Riesgo Operacional realizada por los bancos. Recomienda que el banco identifique claramente los principales activos de información e infraestructura física y defina políticas explícitas para el manejo del riesgo operacional que consideren el volumen y complejidad de sus actividades, el nivel de tolerancia al riesgo del Directorio y las líneas específicas de responsabilidad.

Asimismo, el capítulo recomienda contar con una función encargada de la evaluación y gestión de riesgo operacional en base a una metodología de evaluación de probabilidad e impacto, y una función de Auditoría Interna que evalúe el desempeño de la primera para que se adopten medidas correctivas de manera oportuna.

RAN Capítulo 20-7

Contiene pautas de carácter general relativas a servicios externalizados y, en forma particular, a la tercerización de servicios de procesamiento de datos y resguardos adicionales en el caso de servicios en la nube. La norma señala las condiciones que debe cumplir una entidad ante la decisión de externalizar un servicio, contempla requisitos esenciales respecto a los sitios de procesamiento; los aspectos de continuidad del negocio, seguridad de la información propia y de sus clientes; entre otros. En cuanto a este último aspecto, la entidad bancaria debe exigir al proveedor asegurar la confidencialidad, integridad, trazabilidad y disponibilidad de sus activos de información y la de sus clientes.

RAN Capítulo 20-8

Establece lineamientos para la información que las entidades supervisadas a las que la misma aplica, deben remitir ante la ocurrencia de incidentes operacionales relevantes que afecten la continuidad del negocio, la seguridad de la información o la imagen de la institución y, además, señala las condiciones mínimas que se deben considerar para el desarrollo y mantención de bases de información respecto de incidentes de ciberseguridad. El 31 de agosto de 2018 se introdujeron cambios que perfeccionan el sistema de reporte de incidentes, creando una plataforma digital especialmente establecida por la CMF para reportar los incidentes al regulador en un plazo máximo de 30 minutos. Adicionalmente, se definió la obligación de designar un encargado de nivel ejecutivo para comunicarse con la CMF en todo momento.

RAN Capítulo 20-9

Contempla una serie de lineamientos para la adecuada gestión de los riesgos de continuidad del negocio, teniendo en cuenta el volumen y la complejidad de las operaciones de las entidades supervisadas a las que la misma aplica. De esta manera, indica la debida existencia de una estrategia aprobada por la máxima instancia de la entidad, de una función de riesgos que se encargue de este ámbito en conjunto con instancias colegiadas de alto nivel, de una estructura para el manejo de situaciones de crisis, de la evaluación de escenarios mínimos de contingencia, entre otros. Dentro de los escenarios de contingencia para los cuales se deben definir y probar planes se encuentran los "ataques maliciosos que afecten la ciberseguridad". Incluye la operatoria de los sitios de procesamiento de datos como parte de los aspectos relevantes que contribuyen a fortalecer la resiliencia operacional de las entidades.

RAN Capítulo 20-10

Contiene una serie de disposiciones, basadas en las mejores prácticas internacionales, que deben ser consideradas para la gestión de la seguridad de la información y ciberseguridad. Entre otros, se definen lineamientos específicos respecto del rol que debe tener el Directorio para la adecuada gestión, tanto de seguridad de la información como de ciberseguridad, otorgándole como responsabilidad la aprobación de la estrategia institucional en esta materia, junto a la responsabilidad de asegurar que las entidades mantengan un sistema de gestión de la seguridad de la información y ciberseguridad. Asimismo, se establece la necesidad de que las entidades definan sus activos críticos, así como las funciones de protección de éstos, la detección de las amenazas y vulnerabilidades, la respuesta ante incidentes y la recuperación de la operación normal de la entidad; además de disponer de políticas y procedimientos para la identificación de aquellos activos que componen la infraestructura crítica de la industria financiera y del sistema de pagos, y para el adecuado intercambio de información técnica de incidentes que afecten o pudieran afectar la ciberseguridad de la entidad.

e) Prestadores de Servicios Financieros (Ley N° 21.512)

Norma de Carácter General N°502

Esta normativa regula el registro y autorización para la prestación de servicios Fintec; los requisitos en materia de gestión de riesgos y gobierno corporativo, capital y garantías y las obligaciones de divulgación y entrega de información a los clientes y al público en general.

Contenido de la propuesta

La propuesta normativa establece un marco de gestión de riesgo operacional para Bolsas de Valores, Bolsas de Productos, Administradoras de Fondos, Sociedades Administradoras de Sistemas de Compensación y Liquidación y Entidades de Depósito y Custodia de Valores, de manera que dichas entidades estén preparadas para gestionar el riesgo operacional en los siguientes ámbitos:

- **Seguridad de la Información y Ciberseguridad:** Gestión de eventos que afecten las infraestructuras y sistemas informáticos de la entidad (instalaciones físicas, activos de información, hardware, software).
- **Continuidad del negocio:** Gestión de eventos relacionados con interrupciones o fallas en las operaciones del negocio, incluyendo su comunicación oportuna a los reguladores y al mercado.
- **Subcontratación de proveedores de servicios:** Gestión de eventos operacionales de un proveedor de servicios que afecten la seguridad de la información y ciberseguridad y/o la continuidad del negocio de la entidad.

III. PRÁCTICAS INTERNACIONALES

La propuesta normativa considera la revisión de estudios y principios internacionales para la gestión de riesgo operacional elaborados por el *Comité de Basilea sobre Supervisión Bancaria* (BCBS, por sus siglas en inglés), la *Autoridad Europea de Bancos* (EBA), la *Organización Internacional de Reguladores de Valores* (IOSCO), el *Grupo de los Siete* (G7), el *Banco de Pagos Internacionales* (BIS) y la *Asociación Internacional de Supervisores de Seguros* (IAIS).

Asimismo, se revisan las disposiciones regulatorias de similar naturaleza presentes en las legislaciones de Australia, Colombia, Estados Unidos, México, Perú y Singapur.

Una descripción más detallada tanto de los estudios internacionales como de las legislaciones de países puede encontrarse en los Anexos A y B de este Informe.

A continuación, se describen los estudios internacionales y legislaciones de países agrupados según los tres ámbitos de gestión de riesgo operacional descritos: Seguridad de la Información y Ciberseguridad, Continuidad del Negocio y Externalización de Servicios.

Seguridad de la Información y Ciberseguridad

El aumento de incidentes operacionales relacionado con las Tecnologías de Información y Comunicación (TIC) y ciberseguridad podrían gatillar eventos de riesgo sistémico en el mercado financiero. En respuesta a ello, la EBA (*European Banking Authority*) establece recomendaciones para el desarrollo un **Marco de Gestión de Riesgos de TIC** (EBA, 2019). Se propone que la Alta Administración esté a cargo de desarrollar y documentar una **Política de Seguridad de la Información**. Dicha política debería identificar y clasificar las funciones comerciales, los activos de información y los procesos de soporte en base a consideraciones de confidencialidad, integridad y disponibilidad de los datos y el monitoreo continuo de posibles vulnerabilidades, estableciendo las funciones y responsabilidades del personal a cargo y los proveedores externos, junto con planes de capacitación.

También se recomienda que la **gestión del riesgo** sea asignada a un área separada de los procesos operativos de TIC, por ejemplo, una función de control independiente que responda directamente a la Alta Administración y no realice labores de auditoría. Dentro de sus prácticas incluye procedimientos de **registro y monitoreo** de operaciones críticas para la detección de actividades anómalas que puedan afectar la seguridad de la información; el **respaldo y restauración** de datos y sistemas de TIC; el desarrollo de un **Plan de Continuidad del Negocio** aprobado por la Alta Administración, que incluya un conjunto de escenarios severos pero plausibles sobre cambios en funciones comerciales críticas, procesos de soporte y activos de información.

Otro aspecto relevante es la implementación de **medidas de seguridad** debidamente documentadas que abarquen los ámbitos de la seguridad física y lógica, mediante revisiones de seguridad, evaluaciones y pruebas periódicas que aseguren la identificación eficaz de vulnerabilidades en los sistemas TIC.

Dentro de las buenas prácticas se incluye mantener un **registro** actualizado de procesos, funciones y activos TIC, clasificados de acuerdo a su nivel de criticidad, como también procesos de soporte y otros servicios brindados por proveedores externos.

Como parte de la gestión de continuidad del negocio las entidades deberían realizar un **Análisis de impacto de negocio** (BIA). El BIA debe considerar la criticidad de las funciones comerciales, los procesos de soporte, los activos de información y sus interdependencias. En base a ello, las entidades deben desarrollar planes de **respuesta y recuperación** de las funciones críticas para el negocio.

Se recomienda participar en el **intercambio oportuno de información** de seguridad cibernética con partes interesadas (autoridades, otras entidades, clientes) sobre amenazas, vulnerabilidades, incidentes y planes de respuesta que limiten el impacto potencial de futuros incidentes y promuevan el **aprendizaje continuo**, revisando el marco de seguridad cibernética regularmente y cuando los eventos lo justifiquen (G7, 2016).

Con respecto a las legislaciones de países, se destaca lo siguiente:

- En Australia se debe notificar al regulador los incidentes de ciberseguridad que detecten. Adicionalmente, en el caso de los Intermediarios de Valores, deben notificar toda conducta que a su juicio les parezca sospechosa en relación a la integridad de las operaciones del mercado.
- En Colombia, las entidades deben mantener un Registro de Eventos de Riesgo Operacional, clasificándolo en dos tipos: Ciberseguridad y Otros. Asimismo, deben realizar una autoevaluación de la eficacia de los controles de Ciberseguridad.
- En EE.UU., se requiere a Intermediarios y Bolsas de Valores realizar auditorías periódicas de sus sistemas y notificar al regulador los incidentes de ciberseguridad detectados, pero no se exige llevar una Base de Registro de Incidentes.
- En México, se requieren políticas y procedimientos de seguridad de TI y de gestión de incidentes operacionales. Asimismo, se requiere mantener una Base de Datos de Eventos por Pérdida de Riesgo Operacional y un cálculo del Capital por Riesgo Operacional.
- En Perú, cada entidad debe contar con una Función de Gestión de Seguridad de la Información y Ciberseguridad encargada del Sistema de Gestión de la Seguridad de la Información. En caso de ocurrencia de eventos de interrupción significativa de operaciones, esta deberá ser comunicada a la SMV al día siguiente hábil. Asimismo,

cada entidad debe mantener una Base de Eventos de Pérdida por Riesgo Operacional y registrar incidentes que signifiquen una pérdida superior a tres mil soles (o inferior, lo que será determinado por el regulador).
- En Singapur, el regulador debe ser notificado a más tardar en una hora sobre el descubrimiento de un incidente importante. Dentro de los 14 días siguientes, la entidad debe presentar un Informe con su impacto y las medidas correctivas adoptadas.

Continuidad del Negocio

El documento *Revisions to the Principles for the Sound Management of Operational Risk* (BCBS, 2021) define el **riesgo operacional** como aquel derivado de fallas en procesos, personas, sistemas o eventos externos[1]. La **gestión del riesgo operacional** busca identificar las causas subyacentes de cada riesgo, medir las exposiciones de la entidad a los mismos y mitigar prontamente las exposiciones dentro de los niveles de tolerancia definidos.

High-level principles for business continuity (BIS, 2006) destaca la importancia de la **gestión de la continuidad operativa**, entendida como el conjunto de políticas, estándares y procedimientos que aseguren la capacidad de mantener las operaciones o su pronta recuperación en el caso de interrupción, de manera tal que se minimicen sus consecuencias en los ámbitos operacionales, financieros, legales y reputacionales de la entidad.

Principles for Operational Resilience (BCBS, 2021) define la **resiliencia operacional** como la capacidad de la entidad de continuar sus operaciones producto de una adecuada gestión de incidentes de riesgo operacional. En el caso de la industria bancaria, el documento advierte de un mayor riesgo operacional derivado de la rápida adopción de infraestructura tecnológica y tercerización de servicios. El incremento en los niveles de capital y liquidez de los bancos no sería suficiente para sobrellevar fallas operativas de gran escala derivadas de pandemias, ciberataques y desastres naturales.

Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business Continuity (IOSCO, 2015) plantea que el acelerado desarrollo tecnológico en las plataformas de negociación podría desencadenar eventos sistémicos de mercado producto de fallas en los **sistemas críticos** [2] de Intermediarios y Bolsas de Valores. En la misma línea, *Revised Consultation on Guidelines on the management of operational risk in market-related activities* (EBA, 2010) recomienda diseñar sistemas de alertas para advertir a la gerencia cuando se detecten operaciones sospechosas o incidentes materiales en el mercado. Para las relaciones entre los *traders* y sus contrapartes del mercado, son considerados mecanismos adecuados de control los procesos de confirmación, liquidación y conciliación de transacciones.

Market Intermediary Business Continuity and Recovery Planning (IOSCO, 2015) recomienda a las entidades financieras incorporar el riesgo de una **interrupción operativa importante** en sus enfoques para la gestión de la **continuidad del negocio**, así como definir **objetivos de recuperación** que reflejen el riesgo que representan para la operación del sistema financiero. Según corresponda, dichos objetivos pueden ser establecidos en consulta con las

[1] Incluyendo el riesgo legal, pero excluyendo los riesgos estratégicos y reputacional.
[2] Ejemplos de sistemas críticos de Bolsas de Valores corresponden a Sistemas de entrada y ejecución de órdenes, Sistemas de enrutamiento de pedidos, Sistemas de difusión de datos históricos y en tiempo real, Sistemas de infraestructura de red, gestión de bases de datos, almacenamiento, cortafuegos y conexiones de red, Sistemas de vigilancia, Sistemas de Gestión de Riesgos para monitoreo de límites y márgenes.

autoridades financieras pertinentes. Junto con lo anterior, *High-level principles for business continuity* (BCBS-IOSCO-IAIS, 2006) recomienda que los planes de respuesta y recuperación estén en línea con el apetito de riesgo e incorporen las lecciones aprendidas.

Con respecto a los estándares de continuidad, gestión y resiliencia operacional del sistema financiero, cabe destacar los siguientes principios emanados de BCBS, IOSCO y EBA:

- La responsabilidad de la gestión del riesgo operacional recae en el Directorio y la Alta Administración.
- El Directorio debe aprobar y revisar periódicamente el marco de gestión del riesgo operacional y de continuidad operativa, y asegurar que la Alta Administración implemente el marco de gestión en todos los niveles de decisión.
- El Directorio debe aprobar y revisar periódicamente una declaración de apetito y tolerancia al riesgo, en donde se definen los niveles y tipos de riesgo operacional que el banco decide gestionar, y los niveles esperados de fallas residuales en los procesos que se está dispuesto a asumir.
- La Alta Administración debe proponer al Directorio una estructura de gobierno clara, eficaz y sólida con recursos materiales y líneas de responsabilidad definidas, transparentes y coherentes. Es responsable de implementar el marco de gestión de riesgo operacional, dentro de los niveles de tolerancia definidos por el Directorio. Dicho marco debiera permitir el monitoreo regular de los riesgos operacionales con mecanismos de información adecuados a nivel del Directorio, la Alta Administración y las unidades de negocio que respalden la gestión proactiva del riesgo operacional.
- El marco de gestión debería ser implementado de modo proporcional a la naturaleza, el tamaño y la complejidad de los servicios ofrecidos por la entidad. Así, debe garantizar la identificación y evaluación integral del riesgo operacional inherente a todos los productos, actividades, procesos y sistemas para asegurarse de que todo el personal de la entidad comprenda los riesgos e incentivos inherentes.
- El marco de gestión debería estar articulado en tres líneas de defensa. La primera línea de defensa corresponde a la gestión de unidades de negocio, la segunda a la gestión de riesgo operacional y la tercera a la de auditoría interna.
- Los planes de continuidad de negocios tienen por finalidad evaluar y mitigar los riesgos asociados a una interrupción operativa importante del negocio producto de fallas en la infraestructura tecnológica, ataques cibernéticos y errores humanos. Deberían estar vinculados al marco de gestión del riesgo operacional, ser actualizados periódicamente y estar en conocimiento del Directorio. Incluyen la asignación de recursos adecuados para su actualización y prueba periódica; evaluaciones de impacto de eventuales interrupciones operativas en sistemas críticos; protocolos de comunicaciones y escalamiento de incidentes; mantenimiento de registros; redundancia de software y hardware; obligaciones de proveedores de servicios y pruebas y escenarios de estrés. Frente a incidentes mayores o con implicaciones transfronterizas, los planes de continuidad deberían incluir estrategias de comunicación con los clientes, otras entidades del sistema financiero y reguladores de distintos países.
- En el caso de Intermediarios y Bolsas de Valores, los planes de continuidad deberían garantizar que sus sistemas críticos se puedan mantener o recuperar de manera oportuna en caso de interrupción. Dichos sistemas deberían ser revisados en forma periódica por un auditor independiente que informe las deficiencias detectadas y las medidas adoptadas para resolverlas a la Alta Administración (y al regulador cuando corresponda). También deberían incluir medidas para monitorear políticas de monitoreo y restricción de operaciones frente a movimientos de precios anómalos, controles de entrada, seguimiento y cancelación de transacciones.

Los Intermediarios y Bolsas de Valores han demostrado su resiliencia operativa a lo largo de la **pandemia** en un contexto marcado por volúmenes récord de negociación y alta volatilidad del mercado. El documento *Operational resilience of trading venues and market intermediaries during the COVID-19 pandemic* (BCBS, 2022) resalta aspectos sobre la **resiliencia operativa** en pandemia tales como la acelerada transición al trabajo remoto, el consecuente aumento del trabajo híbrido en muchas jurisdicciones y una mayor dependencia en sistemas de Tecnologías de Información y Comunicación (TIC).

Con respecto a las legislaciones de países, se destaca lo siguiente:

- En Australia, EE.UU. Singapur y Perú, se deben contar con planes de continuidad de negocios y recuperación ante desastres incluido el respaldo de datos y la realización de pruebas de vulnerabilidad. Cada entidad debe identificar las funciones críticas de su negocio y contar con una función de gestión de riesgo operacional que asegure la continuidad del negocio.
- En EE.UU. se requiere a Intermediarios y Bolsas la reanudación de funciones críticas a las 2 horas de producida una interrupción. Asimismo, a las Contrapartes Centrales contar con una Unidad de Gestión de Riesgos y otra de Auditoría Interna independientes que respondan al Directorio. Por último, las entidades que operan con derivados deben presentar periódicamente una evaluación de riesgos que incluye la aprobación de límites de tolerancia al riesgo por el Directorio.
- En Colombia, el regulador define las actividades críticas del negocio y elabora una matriz de riesgos con sugerencias de mejora en los planes de continuidad del negocio. Lo anterior, sin perjuicio de que trimestralmente las entidades envían una evaluación integral de la gestión de riesgos, incluido el riesgo operacional.
- En México, las entidades deben llevar a cabo un Análisis de Impacto del Negocio (BIA, por sus siglas en ingles) y contar con un Plan de Continuidad de Negocio que incluya al menos una vez al año pruebas de seguridad de TI y ejercicios de crisis (no se requiere enviar los resultados de estas pruebas). Asimismo, deben contar con una Unidad de Administración Integral de Riesgos, un Área de Auditoría Interna independiente, un Comité de Riesgos y un Comité de Auditoría.
- En Perú, cada entidad debe contar con una Función de Continuidad del Negocio encargada del Sistema de Gestión de la Continuidad del Negocio. Asimismo, debe remitir trimestralmente al regulador un Reporte de Indicadores Clave de Gestión de Riesgo Operacional.
- En Singapur, cada entidad debe realizar un BIA y contar con una Base de Registro de Riesgos, que facilite la respuesta ante incidentes (incluyendo proveedores de servicios críticos).

Externalización de servicios

En los últimos años, ha habido una tendencia creciente por parte de las entidades financieras a **tercerizar servicios** para reducir costos y digitalizar sus procesos. A pesar de sus beneficios, la tercerización implica riesgos en los ámbitos de la seguridad de información y continuidad operacional. Como respuesta a ello, la EBA en su estudio *Guidelines on outsourcing arrangements* recomienda mejores prácticas y directrices para su adecuada gestión. Allí se define **externalización de servicios** [3] a los acuerdos comerciales por medio

[3] No se considera tercerización: (1) Funciones que por ley deben ser realizadas por un proveedor específico, como por ejemplo las auditorias. (2) Servicios de información de mercado como Bloomberg, Fitch. (3) Infraestructuras

de los cuales un proveedor realiza actividades que de otra forma serían llevadas a cabo por la entidad que lo contrata (EBA, 2019). En ningún caso, la externalización podría dar lugar a la delegación de responsabilidades, siendo la entidad contratante totalmente responsable de garantizar la prestación adecuada del servicio y cumpliendo con todas sus obligaciones regulatorias.

Dentro de las responsabilidades de la Alta Administración se incluye la elaboración de una **política de subcontratación**. Esta debe incluir las principales etapas del ciclo de vida del servicio subcontratado, los procesos asociados a cada etapa, los roles y responsabilidades del personal, las líneas de negocio involucrada y los controles pertinentes.

El marco de gestión de riesgos debería abordar **planes de continuidad de negocios** para los servicios subcontratados críticos para gestionar posibles fallas o caídas en calidad por debajo de estándares predefinidos. De este modo, se recomienda **previo a cualquier acuerdo de subcontratación**, que las entidades evalúen en primer lugar si el servicio corresponde a una **función crítica** [4], y si se cumplen las condiciones adecuadas para implementar los mecanismos de control y supervisión del proveedor externo. La gestión de la continuidad incluye **planes de salida** para transferir el servicio a otro proveedor en caso de deterioro, interrupción o falla del servicio.

Las entidades deben **monitorear** de forma continua el desempeño de los prestadores de servicios subcontratados. Fundamental en ello es levantar un **registro de subcontratación** de todos los acuerdos de externalización debidamente documentado, en donde se distinga la subcontratación de funciones críticas. También, debe tomar las medidas apropiadas para garantizar que el regulador y auditores puedan obtener rápidamente, previa solicitud, **información y reportes periódicos sobre las tareas subcontratadas** que sea relevante para el cumplimiento contractual y/o la supervisión regulatoria.

Con el objetivo de prevenir fallas potenciales en las actividades tercerizadas, el marco de gestión debería contemplar estándares para la debida diligencia sobre los prestadores previo a la firma de un acuerdo de subcontratación. Para ello, se debe revisar que el prestador tenga la reputación comercial, la experiencia y los recursos suficientes para proveer la función y si está supervisado por las autoridades competentes. Concluida la etapa anterior, el contrato al menos debería contemplar los derechos y obligaciones de las partes en un acuerdo por escrito, una descripción clara de la función subcontratada y la fecha de finalización, las causas del término de la relación contractual (por ej. cuando haya cambios materiales que afecten la calidad del servicio) y las obligaciones financieras de las partes. Aspectos de importancia también refieren a la disponibilidad y seguridad de los datos, incluyendo el derecho de la entidad y las autoridades a auditar al proveedor con respecto a la función crítica subcontratada.

Por último, en el informe *Principles on Outsourcing* (IOSCO, 2021) se resalta la necesidad de incluir el trabajo remoto en los procesos de diligencia, los planes de recuperación y la

globales de red como Visa, Mastercard. (4) Acuerdos de compensación con cámaras de contraparte central. (5) Infraestructuras globales de mensajería reguladas, entro otros.

[4] Se define como función critica aquella cuya interrupción perjudique seriamente la resiliencia operacional, la continuidad del negocio, la viabilidad financiera de la entidad y/o afecte de manera importante a sus clientes o perjudique su reputación a largo plazo. Aquella relacionada con procesos comerciales complejos o importantes. Aquella que no pueda transferirse rápidamente a otro proveedor de servicios, considerando los costos y el tiempo para hacerlo. Aquella cuya interrupción tenga impacto potencial en la confidencialidad e integridad de los datos entregados al proveedor.

ejecución de pruebas de la entidad contratante y el proveedor, asegurando el resguardo y la confidencialidad de los datos.

Con respecto a las legislaciones de países, se destaca lo siguiente:

- En EE.UU., el regulador está facultado para auditar todo servicio subcontratado por Intermediarios y Bolsas de Valores, pero no se exige llevar una Base de Registro de Proveedores.
- En México, se exige contar con una política de externalización de servicios que asegure contar con esquemas de registro, redundancia, continuidad y monitoreo de la calidad del servicio.
- En Perú, la política de subcontratación debe contar con procedimientos para evaluar el nivel de riesgo del servicio subcontratado, selección del proveedor, monitoreo del servicio y planes de continuidad del servicio en caso de término anticipado de la relación con el proveedor. Se requiere llevar una Base de Registro de Proveedores.
- En Singapur, está prohibido subcontratar servicios por plazos inferiores a 6 meses, y el regulador está facultado a realizar una auditoría sobre los mismos.

VI. CONSULTA PÚBLICA

Entre el 08 de agosto y el 14 de septiembre de 2023 esta Comisión sometió a consulta pública la propuesta normativa que fija los requerimientos de gestión de riesgo operacional para las Sociedades Administradoras de Sistemas de Compensación y Liquidación, Empresas de Depósito y Custodia de Valores, Bolsas de Valores, Bolsas de Productos y Administradoras Generales de Fondos. En este proceso consultivo se recibieron comentarios de 26 entidades.

En lo que se refiere a la posibilidad de delegar parte de la gestión de riesgo operacional en terceros, se estableció que las Bolsas e Infraestructuras pueden delegar las funciones del encargado de Seguridad de la Información y Continuidad del Negocio en una misma persona del grupo empresarial de la entidad, provisto que mantenga su independencia de las áreas operativas y de auditoría interna del grupo.

Asimismo, las pruebas de seguridad de la información deberán ejecutarse con una periodicidad al menos anual para identificar amenazas y vulnerabilidades.

Por su parte, respecto del requisito de contar con un sitio secundario, se aclaró que éste podría ser físico o en la nube, debiendo la entidad contar con procedimientos adecuados de disponibilidad y recuperación de los servicios contratados con el proveedor

Asimismo, en la sección de externalización de servicios, se aclaró que aplica a los proveedores que sean relevantes para el suministro de servicios asociados a actividades estratégicas o del negocio de la entidad. También se especificó que las entidades deben evaluar más bien que verificar o monitorear proveedores extranjeros de tecnología, cuyos contratos de prestación de servicios son más bien contratos de adhesión.

Respecto del Reporte de Incidentes Operacionales, se solicitó aumentar el plazo de envío a más de 2 horas, pero se mantuvo este plazo de forma homogénea para las distintas entidades, considerando la necesidad de una pronta comunicación con el regulador frente a la interrupción de servicios que impacten a las personas y, eventualmente, el posible impacto sistémico que una disrupción pudiera tener en determinadas industrias o en el sistema financiero en conjunto.

Por último, respecto al Reporte de Pérdidas Operacionales, se precisó que deben informarse los incidentes que individualmente (no en conjunto) superen las 150 UF.

IV. PROPUESTA NORMATIVA

Texto de la propuesta

REF: ***IMPARTE INSTRUCCIONES SOBRE GESTIÓN DE RIESGO OPERACIONAL. DEROGA CIRCULARES N° 1.939 y 2.020, Y LA NORMA DE CARÁCTER GENERAL N° 256. MODIFICA LA NORMA DE CARÁCTER GENERAL N° 480.***

_____

NORMA DE CARÁCTER GENERAL N°xxx

[dd] de [mes] de [año]

Esta Comisión en uso de las atribuciones conferidas en el Decreto Ley N°3.538, la Ley N°18.045, la Ley N°18.876, la Ley N°19.220, la Ley N°20.345, la Ley N°20.712 y Ley N°21.521; y teniendo en consideración que su mandato legal es velar por el correcto funcionamiento, desarrollo y estabilidad del mercado financiero, ha estimado pertinente impartir las siguientes instrucciones respecto de la gestión de riesgo operacional para Administradoras Generales de Fondos, Bolsas de Valores, Bolsas de Productos, Sociedades Administradoras de Sistemas de Compensación y Liquidación de Instrumentos Financieros y Entidades de Depósito y Custodia de Valores.

I. GESTIÓN DE RIESGO OPERACIONAL

El riesgo operacional corresponde al riesgo que las deficiencias que puedan producirse en los sistemas de información, los procesos internos o el personal, o las perturbaciones ocasionadas por acontecimientos externos provoquen la reducción, el deterioro o la interrupción de los servicios que presta la entidad y, eventualmente, le originen pérdidas financieras. Incluye el riesgo de pérdidas ante cambios regulatorios que afecten las operaciones de la entidad, como también pérdidas derivadas de incumplimiento o falta de apego a la regulación vigente.

La entidad deberá tener la capacidad de seguir entregando sus servicios en caso de que se presente un evento disruptivo, para lo cual deberá gestionar el riesgo operacional mediante una adecuada combinación de políticas, procedimientos, controles, estructura organizacional y sistemas de información, conforme a la naturaleza, volumen y complejidad de sus operaciones.

Con el objeto de que la entidad desarrolle una adecuada gestión de riesgo operacional, se deberá dar cumplimiento a los principios y elementos que se señalan a continuación:

1. *Las políticas y procedimientos de gestión de riesgo operacional deberán estar formalmente establecidas y documentadas, debiendo formar parte de las políticas y procedimientos de*

gestión de riesgos de la entidad, de acuerdo con la normativa de gobierno corporativo y gestión de riesgos emitida a tal efecto por esta Comisión.

2. *Los planes de trabajo y la emisión de informes de gestión de riesgo operacional al directorio, u órgano equivalente, deberán formar parte de la gestión de riesgo integral, de acuerdo con la normativa de gobierno corporativo y gestión de riesgos de la entidad.*

3. *Las políticas y procedimientos de gestión de riesgo operacional deberán incluir, al menos, los siguientes ámbitos relacionados, descritos en las próximas secciones: A) seguridad de la información y ciberseguridad, B) continuidad de negocio; y C) externalización de servicios. Los ámbitos mencionados deberán ser considerados por la entidad en los informes que realicen las instancias encargadas de la gestión de riesgos y la auditoría interna, según corresponda.*

4. *Las políticas de gestión de riesgo operacional deben estar diseñadas para brindar una seguridad razonable que la entidad pueda desarrollar las operaciones del negocio en forma continua y eficiente, incluso ante la presencia de eventos disruptivos, salvaguardando sus servicios, procesos y activos de información. Estas políticas deben ser aprobadas por el directorio, u órgano equivalente, y ser difundidas a todo el personal dentro de la organización. Además, dichas políticas deben establecer los niveles de apetito por riesgo definidos por el directorio u órgano equivalente, que determinará la necesidad de implementar un plan de tratamiento, de forma de evitar, reducir, transferir o aceptar los riesgos, y acorde con ello, diseñar controles mitigantes.*

5. *El directorio, u órgano equivalente, debe velar porque las políticas, procesos y sistemas dentro de la organización sean consistentes con el apetito por riesgo definido y contengan líneas claras de responsabilidad sobre la gestión de riesgo operacional. Asimismo, deberá dotar a las instancias pertinentes de la entidad con los recursos y personal necesario para la gestión de riesgo operacional, en función del volumen y complejidad de las operaciones de la entidad.*

6. *Contar con indicadores claves de medición del riesgo operacional consistentes con la metodología de evaluación y monitoreo de riesgos integrales de la entidad, permitiendo al mismo tiempo establecer niveles de alerta y evaluar la eficacia de los controles adoptados. El detalle de cálculo de estos indicadores deberá ser incluido expresamente en las políticas y procedimientos de gestión de riesgo operacional de la entidad.*

A. SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

A.1. Disposiciones generales

En el ámbito de seguridad de la información y ciberseguridad, la gestión de riesgo operacional deberá incluir los siguientes elementos, tomando en consideración el volumen y complejidad de las operaciones de la entidad:

1. *Contar con una política de seguridad de la información y ciberseguridad que considere al menos lo siguiente:*

- ***1.1.*** *Procedimientos para la implementación y mantención de un sistema de gestión de seguridad de la información y ciberseguridad, de forma resguardar la disponibilidad, confidencialidad e integridad de los activos de información.*
- ***1.2.*** *Niveles de apetito por riesgo en materia de seguridad de la información y*

ciberseguridad.

1.3. *Principales funciones y responsabilidades sobre la materia.*

1.4. *Procedimientos para la evaluación de los riesgos de seguridad de la información y ciberseguridad que se podrían estar asumiendo al introducir nuevos productos, sistemas, emprender nuevas actividades o definir nuevos procesos.*

1.5. *Una actualización al menos anual o cuando ocurran cambios significativos, debiendo ser aprobada dicha actualización por el directorio, u órgano equivalente.*

2. *Contar con una política de tecnologías de información y comunicación (TIC), que considere al menos lo siguiente:*

2.1. *Definición de las líneas de responsabilidad en cuanto a la gestión de los activos de información en la entidad.*

2.2. *Definición de los procesos TIC que aseguren un adecuado diseño, transición, operación de servicio y gestión a través de sus activos de información.*

2.3. *Definición de los procedimientos que se deberán seguir para la adecuada gestión de los procesos TIC.*

3. *Definir el perfil y número necesario de personas con conocimientos comprobables en estándares de seguridad de la información y ciberseguridad.*

4. *Establecer los procedimientos para que el personal de la entidad, incluyendo el directorio u órgano equivalente, contribuya a una adecuada gestión de los riesgos de seguridad de la información y ciberseguridad, de conformidad con sus roles y responsabilidades, mediante la implementación de:*

4.1. *Procedimientos de difusión, capacitación y concientización que traten sobre los riesgos, vulnerabilidades y amenazas a la seguridad de la información, la gestión de los mismos, y las lecciones aprendidas respecto de los incidentes en esta materia para garantizar que el personal de la entidad esté debidamente preparado para enfrentar los escenarios de contingencia definidos y que comprendan sus responsabilidades en la gestión de dichos riesgos.*

4.2. *Acuerdos contractuales con los empleados que establezcan sus responsabilidades y las de la entidad en materia de seguridad de la información y ciberseguridad, incluyendo sanciones. Asimismo, dichos acuerdos deberán incluir la revocación de derechos de acceso a información y devolución de activos de información ante un proceso de cambio de posición o desvinculación de un empleado.*

5. *Auditar los procesos de gestión de la seguridad de la información y ciberseguridad, con la profundidad y alcance necesario, que considere aspectos tales como el cumplimiento de las políticas y la eficacia de los procedimientos y controles definidos en estas materias.*

6. *Establecer procedimientos que le permitan al directorio u órgano equivalente mantenerse informado en forma oportuna y periódica sobre el sistema de gestión de la seguridad de la información y ciberseguridad. Deberá dejarse constancia del reporte de la información de estas materias en las respectivas actas del directorio u órgano equivalente y los comités que se conformen para revisar estas materias.*

7. *En el caso de las Bolsas de Valores, Bolsas de Productos, Entidades de Depósito y Custodia y Sociedades Administradoras de Sistemas de Compensación y Liquidación, se deberá dar cumplimiento a las siguientes disposiciones adicionales:*

7.1. *Efectuar la gestión de los riesgos de seguridad de la información y ciberseguridad a nivel de activos.*

7.2. *Realizar una evaluación del estado actual de la seguridad de la información y ciberseguridad de la entidad a partir de un estándar o práctica internacional de común aceptación, y definir el estado deseado.*

7.3. *Establecer los planes que se deberán implementar para llegar al estado deseado.*

7.4. *Disponer de una estructura de alto nivel para la administración de crisis, con las atribuciones necesarias para gestionar los eventos disruptivos relacionados con la seguridad de la información y ciberseguridad que se puedan presentar.*

7.5. *Cuantificar el riesgo, ya sea a través de un modelo cuantitativo o cualitativo, teniendo en consideración, a lo menos, la criticidad del activo y el efecto en las dimensiones de disponibilidad, confidencialidad e integridad. Asimismo, en la definición de la probabilidad del riesgo se deberá tener en consideración, entre otros, la base de incidentes operacionales.*

7.6. *Identificar las amenazas y vulnerabilidades que puedan afectar a los activos de información, para lo cual se deberá tener en consideración toda la información disponible, interna y especialmente externa, tales como las bases de conocimiento disponibles o marcos de trabajo, públicas y no públicas, que detallen tácticas y técnicas de ataque y vulnerabilidades de activos.*

7.7. *Contar con una persona encargada de la seguridad de la información, independiente de las áreas operativas y de auditoría interna, que evalúe y provea información relevante al directorio, gerente general y otras áreas sobre el nivel de exposición a los riesgos de seguridad de la información y ciberseguridad. Sus funciones podrán ser desempeñadas por una persona del grupo empresarial al que pertenezca la entidad, siempre que mantenga su independencia de las áreas operativas y de auditoría interna del grupo.*

A.2. Procedimientos para la gestión de seguridad de la información y ciberseguridad

Sin perjuicio de lo establecido en el literal A.1 de esta sección, las entidades mencionadas a continuación deberán considerar los siguientes procedimientos:

A.2.1. Administradoras Generales de Fondos

a. Identificación

1. *Contar con una definición clara de activos de información que sea suficiente para la adecuada gestión de los riesgos asociados.*

2. *Clasificar la información, teniendo en consideración las dimensiones de disponibilidad, confidencialidad e integridad.*

3. *Definir los activos de información críticos, que son los activos considerados como indispensables para el funcionamiento del negocio, con un nivel suficiente de detalle que permita su gestión, clasificados desde una perspectiva de disponibilidad, confidencialidad e integridad.*

4. *Implementar un inventario de activos de información que permita conocer las principales características del activo, considerando al menos: hardware, software, aplicaciones, dispositivos, sistemas, datos, personal, sistemas de información externos, procesos, instalaciones, estaciones de trabajo, servidores, medios de almacenamiento y documentación física.*

5. *Actualizar el inventario de activos de información en forma continua, para lo cual los distintos procesos de gestión de riesgo operacional deberán reportar la información que pueda tener efecto en dicho inventario.*

b. Protección y Detección

1. *Establecer controles de acceso a las instalaciones e infraestructuras de negocios, operativas y dependencias técnicas, dentro de las que se encuentran los centros de datos, fuentes de energía alternativa y respaldos de datos y aplicativos.*

2. *Establecer controles de acceso a los sistemas, de manera de mitigar los riesgos de suplantación o uso indebido por parte de terceros. En el caso de instalaciones, infraestructuras y sistemas críticos, se deberá privilegiar el uso de mecanismos de autenticación multifactor.*

3. *Implementar herramientas de registro, control y monitoreo de las actividades realizadas por los usuarios y administradores de sistemas y activos de información, incluyendo usuarios de alto privilegio.*

4. *Establecer procedimientos para otorgar, revocar o modificar los privilegios otorgados a los usuarios de los sistemas, servicios de red, sistemas operativos, bases de datos y aplicaciones de negocios en función de los roles y responsabilidades del personal y sólo lo estrictamente necesario para que éste cumpla sus funciones actuales.*

5. *Establecer controles que permitan mitigar los riesgos derivados del uso de dispositivos móviles y del acceso remoto realizado por personal interno o externo, así como también los dispositivos Internet de las Cosas ("IoT").*

6. *Establecer mecanismos de control y monitoreo de las condiciones ambientales para la localización segura para los equipos y herramientas, teniendo en consideración las condiciones de humedad, temperatura y la posibilidad de desastres y otras contingencias.*

7. *Establecer procedimientos de seguridad de las operaciones y comunicaciones de la entidad, mediante la implementación de:*

> ***7.1.*** *Herramientas y controles para la detección y protección proactiva de ataques cibernéticos y otras actividades anómalas, diseñadas en función del volumen y complejidad de las operaciones de la entidad. Por ejemplo, el uso de firewalls de aplicaciones web, sistemas de prevención de intrusos, sistemas de prevención de pérdida de datos, sistemas anti-denegación de servicios, filtrado de correo electrónico, antivirus, anti-spyware y anti-malware, entre otros.*
>
> ***7.2.*** *Procesos de gestión de la configuración de los sistemas y activos de información.*
>
> ***7.3.*** *Herramientas y procedimientos para el respaldo, transferencia, restauración y eliminación segura de la información, al interior de la organización y con terceros, incluyendo medios físicos y electrónicos. Para ello se deberá considerar:*
>
> > ***a.*** *Disposiciones relativas al respaldo, transferencia, restauración y eliminación de información en las normas que resguardan la protección de datos y los derechos del inversionista, incluyendo acuerdos de no divulgación.*
> >
> > ***b.*** *Técnicas de encriptación y segmentación de redes para información en tránsito y en reposo.*
> >
> > ***c.*** *Procesos de administración de respaldos que aseguren la disponibilidad confidencialidad e integridad de la información ante la ocurrencia de un incidente, el que debe ser concordante con el análisis de los riesgos para la gestión de la continuidad del negocio de acuerdo con lo dispuesto en la sección I.B de la presente norma. Los respaldos de la información se deben mantener en ambientes libres de códigos maliciosos y en instalaciones distintas a los sitios de producción. Además, se deben realizar pruebas de restauración de respaldos periódicas, al menos anuales, con el fin de verificar que la información crítica puede ser recuperada en los tiempos predefinidos en caso de que los datos originales se pierdan o se dañen.*

d. *Herramientas y procedimientos de identificación, autenticación y control de acceso para los canales digitales a través de los cuales la entidad interactúa con sus clientes.*

e. *Herramientas y procedimientos para que la información que la entidad decidiere almacenar o procesar mediante servicios en la nube conserve sus características de disponibilidad, confidencialidad e integridad.*

c. Respuesta y Recuperación

1. *La entidad deberá contar con procedimientos para la gestión de incidentes de seguridad de la información y ciberseguridad, considerando:*

1.1. *Una instancia de alto nivel definida por el directorio u órgano equivalente encargada de la gestión de incidentes de seguridad de la información y ciberseguridad.*

1.2. *Procedimientos de respuesta y recuperación ante incidentes, aprobados por el directorio u órgano equivalente, que consideren la recuperación oportuna de las funciones críticas, los procesos de respaldo y soporte, los activos de información críticos y las interdependencias con terceros en caso de incidentes. Dichos procedimientos deberán considerar las disposiciones relativas al registro, reporte y comunicación de incidentes de la sección I.D de esta norma. Asimismo, dependiendo de la severidad del incidente, corresponderá escalar la situación al directorio u órgano equivalente para la toma de decisiones. Los procedimientos de respuesta y recuperación ante incidentes deberán actualizarse al menos anualmente y cada vez que se registren cambios en los activos de información o se produzcan incidentes que amenacen la seguridad de éstos.*

1.3. *Procedimientos de comunicaciones para mantener informado en forma oportuna al directorio u órgano equivalente, a otras partes interesadas (tanto internas como externas), a las autoridades pertinentes en materia de seguridad de la información y ciberseguridad y a esta Comisión de la ocurrencia de un incidente y las medidas adoptadas para resolverlo. Estos procedimientos deberán considerar las disposiciones relativas al registro, reporte y comunicación de incidentes de la sección I.D de esta norma. Asimismo, tratándose de incidentes que afecten la calidad o continuidad de los servicios a los clientes o de un hecho de público conocimiento, la institución será responsable de informar oportunamente a los usuarios sobre la ocurrencia de dicho evento, debiendo actualizar la información disponible hasta que se conozcan las conclusiones sobre las causas del incidente y las medidas adoptadas para resolverlo, incluyendo el cumplimiento de las normas que resguardan la protección de datos personales y los derechos de los inversionistas.*

1.4. *Sin perjuicio de la información que debe ser reportada a esta Comisión, las entidades deberán evaluar la posibilidad de participar activamente en grupos o colectivos de intercambio de información, incluidos los grupos de la industria, el gobierno y los grupos transfronterizos para recopilar, distribuir y evaluar información sobre prácticas cibernéticas, amenazas cibernéticas e indicadores de alerta temprana relacionados con las amenazas cibernéticas.*

2. *Procedimientos para el desarrollo, adquisición y actualización de la infraestructura tecnológica de la entidad, que consideren los siguientes elementos:*

2.1. *Evaluación de las necesidades de infraestructura tecnológica de la entidad.*

2.2. *Implementación de un proceso de gestión de cambio, de forma de asegurar que las modificaciones realizadas a los activos de información producto de la introducción de nuevos productos, sistemas y actividades sean efectuadas y monitoreadas de manera segura y controlada.*

2.3. *Realización de pruebas de carácter funcional, integral, de seguridad, de ciberseguridad, de continuidad y normativas, previo al paso de producción de un servicio*

o activo de información, con el propósito de asegurar que no se produzca un impacto adverso en la seguridad de la información y en las operaciones del negocio.

2.4. *Implementación de un proceso de gestión de obsolescencia tecnológica, que permita mantener el software y hardware con soporte, salvo las excepciones debidamente fundamentadas que no generen efectos adversos para la operación de los servicios de la entidad. Se deberá prevenir el uso de software no autorizado o sin licenciamiento comercial.*

2.5. *Implementación de un proceso de gestión de actualizaciones de seguridad de software (parches).*

3. *La entidad deberá contar con un procedimiento para el mejoramiento continuo de las herramientas, procedimientos y controles de seguridad de la información y ciberseguridad que considere:*

3.1. *La recolección y análisis de información sobre el funcionamiento de activos de información.*

3.2. *El análisis de los incidentes de seguridad de la información y ciberseguridad y la efectividad de las medidas adoptadas para resolverlo.*

3.3. *La ejecución de pruebas con periodicidad al menos anual para identificar amenazas y vulnerabilidades en la seguridad de la información, con las siguientes características:*

a. *Las pruebas deberán ser diseñadas en función del volumen y complejidad de las operaciones de la entidad y supervisadas por la instancia responsable de la gestión de riesgos de la entidad.*

Las pruebas deberán estar basadas en escenarios de riesgo planificados diseñados para demostrar que los mecanismos y herramientas implementados para preservar la seguridad de la información cumplen adecuadamente con su objetivo, incluyendo ataques cibernéticos.

b. *Los resultados de las pruebas realizadas deberán ser reportados al directorio u órgano equivalente, incluyendo recomendaciones de mejora en las herramientas, procedimientos y controles.*

A.2.2. Bolsas de Valores, Bolsas de Productos, Entidades de Depósito y Custodia y Sociedades Administradoras de Sistemas de Compensación y Liquidación

a. Identificación

1. *Contar con una definición clara de activos de información que sea suficiente para la adecuada gestión de los riesgos asociados.*

2. *Clasificar la información, teniendo en consideración las dimensiones de disponibilidad, confidencialidad e integridad. Esta clasificación deberá ser utilizada para la clasificación de los activos de información.*

3. *Definir los activos de información críticos, que son los activos considerados como indispensables para el funcionamiento del negocio, con un nivel suficiente de detalle que permita su gestión.*

4. *Implementar un inventario de activos de información, el que deberá estar permanentemente actualizado. Este inventario de activos deberá ser consistente con los procesos de la entidad, además deberá contener la información que permita conocer las principales características del activo. El inventario deberá considerar a lo menos hardware,*

software, aplicaciones, dispositivos, sistemas, datos, personal, sistemas de información externos, procesos, instalaciones, medios de almacenamiento y documentación física.

***5.** Implementar un inventario de servicios. Este inventario de servicios deberá ser relacionado con los activos de información, los niveles de servicios acordados y los niveles operacionales acordados.*

***6.** Contar con un registro de todas las redes y subredes implementadas y los activos de información que conforman dichas redes. Además, se deberán identificar las conexiones entre estas redes, con las redes externas y con otras infraestructuras de mercado, nacionales y extranjeras.*

***7.** Actualizar de manera continua los inventarios y registros, para lo cual los encargados de los procesos, tales como gestión de personas, gestión de cambio, gestión de implementación y gestión de configuración, deberán reportar la información que pueda tener efecto en estos inventarios y registros.*

b. Protección y Detección

***1.** Resguardar los activos de información de manera adecuada en términos de seguridad física y ambiental, teniendo en consideración las condiciones de humedad, temperatura y la posibilidad de desastres y otras contingencias como, por ejemplo: la protección de las áreas sensibles de negocios, operativas y dependencias técnicas, dentro de las que se encuentran los centros de datos, fuentes de energía alternativa y respaldos de datos y aplicativos.*

***2.** Realizar pruebas de carácter funcional, integral, de seguridad, de ciberseguridad, de continuidad y normativas previo al paso de producción de un servicio, proceso o activo de información, o modificaciones de ellos, con el propósito de evitar que se afecte la disponibilidad, confidencialidad e integridad de los servicios vigentes. Se deberán establecer umbrales de aceptación.*

***3.** Implementar un proceso de gestión de cambio, de forma de asegurar que las modificaciones realizadas a los activos de información sean efectuadas de manera segura y controlada, que los cambios realizados son controlados y monitoreados y que las pruebas previas al paso producción hayan cumplido los umbrales definidos.*

***4.** Implementar un proceso de gestión de implementación y despliegue, de forma de asegurar el paso de producción de nuevos componentes, servicios, infraestructura u otros componentes, o la modificación de éstos.*

***5.** Implementar un proceso de gestión de capacidad, que permita asegurar que la infraestructura TIC cubre las necesidades presentes y futuras. El proceso de gestión de capacidad deberá ser a nivel de servicio, sistemas y componentes. Además, se deberá implementar un modelo que relacione las operaciones con el uso de sistemas y componentes.*

***6.** Implementar un proceso de gestión de disponibilidad, de forma de asegurar que se cumplan con los niveles de servicio de disponibilidad acordados.*

***7.** Implementar un proceso de gestión de obsolescencia tecnológica, que permita mantener el software y hardware con soporte, salvo las excepciones debidamente fundamentadas mediante una evaluación de riesgos, y que no generen efectos adversos no previstos para la operación de los servicios de la entidad. Se deberá prevenir el uso de software no autorizado o sin licenciamiento comercial.*

***8.** Implementar un proceso de gestión de configuraciones que permite asegurar adecuados controles a los elementos configurables de los activos de información; y que su acceso sea controlado y monitoreado.*

9. *Implementar un proceso de gestión de cumplimiento de los niveles de servicios acordados (SLA) y los niveles operacionales acordados (OLA).*

10. *Implementar un proceso de parches sobre la infraestructura TIC, con apoyo de una herramienta automatizada.*

11. *Proteger adecuadamente las redes informáticas de ataques provenientes de Internet o de otras redes externas, a través de la implementación de herramientas que se complementan, tales como: firewalls, firewalls de aplicaciones web (WAF), sistemas de prevención de intrusos (IPS), sistemas de prevención de pérdida de datos (DLP), sistemas anti-denegación de servicios, filtrado de correo electrónico, antivirus y anti-malware.*

12. *Segmentar las redes informáticas de manera de implementar controles diferenciados, considerando aspectos como grupos de usuarios, tráfico de datos encriptado, tipo de servicios y sistemas de información, a fin de proteger las comunicaciones y los activos de información críticos, así como aislar la propagación de los efectos adversos que podrían derivarse de ciberataques.*

La segmentación de redes debe aplicarse a los diferentes ambientes dispuestos por la entidad, entre los que se encuentran aquellos de desarrollo, de pruebas y de producción.

13. *Establecer controles que permitan mitigar los riesgos derivados del uso de dispositivos móviles y del trabajo a distancia realizado por personal interno o externo; así como también los dispositivos Internet de las Cosas ("IoT").*

14. *Implementar herramientas, procedimientos, controles y pruebas que permitan proteger, detectar y contener ataques a los activos de información realizados a través del uso de códigos maliciosos.*

15. *Implementar una gestión de identidades y de acceso físico y lógico, que contemple adecuados controles para resguardar las áreas de acceso restringido. Se deben establecer procedimientos para otorgar, revocar o modificar los privilegios otorgados a los usuarios de los sistemas, los derechos de accesos a los servicios de red, a los sistemas operativos, a las bases de datos y a las aplicaciones de negocios, entre otros.*

16. *Contar con apropiados mecanismos de control de acceso a los sistemas, de manera de mitigar, entre otros, los riesgos de suplantación o uso indebido por parte de terceros. En la medida de ser necesario, se deberá implementar un segundo factor de autenticación.*

17. *Limitar los accesos a lo estrictamente necesario para que el personal cumpla sus funciones.*

18. *Mantener un registro actualizado de los derechos de acceso individuales y del sistema, de forma de tener conocimiento de los permisos de acceso a los activos de información y sus sistemas de respaldo.*

19. *Implementar herramientas para controlar, registrar y monitorear las actividades realizadas por los usuarios sobre los activos de información, así como de aquellos con privilegios especiales.*

20. *Definir procedimientos que determinen la información que requiere ser protegida a través de técnicas de cifrado, así como los algoritmos criptográficos permitidos o autorizados, tanto para la información en tránsito y en reposo.*

21. *Implementar adecuados resguardos para la conservación, transferencia y eliminación de la información, en conformidad con lo establecido en las políticas internas y la regulación vigente.*

22. *Implementar procedimientos y herramientas que permitan en forma proactiva identificar, recolectar y analizar información interna y externa respecto de nuevas amenazas y*

vulnerabilidades que puedan afectar sus activos de información.

23. *Implementar procesos de administración de respaldos que le permita asegurar la disponibilidad, confidencialidad e integridad de su información y de sus medios de procesamiento, ante la ocurrencia de un incidente, desastre u otra contingencia, el que debe ser concordante con el análisis de los riesgos para la gestión de la continuidad del negocio. Los respaldos de la información se debiesen mantener en ambientes libres de códigos maliciosos, adecuadamente controlados, y en instalaciones distintas a los sitios de producción. Además, se deben realizar al menos anualmente pruebas de restauración de sus respaldos, con el fin de verificar que la información crítica puede ser recuperada en caso de que los datos originales se pierdan o se dañen.*

24. *Implementar un Security Operation Center (SOC), propio o a través de un servicio externo, con instalaciones, herramientas tecnológicas, procesos y personal dedicado y entrenado, a fin de prevenir, detectar, evaluar y responder a amenazas e incidentes de ciberseguridad.*

25. *Identificar y evaluar en forma continua los vectores de ataque a los cuales pudieran estar expuestos los activos de información, como por ejemplo la manipulación o interceptación de las comunicaciones, phishing, malware, elevación de privilegios, inyección de código, denegación de servicios, ingeniería social, etc.; distinguiendo claramente entre aquellos que pueden afectar la infraestructura física, la infraestructura lógica o el equipamiento de usuarios finales (endpoint).*

26. *Realizar en forma continua, con el suficiente alcance y profundidad, pruebas de seguridad de infraestructura tecnológica para detectar las amenazas y vulnerabilidades que pudieran existir, tales como pentesting, red team o ethical hacking.*

27. *Implementar herramientas, procedimientos y controles que permita identificar vulnerabilidades de día cero.*

28. *Implementar una gestión de vulnerabilidades, para asegurar que las vulnerabilidades identificadas en los activos de información, a través de las diferentes herramientas, procedimientos y controles sean oportunamente solucionadas.*

29. *Implementar procedimientos para verificar que las principales vulnerabilidades identificadas no han sido explotadas.*

30. *Implementar procedimientos para la gestión de las alertas o amenazas de seguridad de la información y ciberseguridad, con el fin de detectar, investigar y generar acciones de mitigación de impacto de estos eventos, y resguardar la disponibilidad, confidencialidad e integridad de sus activos de información.*

c. Respuesta y Recuperación

1. *Implementar procedimientos de respuesta y recuperación ante incidentes de seguridad de la información y ciberseguridad, aprobados por el directorio. Estos procedimientos deberán considerar las disposiciones relativas al registro, reporte y comunicación de incidentes de la sección I.D de esta norma. Asimismo, dependiendo de la severidad del incidente, corresponderá escalar la situación al directorio u órgano equivalente para la toma de decisiones.*

Estos planes deben ser probados al menos anualmente, y actualizados cada vez que se registran cambios en los activos de información o se materialicen eventos que amenacen la seguridad de la información y ciberseguridad.

2. *Establecer procedimientos de comunicaciones, considerando todas las partes interesadas, ya sea internas o externas, a fin de mantenerlas adecuadamente informadas. Asimismo,*

tratándose de incidentes que afecten la calidad o continuidad de los servicios a los clientes o de un hecho de público conocimiento, la entidad será responsable de informar oportunamente a los usuarios sobre la ocurrencia de dicho evento, debiendo actualizar la información disponible hasta que se conozcan las conclusiones sobre las causas del incidente y las medidas adoptadas para resolverlo, incluyendo el cumplimiento de las normas que resguardan la protección de datos personales y los derechos del inversionista.

3. *Implementar un proceso de análisis forense para los incidentes relevantes, que incluya al menos las etapas de identificación, recopilación, adquisición, examen y análisis de evidencias digitales, junto con la generación de documentación e informes de la investigación forense, interpretación de evidencia digital y las conclusiones del trabajo realizado; además de los requerimientos necesarios para custodiar adecuadamente las evidencias generadas.*

4. *Mantener con una base de incidentes de los activos de información suficientemente detallada que le permita perfeccionar la capacidad de respuesta de éstos.*

5. *Realizar autoevaluaciones al menos anuales para determinar el grado de cumplimiento con las políticas internas, la regulación vigente y la adherencia a las mejores prácticas, de manera de determinar las vulnerabilidades de su infraestructura y tomar las acciones para su mitigación, así como para prever la adopción oportuna de medidas ante escenarios de amenazas de ciberseguridad. Además, se deberá evaluar la certificación a estándares disponibles.*

6. *En el caso de las Bolsas de Valores y las Bolsas de Productos, éstas deberán evaluar la posibilidad de participar activamente en grupos o colectivos de intercambio de información, incluidos los grupos de la industria, el gobierno y los grupos transfronterizos para recopilar, distribuir y evaluar información sobre prácticas cibernéticas, amenazas cibernéticas e indicadores de alerta temprana relacionados con las amenazas cibernéticas. Además, también deberán compartir la información de estos incidentes entre sus corredores, disponiendo de sistemas especializados y seguros para este fin.*

B. CONTINUIDAD DEL NEGOCIO

B.1. Disposiciones generales

En el ámbito de continuidad de negocio, la gestión de riesgo operacional deberá incluir los siguientes elementos:

1. *Contar con una política de continuidad de negocio que contenga al menos lo siguiente:*

1.1. *Procedimientos de respuesta ante la ocurrencia de eventos internos o externos que pudieran crear una interrupción en la continuidad de las operaciones del negocio. Estos procedimientos se deberán referir al menos a la ejecución de un análisis de impacto de negocio (BIA, por su sigla en inglés) y un Análisis de Impacto de Riesgo (RIA, por su sigla en inglés).*

1.2. *Principales funciones y responsabilidades sobre la materia, en especial, cuáles serán las instancias encargadas de definir, diseñar, ejecutar y mejorar los procedimientos y metodologías para la gestión de continuidad de negocio. La política de continuidad del negocio formará parte de las políticas de gestión de riesgos de la entidad, debiendo ser actualizada y aprobada al menos anualmente por el directorio u órgano equivalente o ante cambios significativos.*

2. *Contar con personas con conocimientos comprobables en estándares de continuidad de negocio y experiencia en la gestión de los riesgos asociados, cuyas actividades principales serán el desarrollo y mejora de las políticas, procedimientos y controles para la gestión de continuidad de negocio.*

3. *Establecer políticas de capacitación y concientización para garantizar que el personal de la*

entidad esté debidamente preparado para enfrentar los escenarios de contingencia definidos y que comprendan sus responsabilidades en la gestión de los riesgos del sistema de continuidad de negocio.

4. *Disponer de procedimientos que permitan al directorio u órgano equivalente estar informado de manera oportuna y periódica sobre la gestión de continuidad de negocio. Deberá dejarse constancia del reporte de la información en estas materias en las respectivas actas del directorio u órgano equivalente y en los comités que se conformen para revisarlas.*

B.2. Procedimientos para la Gestión de la Continuidad de Negocios

Sin perjuicio de lo establecido en el literal B.1, se deberán implementar los siguientes elementos mínimos para la gestión de la continuidad de negocios:

1. *Contar con un Plan de Continuidad de Negocio y Recuperación de Desastres, aprobado anualmente por el directorio u órgano equivalente, que contenga:*

1.1. *Los procedimientos para la gestión de eventos de continuidad, con un nivel de detalle que permita a las distintas instancias afectadas determinar las actividades a desarrollar en cada escenario definido.*

1.2. *Los criterios para la activación del Plan y para la vuelta a la normalidad. Esto incluye evaluar oportunamente los riesgos asociados a la continuidad de negocios que se podrían estar asumiendo al introducir nuevos productos, sistemas, emprender nuevas actividades o definir nuevos procesos.*

1.3. *Roles y responsabilidades del personal.*

La periodicidad de actualización de este Plan podría ser mayor dependiendo de la normativa propia de la entidad, o a requerimiento de esta Comisión.

2. *Realizar o actualizar, al menos anualmente o ante eventos que amenacen la continuidad de las operaciones del negocio, un BIA con el objeto de identificar los procesos de mayor relevancia para la continuidad de negocio, el impacto que tendría una interrupción de esos procesos, y los tiempos y recursos necesarios para la continuidad y recuperación de éstos. El BIA deberá realizarse a nivel estratégico, táctico y operativo. De esos procesos, y considerando los niveles de apetito por riesgo definidos, se deberá determinar:*

2.1. *Los tiempos máximos tolerables de interrupción (MTPD por sus siglas en inglés);*

2.2. *Los tiempos objetivos de recuperación (RTO por sus siglas en inglés);*

2.3. *Los puntos objetivos de recuperación (RPO por sus siglas en inglés);*

2.4. *Los niveles mínimos aceptables de operación (MBCO por sus siglas en inglés); y*

2.5. *Los recursos humanos, tecnológicos y de infraestructura e información necesarios para su continuidad y recuperación.*

Los resultados del BIA deberán ser aprobados por el directorio u órgano equivalente.

3. *Disponer de un sitio secundario físico o en la nube que permita a la entidad reanudar la operación en caso de que esta se vea interrumpida en el sitio principal, permitiendo restablecer los procesos de mayor relevancia del negocio, tales como plataformas, infraestructura, sistemas y procesamiento de datos.*

4. *Realizar o actualizar, al menos anualmente, una evaluación de impacto de riesgos (RIA) que permita identificar y analizar los riesgos de continuidad de negocio que, de materializarse, provocarían una interrupción en los procesos de mayor relevancia de la entidad. Para lo anterior, se deberá considerar escenarios internos y externos, contemplando, entre otros, la falta total y parcial de los sistemas tecnológicos; ataques maliciosos que afecten la*

ciberseguridad; la ausencia de personal crítico; la imposibilidad de acceder o utilizar las instalaciones físicas y la falta de provisión de los servicios críticos contratados a proveedores.

5. *Definir, en base a los resultados del BIA y el RIA, una estrategia de continuidad de negocio que tenga por objetivo mantener la continuidad de los procesos de mayor relevancia, considerando medidas preventivas para reducir la probabilidad de materialización de daños, minimizar el tiempo de recuperación y limitar el impacto en las operaciones del negocio de la entidad.*

6. *Implementar un Plan de gestión de crisis en el que se determine los procedimientos de escalamiento, comunicaciones, gestión y reporte de eventos de continuidad operacional para mantener informado en forma oportuna al directorio u órgano equivalente, a todas las partes interesadas y a esta Comisión, respecto de información relevante del evento de continuidad, las medidas adoptadas para resolverlo y la coordinación de una respuesta adecuada. La coordinación de una respuesta adecuada deberá considerar los puntos objetivos y tiempos objetivos de recuperación previstos en el BIA.*

7. *Contar con un procedimiento para el mejoramiento continuo de las políticas, planes y procedimientos de continuidad del negocio con el objeto de disminuir los tiempos de respuesta cuando se repita un incidente igual o similar; identificar posibles mejoras en los procesos; facilitar el intercambio de conocimientos; y disponer de información que permita apoyar la toma de decisiones en caso de materializarse nuevos incidentes.*

8. *Probar anualmente el Plan de Continuidad de Negocio y Recuperación de Desastres, de forma de asegurar que son adecuados y efectivos. Lo anterior, sin perjuicio de que esta Comisión pueda solicitar una periodicidad diferente en función del volumen y complejidad de las operaciones de la entidad. Estas pruebas deberán considerar al menos lo siguiente:*

> ***8.1.*** *Deberán ser diseñadas en función del volumen y complejidad de operaciones de la entidad y ser supervisadas por la instancia responsable de la Gestión de Riesgos de la entidad.*
>
> ***8.2.*** *Deberán estar basadas en escenarios de riesgo que se asimilen a eventos reales, incluyendo escenarios severos pero plausibles. Lo anterior, para demostrar que los procedimientos de continuidad de negocio funcionarán en caso de ser necesarios, incluyendo ataques cibernéticos, desastres y otras contingencias.*

Se deberán emitir reportes de los resultados de las pruebas realizadas al directorio u órgano equivalente, que contengan recomendaciones y acciones para implementar mejoras al Plan de Continuidad de Negocio y Recuperación ante Desastres.

B.3. Disposiciones adicionales para Bolsas de Valores, Bolsas de Productos, Entidades de Depósito y Custodia y Sociedades Administradoras de Sistemas de Compensación y Liquidación

1. *Contar con una persona encargada de la continuidad del negocio, independiente de las áreas operativas y de auditoría interna, que evalúe y provea información relevante al directorio, gerente general y otras áreas sobre el nivel de exposición a los riesgos de continuidad de negocios. Sus funciones podrán ser desempeñadas por una persona del grupo empresarial al que pertenezca la entidad, siempre que mantenga su independencia de las áreas operativas y de auditoría interna del grupo.*

2. *Diseñar e implementar el Plan de Continuidad del Negocio y Recuperación ante Desastres para permitir la reposición de los servicios con un tiempo objetivo de recuperación no mayor a 2 horas y un punto objetivo de recuperación cercano a 0.*

3. *En el caso de las Bolsas de Valores:*

3.1. *Contar con infraestructura y sistemas que tengan una capacidad instalada que permita procesar el mayor entre: (i) el doble del mayor número de transacciones por segundo registrado en las bolsas del país durante los últimos cinco años o; (ii) mil órdenes por segundo. Sin perjuicio de lo anterior, las bolsas deberán garantizar que sus sistemas puedan hacer frente a un aumento súbito de transacciones, sin deterioro importante del funcionamiento de los sistemas. Lo anterior debe ser probado anualmente.*

A su vez, la bolsa deberá adoptar los resguardos que sean necesarios para garantizar que sus sistemas comunicarán en tiempo real y con la menor latencia posible a los sistemas de las otras bolsas aquellas órdenes compatibles con la mejor oferta vigente en tales sistemas. Además, que esos sistemas comunicarán los calces y anulaciones que en ellos ocurran a la bolsa de la que emanó la orden respectiva.

3.2. *Contar con un centro de procesamiento de datos principal y, al menos, uno de respaldo, permanentemente homologados en infraestructura y software, con capacidad, en cuanto a energía, refrigeración y mantenimiento, para alcanzar una disponibilidad de operación de a lo menos 99,98% o downtime de 1,6 horas anuales. El diseño, construcción y operación de esos centros de procesamiento de datos debe ser certificado por una entidad especializada e independiente. Estos sitios deben estar ubicados de forma tal de evitar quedar expuestos a los mismos riesgos.*

No obstante, quedarán exceptuadas de cumplir con la certificación de uno de los centros de procesamiento de datos aquellas bolsas de valores que, dentro de los doce meses anteriores al día de cálculo, no hayan alcanzado un volumen igual o superior a las 400 mil operaciones mensuales sobre instrumentos de renta variable en sus sistemas de calce automático. A partir de los 15 meses posteriores de alcanzado ese volumen de operaciones, dicha bolsa deberá tener certificados ambos centros de procesamiento de datos. El centro de procesamiento certificado deberá corresponder al sitio principal, en caso de no poseer la modalidad activo-activo entre ambos centros de procesamiento de datos.

Similar obligación en cuanto a la mantención de centros de procesamiento será aplicable para las Bolsas de Productos, no obstante, la certificación solo será exigible a uno de los sitios, debiendo ser el sitio principal, en caso de no poseer la modalidad activo-activo.

3.3. *Establecer niveles mínimos de servicio, tales como disponibilidad y latencia para los servicios brindados, los que deben ser aprobados por el directorio. Estos niveles mínimos de servicio deberán ser definidos considerando las obligaciones establecidas en el marco normativo y las necesidades de mercado. A partir de estos niveles de servicios, se deben definir los niveles operacionales acordados para la infraestructura que soporta los servicios, debiéndose verificar el cumplimiento de estos niveles. Se debe implementar un proceso de gestión de cumplimiento de los niveles de servicios acordados y los niveles operacionales acordados.*

3.4. *Contar con la infraestructura de telecomunicaciones y equipamiento computacional con la redundancia necesaria de forma de evitar los puntos únicos de falla.*

3.5. *Remitir información sobre disponibilidad y latencia de sus sistemas, información operacional, Plan de Continuidad Operacional y Recuperación ante Desastres, planificación de ejercicios de continuidad operacional y proyectos de infraestructura tecnológica en los plazos y condiciones establecidos en las normativas de envío de información de Bolsas de Valores de esta Comisión.*

C. EXTERNALIZACIÓN DE SERVICIOS

C.1. Riesgos de externalización

1. *Los servicios prestados por los proveedores, relacionados con el cumplimiento normativo, la continuidad del negocio, la seguridad de la información y la calidad de los servicios, productos, información e imagen de la entidad contratante, deberán ser considerados en los procesos de gestión de riesgo de la entidad. En tal sentido, para la evaluación de riesgos de contratación de proveedores, se deberán considerar, entre otros, los siguientes riesgos:*

1.1. *Riesgo de sustitución: la posibilidad de sustituir o no a un proveedor dentro de un plazo determinado que garantice la continuidad del servicio contratado.*

1.2. *Riesgo de intervención: la posibilidad que la entidad tenga que hacerse cargo de la función contratada.*

1.3. *Riesgo de subcontratación: la posibilidad que el proveedor subcontrate a su vez todo o parte del servicio, reduciendo la capacidad de la entidad de supervisar la función subcontratada.*

1.4. *Riesgo de concentración: la posibilidad que una entidad contrate uno o varios servicios en un mismo proveedor que sea difícil de sustituir, incrementando la posibilidad de fallas o interrupciones prolongadas.*

1.5. *Riesgo legal: la posibilidad de contingencias legales que pudieran afectar la integridad y exactitud de la información que mantiene la entidad de proveedores para fines de cumplimiento regulatorio.*

C.2. Procedimientos para la gestión de servicios externalizados

En el ámbito de externalización de servicios, la gestión de riesgo operacional de los servicios referidos en la sección C.1 deberá considerar los siguientes elementos:

1. *Contar con una política para la externalización de servicios que considere a lo menos lo siguiente:*

1.1. *Definir la estructura de gobierno y de los procedimientos a seguir para autorizar y gestionar la externalización de servicios por terceros, incluyendo las líneas de reporte y de responsabilidad.*

1.2. *Establecer los objetivos en materia de externalización de servicios.*

1.3. *Establecer los niveles de apetito a los riesgos definidos en la sección C.1 y las estrategias de mitigación.*

1.4. *Cumplir con las disposiciones en materia de seguridad de la información, ciberseguridad y continuidad de negocios.*

1.5. *Establecer los procedimientos para la determinación de los servicios críticos. En tal sentido, para entender como crítico un servicio se deberán tener en cuenta lo siguiente:*

a. *El efecto que una debilidad o falla en la provisión o ejecución del servicio tenga sobre el cumplimiento normativo, continuidad del negocio, seguridad de la información y la calidad de los servicios, productos, información e imagen de la entidad contratante.*

b. *La complejidad de las funciones comerciales asociadas.*

c. *El grado en que el servicio puede transferirse rápidamente a otro proveedor, considerando los costos y el tiempo para hacerlo.*

1.6. *Definir los servicios que solo pueden ser externalizados con la aprobación previa del*

directorio u órgano equivalente.

1.7. *Definir los elementos mínimos que deberá incorporar el contrato de prestación de servicios.*

1.8. *Definir los elementos de la gestión de riesgo que no serán aplicados a actividades que por su naturaleza no tengan impacto relevante en la prestación de los servicios.*

1.9. *Incluir a la política de externalización de servicios como parte de las políticas de gestión de riesgos de la entidad, debiendo ser aprobada y actualizada al menos anualmente por el directorio u órgano equivalente, o con una frecuencia mayor en caso de cambios internos o externos significativos.*

2. *Establecer procedimientos para la selección, contratación y monitoreo de proveedores que consideren:*

2.1. *Una definición de los criterios particulares de contratación, cuando el proveedor se trate de una entidad relacionada. Estos criterios deberán estar destinados a evitar los conflictos de interés que se pueden presentar. En el caso de Administradoras Generales de Fondos, la gestión de servicios externalizados deberá también considerar aquellos servicios que se encuentren externalizados para los fondos fiscalizados administrados por ella.*

2.2. *La incorporación al análisis de elementos que permitan llevar a cabo un proceso de debida diligencia, de forma de asegurar que los proveedores tengan una adecuada reputación comercial, solvencia financiera, experiencia y recursos suficientes para garantizar la calidad de la provisión del servicio. En el caso de servicios de procesamiento de datos realizados en el extranjero, el directorio u órgano equivalente de la entidad deberá revisar y evaluar antecedentes que respalden la calidad del servicio prestado, la solidez financiera del proveedor y la existencia de una adecuada legislación de protección de datos personales en la jurisdicción aplicable, haciéndose responsable por la disponibilidad, confidencialidad e integridad de la información entregada al proveedor contratado.*

3. *Contemplar en los contratos con los proveedores de servicios externalizados los siguientes contenidos mínimos:*

3.1. *Una descripción clara del servicio contratado y el plazo de vigencia.*

3.2. *Las obligaciones de prestación del servicio por parte del proveedor, definiendo niveles de servicio acordados. La entidad deberá definir las situaciones que se considerarán graves incumplimientos contractuales y causales de término anticipado del contrato.*

3.3. *La obligación de comunicar cualquier acontecimiento que pueda tener un impacto material en la capacidad para llevar a cabo el servicio externalizado.*

3.4. *Los requisitos de seguridad de la información, ciberseguridad y continuidad de negocios que deberá cumplir el proveedor, que deben ser concordantes con las disposiciones establecidas en esta materia por la entidad. Los proveedores deberán contar con procedimientos de gestión de incidentes y continuidad de negocios que le permitan seguir brindando los servicios en el evento que se presenten situaciones disruptivas.*

3.5. *La documentación de los procedimientos operacionales, administrativos y tecnológicos propios del servicio contratado. En el caso de existir subcontratación en cadena, la entidad deberá verificar el cumplimiento de las condiciones pactadas con el proveedor de servicios inicial y las entidades subcontratadas por este último.*

3.6. *Los procedimientos para la evaluación y monitoreo periódico de la calidad de la provisión del servicio externalizado. La entidad podrá pactar con el proveedor la realización de auditorías por terceros designados o por la propia entidad, quien será responsable en última instancia por garantizar la calidad de la provisión del servicio externalizado.*

3.7. *Las estrategias para el término de la prestación de servicios externalizados sin perjudicar las operaciones de la entidad, incluyendo el caso en que se produzcan contingencias legales. Estas situaciones deberán ser consideradas en el Plan de Continuidad del Negocio y Recuperación ante Desastres.*

4. *Contar con un registro de servicios externalizados para gestionar los riesgos de subcontratación. Dicho registro deberá estar disponible para su consulta permanente por esta Comisión y deberá incluir al menos la siguiente información:*

4.1. *Identificación del servicio externalizado, incluyendo una breve descripción del mismo y de los datos involucrados si corresponde a un servicio crítico, el área usuaria, si existe subcontratación en cadena, y si se lleva a cabo en la nube.*

4.2. *Identificación del proveedor, incluyendo si corresponde a una entidad relacionada o no.*

4.3. *Fecha de inicio, renovación y término del servicio.*

4.4. *En el caso de servicios de procesamiento de datos, una descripción de los datos y tratamientos que se subcontratan, las medidas de seguridad adoptadas, y la ubicación geográfica del proveedor.*

4.5. *En caso de subcontratación en cadena, se deberá detallar cuáles son las entidades a las que el proveedor subcontrata el servicio, una descripción de los riesgos asociados y si el proveedor realiza un control de la calidad de la provisión del servicio subcontratado en cadena.*

5. *Monitorear periódicamente que los proveedores cumplen con las condiciones pactadas para garantizar la calidad de la provisión del servicio. La entidad será responsable de la calidad de los servicios externalizados.*

6. *En el caso que la entidad decida contratar servicios de acceso y tratamiento de información en la nube, o que el proveedor como parte de la subcontratación en cadena considere los servicios en la nube, realizar un análisis reforzado de los riesgos inherentes a esos servicios, analizando en particular cómo podría afectarse la disponibilidad, confidencialidad e integridad de la información, y la continuidad de negocio de la entidad. Ese análisis deberá tener en consideración factores tales como:*

6.1. *Las certificaciones independientes respecto a la gestión de la seguridad de la información y la calidad de la prestación del servicio del proveedor.*

6.2. *La celebración del contrato de externalización de servicios directamente entre la entidad y el proveedor, con la finalidad de minimizar los riesgos que podría aportar el intermediario en este tipo de servicios.*

6.3. *El procesamiento o almacenamiento de información en otras jurisdicciones, y en ese caso la existencia de normas que resguardan la protección de datos personales, la disponibilidad, confidencialidad e integridad de la información y la resolución de contingencias legales.*

6.4. *La existencia de adecuados mecanismos de seguridad del proveedor, tanto físicos como lógicos, que permitan aislar los componentes de la infraestructura en la nube que la entidad comparte con otros clientes del proveedor, de manera de prevenir fugas de información o eventos que puedan afectar la disponibilidad, confidencialidad e integridad de los datos de la entidad.*

6.5. *La utilización de técnicas de encriptación para los datos que la entidad establezca, de acuerdo con su naturaleza y sensibilidad.*

7. *Evaluar que el proveedor de los servicios contratados posea adecuados conocimientos y*

experiencia.

8. *Mantener personal con el debido conocimiento para efectuar el control de la prestación de servicios efectuada por sus proveedores. Asimismo, también deberá vigilar el debido cumplimiento de aquellos aspectos regulatorios y legales que pudiesen afectar la provisión de los servicios contratados.*

El directorio u órgano equivalente deberá mantenerse informado sobre las materias referidas a la externalización de servicios, para lo cual deberá disponer de procedimientos que le permitan informarse de manera oportuna y periódica. Deberá dejarse constancia del reporte de la información en estas materias en las respectivas actas del directorio u órgano equivalente y en los comités que se conformen para revisar estas materias.

D. INFORMACIÓN DE INCIDENTES OPERACIONALES

D.1. Registro y comunicación de incidentes operacionales

1. *Las entidades deberán comunicar a esta Comisión los incidentes operacionales que afecten la continuidad del negocio, los recursos e información de la entidad o de sus clientes y la calidad de los servicios. A modo de ejemplo, y sin el objeto de ser exhaustivos ni taxativos, deberán ser reportadas las fallas en servicios y sistemas importantes para las operaciones del negocio; problemas tecnológicos que afecten la seguridad de la información; ataques del ciberespacio; virus o malware detectados en los activos de información críticos; eventos de indisponibilidad o interrupción de algún servicio o producto que afecte a los clientes, en cualquier canal; pérdidas o fugas de información de la entidad o de clientes; los incidentes que afecten el patrimonio de la entidad producto de fraudes internos o externos; problemas que afecten la continuidad de proveedores de servicios críticos; entre otros. Esta información deberá ser mantenida por la entidad en una base de datos de incidentes y otra base de datos de pérdidas operacionales para el mejoramiento continuo del proceso de gestión de riesgo operacional.*

En el caso de las Bolsas de Valores y Bolsas de Productos, a modo de ejemplo, también deberá considerarse lo siguiente: eventos de aumento de latencia de los servicios de negociación; eventos de caída de rendimiento sobre el registro y calce de las órdenes en los sistemas de negociación; eventos que afecten el accesos a los sistemas por parte de los corredores o de los clientes de éstas; problemas de comunicación con otras bolsas o entidades relevantes como Sociedades Administradoras de Sistemas de Compensación y Liquidación de instrumentos financieros y Entidades de Depósito y Custodia de valores; los incidentes que afecten la disponibilidad, confidencialidad, integridad y oportunidad de divulgación de información bursátil a través de los distintos canales que posea.

2. *En el caso de las Bolsas de Valores, Bolsas de Productos, Sociedades Administradoras de Sistemas de Compensación y Liquidación y Entidades de Depósito y Custodia de Valores, la ocurrencia de un incidente operacional de aquellos mencionados en el numeral anterior deberá ser informada a esta Comisión en un plazo máximo de 15 minutos transcurridos desde que la entidad tomó conocimiento del hecho. En el caso de las Administradoras Generales de Fondos, el plazo máximo será de 2 horas desde que la entidad tomó conocimiento del hecho. Las instrucciones para reportar los incidentes operacionales a esta Comisión se encuentran en los Anexos N° 2 y 4.*

Los plazos señalados anteriormente son sólo para efectos de notificar a esta Comisión de la ocurrencia del incidente con la información disponible en ese momento y no implica que la entidad deba tener resuelto el problema, haber tomado determinadas acciones o tener aclarada las causas del incidente, lo que podría ser materia de reportes de seguimiento del incidente enviados a esta Comisión posteriormente.

3. *Para estos efectos, el directorio u órgano equivalente deberá definir un funcionario encargado y un suplente para la realización de reportes y envío de información según lo indicado en esta sección. Estas personas deberán tener un nivel ejecutivo y ser designados por la entidad, tanto para este efecto como para responder eventuales consultas por parte de esta Comisión.*

4. *En los casos en que esta Comisión lo estime necesario, podrá requerir a la entidad la elaboración de un informe interno que contenga al menos: el análisis de las causas del incidente; la generación de documentación e informes de investigación; un análisis del impacto generado en los servicios; el plan de tratamiento para evitar con alto grado de seguridad que se vuelva a presentar; y las materias adicionales que esta Comisión pueda requerir.*

5. *Sin perjuicio de lo anterior, la entidad deberá mantener informado en forma oportuna al directorio u órgano equivalente de todos los incidentes operacionales relevantes y las medidas adoptadas para resolverlo.*

6. *En adición a lo expuesto, las Sociedades Administradoras de Sistemas de Compensación y Liquidación de Instrumentos Financieros y las Entidades de Depósito y Custodia con las disposiciones adicionales establecidas en el Anexo N° 4 de esta norma.*

D.2. Registro y comunicación de pérdidas operacionales

1. *Se entiende por pérdida operacional toda pérdida financiera resultante de la materialización del riesgo operacional de acuerdo con lo definido anteriormente. Esto incluye las pérdidas financieras debido a cambios legales o regulatorios que afecten las operaciones de la entidad, o producto de incumplimientos con la regulación vigente.*

2. *Las entidades deberán enviar a esta Comisión la información de todos los incidentes que se materialicen individualmente en pérdidas operacionales mayores a 150 Unidades de Fomento, de acuerdo con las instrucciones del Anexo N° 3 de la presente norma, 15 días hábiles después del cierre de junio y diciembre de cada año.*

3. *Los criterios para la confección del registro de pérdidas operacionales son los siguientes:*

3.1. *La entidad deberá contar con procesos y procedimientos documentados para la identificación, recopilación, uso y comunicación de los registros de pérdida operacional. Esta Comisión podrá exigir que el cumplimiento de tales requisitos sea validado a través de un pronunciamiento emitido por empresas de auditoría externa, de aquellos inscritos en el Registro de Empresas de Auditoría Externa de esta Comisión, que cuenten con unidades especializadas en la evaluación de procedimientos y mecanismos de gestión de riesgo operacional, con una experiencia no inferior a 5 años en dichas materias.*

3.2. *Los registros internos sobre pérdidas operacionales de la entidad deberán ser integrales e incluir la totalidad de las actividades y exposiciones relevantes, en todos los sistemas y en todas las ubicaciones geográficas pertinentes.*

3.3. *La entidad deberá recopilar información sobre los importes brutos de las pérdidas, y sobre las fechas de referencia de los eventos de riesgo operacional. Además, la entidad deberá recoger información sobre recuperaciones de importes brutos de pérdidas, e información descriptiva sobre los factores determinantes o las causas del evento de pérdida. El grado de detalle de la información descriptiva deberá ser proporcional al importe bruto de la pérdida.*

3.4. *La entidad deberá utilizar la fecha de contabilización del evento para construir el conjunto de registros sobre pérdidas. En el caso de eventos legales, la fecha de contabilización se refiere a cuando se constituye una provisión para esta contingencia legal en el estado de situación financiera, con su reflejo correspondiente en el estado de*

resultados.

3.5. *Las pérdidas causadas por un evento de riesgo operacional común o por varios eventos de riesgo operacional relacionados a lo largo del tiempo, pero contabilizadas en el transcurso de varios años, deberán asignarse a los años correspondientes en la base de datos de pérdidas, en consonancia con su tratamiento contable.*

4. *Por pérdida bruta se entiende una pérdida antes de recuperaciones de cualquier tipo.*

4.1. *Los siguientes ítems deberán ser incluidos en los cálculos de las pérdidas brutas para la base de datos de pérdidas:*

a. *Cargos directos en las cuentas de estados de resultados de la entidad y amortizaciones debido a eventos de riesgo operacional del período. Por ejemplo, costos incurridos como consecuencia de un evento, incluyendo gastos externos con una relación directa al evento por riesgo operacional (por ejemplo, gastos legales directamente relacionados al evento y comisiones pagadas a los asesores, abogados o proveedores) y costos de reparación o reemplazo incurridos para restaurar la posición que prevalecía antes del evento de riesgo operacional.*

b. *Cargos directos en las cuentas de estados de resultados de la entidad y amortizaciones debido a eventos por riesgo operacional de ejercicios contables previos que afecten los estados financieros de la entidad en el presente periodo.*

4.2. *Los siguientes ítems deberán ser excluidos de las pérdidas brutas registradas en la base de datos de pérdidas:*

a. *Costos por contratos de mantenimientos generales de la propiedad, planta o equipos.*

b. *Gastos internos o externos con el fin de mejorar el negocio después de las pérdidas por riesgo operacional: actualizaciones, mejoras, iniciativas de gestión del riesgo y mejoras en ellas.*

c. *Primas de seguro.*

5. *Por pérdida neta se entiende la pérdida después de tener en consideración los efectos de las recuperaciones. La recuperación es un hecho independiente, relacionado con el evento de pérdida inicial, que no necesariamente se efectúa en el mismo periodo en el que se perciben los fondos respectivos.*

La entidad deberá ser capaz de identificar las recuperaciones no procedentes de seguros y las recuperaciones originadas por el pago de indemnizaciones de seguros para todos los eventos de pérdidas operacionales. Asimismo, deberá utilizar las pérdidas netas de recuperaciones (incluidas las procedentes de seguros) en el conjunto de registros sobre pérdidas operacionales, aunque las recuperaciones sólo podrán utilizarse para reducir las pérdidas cuando se haya recibido el pago.

II. DISPOSICIONES ADICIONALES PARA SOCIEDADES ADMINISTRADORAS DE SISTEMAS DE COMPENSACIÓN Y LIQUIDACIÓN Y ENTIDADES DE DEPÓSITO Y CUSTODIA DE VALORES

Las Sociedades Administradoras de Sistemas de Compensación y Liquidación de Instrumentos Financieros y las Entidades de Depósito y Custodia de Valores, deberán adoptar las siguientes disposiciones adicionales en materia de gestión de riesgo operacional:

1. *Establecer sus políticas de gestión de riesgo operacional en línea con los Principios para las Infraestructuras del Mercado Financiero del Comité de Sistemas de Pago y Liquidación y*

el Comité Técnico de la Organización Internacional de Comisiones de Valores.

2. *Gestionar los riesgos derivados de su interdependencia con proveedores externos de servicios, participantes de sistemas de compensación y liquidación de instrumentos financieros, sociedades administradoras de dichos sistemas, entidades de depósito y custodia de valores y otras entidades del mercado financiero. Para ello deberán:*

2.1. *Implementar procedimientos para recopilar y analizar información de sus operaciones en forma continua, con el fin de asegurar la provisión de servicios de infraestructura en distintos escenarios (por ejemplo, cambios en la demanda por sus servicios) acorde con los niveles de apetito por riesgo definidos.*

2.2. *Disponer de acuerdos preestablecidos de intercambio de información con proveedores, clientes y otras entidades relacionadas que faciliten la prevención y gestión de incidentes (por ejemplo, comunicar la firma de acuerdos de interconexión y subcontratación de servicios críticos).*

3. *Disponer de un sitio secundario físico o en la nube que deberá contar con recursos, capacidades y funcionalidades adecuadas, idealmente ubicado a una distancia geográfica del sitio principal que sea suficiente para tener un perfil de riesgo distinto. Lo anterior debería incluir la realización de pruebas, como mínimo anualmente, conjuntas con proveedores externos, participantes y entidades relacionadas.*

4. *Incluir en el Plan de Continuidad y Recuperación ante Desastres escenarios donde la entidad deba adaptar su infraestructura tecnológica ante cambios en la demanda por sus servicios, tanto en condiciones normales como de estrés, resguardando restablecer sus operaciones de manera oportuna.*

5. *En el caso de las sociedades administradoras de sistemas de compensación y liquidación, los participantes de tales sistemas deberán acreditar ante ella el cumplimiento de los requisitos que se establecen a continuación, tanto en forma previa a la aceptación de la entidad que hubiere solicitado adquirir el carácter de participante, como permanentemente una vez adquirida esa condición:*

5.1. *Capacidades operativas de los participantes: Los participantes deberán asegurar una adecuada disponibilidad, conectividad y capacidad de sus sistemas informáticos y de comunicación, así como de sus fuentes de datos, para soportar el procesamiento de sus transacciones. Adicionalmente, deberán contar con un Plan de Continuidad de Negocio y Recuperación ante Desastres aprobado anualmente por el directorio. Con este fin, las sociedades administradoras deberán establecer en el contrato de adhesión al sistema y en las normas de funcionamiento del mismo, la facultad para que ella pueda evaluar lo indicado en este numeral. Al respecto, la sociedad administradora deberá establecer procedimientos para salvaguardar la disponibilidad, confidencialidad e integridad de la información a la que tenga acceso a causa de dicha facultad.*

5.2. *Idoneidad del personal que administra los sistemas del participante: El personal del participante, encargado de operar las aplicaciones provistas por la sociedad administradora, deberá contar con la experiencia y formación profesional acorde a las responsabilidades de su cargo y cumplir al menos con haber recibido y aprobado un programa de capacitación que defina la sociedad administradora.*

5.3. *Gestión de riesgo operacional de los participantes: Los participantes de un sistema de compensación y liquidación deberán contar con procedimientos para la gestión de riesgo operacional en los ámbitos de seguridad de la información y ciberseguridad, continuidad del negocio y externalización de servicios, sobre los procesos relativos a la compensación y liquidación de instrumentos financieros, incluidos aquellos que se generen por el ingreso directo de órdenes de compensación por parte de los clientes de un participante. Tales*

procedimientos tendrán como objetivo evaluar, controlar y monitorear los riesgos que sean inherentes a dichos procesos.

Los procedimientos mencionados dependerán del tamaño del participante, el volumen de órdenes de compensación que ingrese al sistema y del tipo de instrumentos financieros sobre los cuales opere. No obstante lo anterior, deberán incluir al menos los siguientes elementos:

a. *Una política de gestión de riesgo operacional aprobada anualmente por el directorio, incluyendo niveles de apetito al riesgo definidos.*

b. *Un manual de procedimientos, formal y actualizado, que al menos describa los procesos que interactúan con los sistemas de compensación y liquidación de instrumentos financieros, así como una descripción de los riesgos identificados y sus controles, junto a los mecanismos de monitoreo y mitigación que sean pertinentes.*

c. *Una persona o unidad responsable de desarrollar, implementar e impulsar la gestión de riesgo operacional sobre las materias indicadas en el primer párrafo de este literal.*

d. *Una persona o unidad responsable de evaluar, de forma permanente e independiente de aquella indicada en la letra c anterior, la efectividad de las políticas y procedimientos de la gestión de riesgo operacional, la cual debe informar de su labor directamente al directorio del participante, pudiendo recaer esta función en la unidad o persona que cumple las funciones de auditoría interna.*

5.4. *La sociedad administradora podrá exigir que el cumplimiento de tales requisitos sea validado a través de un pronunciamiento emitido por Empresas de Auditoría Externa, de aquellas inscritas en el Registro de Empresas e Auditoría Externa de esta Comisión, que cuenten con unidades especializadas en la evaluación de procedimientos y mecanismos de gestión de riesgo operacional, con una experiencia no inferior a 5 años en dichas materias.*

5.5. *Asimismo, la sociedad administradora podrá establecer requisitos tecnológicos diferenciados a los participantes, en la medida que ello obedezca a una segmentación basada en criterios objetivos, los cuales deberán contemplarse en las normas de funcionamiento de los respectivos sistemas.*

5.6. *Por último, en caso de que la entidad que hubiere solicitado adquirir el carácter de participante no cumpla con los requerimientos mínimos exigibles, la sociedad administradora deberá emitir un informe en el cual se fundamenten los elementos que deberán ser considerados para satisfacer dichos requerimientos.*

III. MODIFICACIONES

1. *Elimínese los numerales 1, 2 y 3 de la letra b) de la sección III de la Norma de Carácter General N°480.*

2. *Reemplácese el primer párrafo de la letra b) de la sección III de la Norma de Carácter General N° 480 por el siguiente:*

"Para efectos de poder acceder al mecanismo de interconexión en tiempo real de sistemas de calce automático establecido por el artículo 44 bis de la Ley N°18.045, la bolsa de valores respectiva deberá contar con los requisitos establecidos en la normativa de gobierno corporativo y gestión de riesgos y en la normativa de gestión de riesgo operacional de dicha entidad."

3. *Reemplácese el primer párrafo de la sección "Vigencia" de la Norma de Carácter General N° 480 por el siguiente:*

"Las instrucciones establecidas en la presente Norma de Carácter General rigen a contar de esta fecha".

IV. DEROGACIÓN

Deróguese las Circulares N° 1.939 y 2.020, y la Norma de Carácter General N°256.

V. VIGENCIA

Las instrucciones establecidas en la presente Norma de Carácter General rigen a contar del 1 de febrero de 2025.

SOLANGE BERSTEIN JÁUREGUI
PRESIDENTA
COMISIÓN PARA EL MERCADO FINANCIERO

ANEXO N° 1: DEFINICIONES

Activos de información: *corresponde a los recursos de información o elementos relacionados con el tratamiento de la información, los cuales pueden ser primarios como la información (física y lógica) y los procesos y actividades de negocio, o de soporte como hardware; software; redes de comunicación; personal; entre otros.*

Amenaza: *se refiere a cualquiera circunstancia o evento que pudiera explotar una vulnerabilidad.*

Análisis de impacto del negocio o BIA: *es el procedimiento de análisis de los efectos que puede tener en los procesos de la entidad una interrupción del negocio.*

Apetito por riesgo: *nivel agregado y tipos de riesgo que una entidad está dispuesta a asumir, previamente decidido y dentro de su capacidad de riesgo, a fin de lograr sus objetivos estratégicos y plan de negocio.*

Ataque: *en el contexto de ciberseguridad, se refiere a un evento que tuviera como intención destruir, exponer, alterar, deshabilitar, robar, u obtener acceso o hacer un uso no autorizado de un activo de información.*

Ciberseguridad: *corresponde al conjunto de acciones que realiza la entidad para mitigar los riesgos y proteger la información e infraestructura que la soporta, de eventos del ciberespacio, siendo este último el entorno resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red.*

Confidencialidad de la información: *protección de los datos contra el acceso y la divulgación no autorizados, definido por el directorio u órgano equivalente. Incluye los medios para proteger la privacidad personal y la información reservada, en especial de los clientes de la entidad.*

Downtime: *la cantidad de tiempo que el proceso o negocio es interrumpido.*

Ethical hacking: *los hackers éticos realizan evaluaciones de vulnerabilidad de seguridad y pruebas de penetración de acuerdo con métodos y protocolos aceptados por la industria. Analizan los sistemas en busca de posibles vulnerabilidades que pueden resultar de una configuración incorrecta del sistema, fallas de hardware o software o debilidades operativas.*

Externalización de servicios: *es la ejecución por un proveedor externo de servicios o actividades en forma continua u ocasional, las que normalmente podrían ser realizadas por la entidad contratante*

Incidente: *evento único o serie de eventos de seguridad de la información inesperados o no deseados, que resultaren en un intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la política de seguridad de la información de la entidad.*

Instancia: *se refiere a un nivel o grado de la estructura organizacional de la entidad, esto incluye, comité, unidad, división, departamento u otro equivalente.*

Malware: *software destinado a realizar un proceso no autorizado que tendrá un impacto adverso en la disponibilidad, confidencialidad e integridad de un sistema de información. Un virus, "worm", troyano u otra entidad basada en código que infecta un host. El "spyware" y algunas formas de adware también son ejemplos de código malicioso.*

Mecanismos de autenticación: *mecanismos utilizados para confirmar la identidad de un usuario. Estos mecanismos pueden utilizar uno o más factores de autenticación, por ejemplo, credenciales, contraseñas, certificados digitales, o características biométricas o biológicas. El mecanismo de autenticación es multifactor cuando utiliza una combinación de factores de autenticación para confirmar la identidad.*

Niveles mínimos aceptables de operación: *corresponde al mínimo nivel de servicios o productos que se consideran aceptables para que la entidad cumpla con sus objetivos durante una interrupción.*

Partes interesadas: *se refiere a las personas u organizaciones que se relacionan con las actividades y decisiones de una empresa, tales como empleados, proveedores, clientes, reguladores, entre otros.*

Phishing: *técnica para intentar adquirir datos confidenciales, como números de cuentas bancarias, a través de una solicitud fraudulenta por correo electrónico o en un sitio web, en la que el perpetrador se hace pasar por una empresa legítima o una persona de confianza.*

Procesamiento de datos: *tratamiento electrónico de datos o de los elementos básicos de información, sometidos a operaciones programadas.*

Proveedor de servicios: *entidad relacionada o no a la institución contratante, que preste servicios o provea bienes e instalaciones a éste.*

Prueba de penetración: *metodología de prueba en la que los evaluadores, que normalmente trabajan bajo restricciones específicas, intentan eludir o derrotar las características de seguridad de un sistema.*

Punto objetivo de recuperación (RPO): *período de tiempo máximo antes que la pérdida de datos que sigue a un incidente se vuelva inaceptable de acuerdo a los estándares de calidad de la propia entidad.*

Red Team (Equipo Rojo): *grupo de personas autorizadas y organizadas para emular las capacidades de ataque o explotación de un adversario potencial contra la postura de seguridad de una empresa. El objetivo del Equipo Rojo es mejorar la ciberseguridad empresarial demostrando los impactos de los ataques exitosos y demostrando lo que funciona para los defensores (es decir, el Equipo Azul) en un entorno operativo.*

Security Operations Center (SOC): *el Centro de Operaciones de Seguridad, SOC (por sus siglas en inglés), se refiere al equipo encargado de garantizar la seguridad de la información. El objetivo del SOC es analizar, identificar y corregir incidentes de seguridad de la información utilizando soluciones tecnológicas y enfoques diferentes.*

Servicios en la nube: *servicios que proveen infraestructura, plataformas o software a lo que el cliente accede a través de la red, sin la necesidad de instalarlos en su propia infraestructura, sino que están ubicados en un servidor remoto del proveedor del servicio.*

Riesgo residual: *aquel riesgo que persiste luego de adoptar las medidas de control y mitigación por parte de la entidad.*

Subcontratación en cadena de servicios externalizados: *las formadas por terceros subcontratados por el proveedor inicial de servicios para realizar parte importante de las actividades contratadas con éste (subcontrato de otros proveedores).*

Tiempos máximos tolerables de interrupción: *tiempo máximo tolerable en que un proceso pudiera estar interrumpido sin provocar efectos relevantes en la continuidad operacional.*

Tiempo objetivo de recuperación: *periodo de tiempo que sigue a un incidente dentro del cual: a) debe reanudarse un producto, servicio o actividad; o b) los recursos deben ser recuperados (entendiendo por recursos los activos, personas, habilidades, información, tecnología, instalaciones, suministros e información necesarios para las operaciones del negocio).*

Vulnerabilidad: *en el contexto de ciberseguridad, se refiere a cualquier debilidad de un activo de información o de un mecanismo de control que pudiera ser explotada por un ataque, es decir, puede ser un fallo en un sistema que lo torna accesible a los atacantes o cualquier tipo de debilidad en el propio activo en los procedimientos que deje la seguridad de la información de la entidad expuesta a una amenaza.*

ANEXO N° 2: REPORTE DE INCIDENTES OPERACIONALES

A través del menú "INCIDENTES Y PÉRDIDAS OPERACIONALES" del canal oficial de comunicación y envío de información entre la Comisión y sus fiscalizados, la entidad deberá reportar el detalle de cada incidente descrito en la sección I.D.1 de acuerdo con el siguiente esquema:

INFORMACION	*DETALLE*
Fecha y hora de inicio del incidente	
Tipo de incidente	
Descripción detallada del incidente	
Causas posibles o identificadas	
Dependencias o activos afectados	
Dirección dependencias afectadas	
Canales afectados	
Nombre de proveedores involucrados	
Tipo de proveedores involucrado	
Número de clientes afectados	
Tipo de clientes afectados	
Productos o servicios afectados	
Número de transacciones afectadas	
Medidas adoptadas y en curso	
Otros antecedentes	
Nombres y cargos de las personas de contacto	
Teléfono de contacto	
Fecha y hora de cierre del incidente	

Para aquellos campos en los que al momento del reporte no se cuente con la información, se debe indicar con texto "En evaluación", y para el caso de los campos numéricos, de no contarse con el dato, éstos deben completarse con un cero.

Será responsabilidad de la entidad la actualización de los antecedentes mencionados cuando se disponga de nueva información y hasta el cierre del incidente (fecha de cierre del incidente).

FECHA Y HORA DEL INICIO DEL INCIDENTE
Se debe señalar la fecha (DD/MM/AAAA) y la hora (HH:MM:SS) en que comenzó el incidente.

TIPO DE INCIDENTE
En este campo se debe señalar el tipo de incidente, eligiendo entre las siguientes opciones:

- *Afectación de instalaciones*
- *Ausencia de Colaboradores*
- *Sin acceso dependencias y otras áreas específicas*
- *Falla Sistemas Base (SO, BD)*
- *Falla aplicativos (negocio, web, batch)*

- *Falla de comunicaciones*
- *Falla Hardware*
- *Falla en servicios básicos (electricidad/agua)*
- *Pérdida de Recursos Monetarios de la entidad, sus clientes y otras partes interesadas*
- *Pérdida de Información de la entidad, sus clientes y otras partes interesadas*
- *Interrupción/ latencia en servicios*
- *Error de envío de información*
- *Otros: especificar*

DESCRIPCIÓN DETALLADA DEL INCIDENTE
En este campo se debe detallar en qué consiste el incidente reportado.

CAUSAS POSIBLES O IDENTIFICADAS
En este campo se debe realizar un análisis sobre las causas del incidente y sobre la efectividad de las medidas adoptadas para resolverlo.

DEPENDENCIAS AFECTADAS
En este campo se deben señalar las dependencias afectadas, eligiendo entre las siguientes opciones:

- *Oficinas*
- *Sitio Producción*
- *Sitio Contingencia*
- *Dependencias proveedor*
- *Otros: especificar*

DIRECCIÓN DEPENDENCIAS AFECTADAS (CALLE, COMUNA, REGIÓN)
En este campo se debe informar la dirección completa de la dependencia afectada. Si existe más de una dependencia afectada, se debe indicar la dirección de cada una de ellas, separándolas con un punto y coma (;).

CANALES AFECTADOS
En este campo se deben seleccionar los canales afectados por el incidente (lo que sea aplicable):

- *Terminales*
- *Mensajería*
- *Servicios de custodia*
- *Sucursales*
- *Otros: especificar*

NOMBRE DE PROVEEDORES INVOLUCRADOS
Corresponde al nombre o razón social del proveedor.

TIPO DE PROVEEDOR INVOLUCRADO

- *Servicios básicos*
- *Telecomunicaciones*
- *Infraestructura tecnológica*
- *Procesamiento*
- *Atención telefónica*
- *Otros: especificar*

NÚMERO DE CLIENTES AFECTADOS:

En este campo se debe completar el número de clientes que fueron afectados por el incidente que se reporta.

TIPO DE CLIENTES AFECTADOS:
En este campo se debe seleccionar el tipo de cliente afectado, entre las siguientes opciones:

- *Personas*
- *Empresas no financieras*
- *Empresas financieras (Especificar)*
-
- *Otros: Especificar*

NÚMERO DE EMPLEADOS AFECTADOS
En este campo se debe completar con el número de empleados que fueron afectados por el incidente que se reporta.

PRODUCTOS O SERVICIOS AFECTADOS
En este campo se deben informar en detalle los productos o servicios afectados por el incidente.

NÚMERO DE TRANSACCIONES AFECTADAS
En este campo se debe completar el número de transacciones que fueron afectadas por el incidente que se reporta (en caso de no conocer el número exacto de transacciones afectadas, se debe completar con 0; luego, en la medida que se tenga más información, se debe actualizar la cifra).

MEDIDAS ADOPTADAS
En este campo se deben informar en detalle las acciones realizadas por la entidad para superar el incidente.

NOMBRE Y CARGO DE PERSONAS DE CONTACTO
Corresponden a las personas que informan el incidente y sus cargos.

TELÉFONO DE CONTACTO
Se debe señalar en este campo el teléfono celular de las personas de contacto.

FECHA Y HORA DE TÉRMINO DEL INCIDENTE
Este campo se incluirá cuando se cierra el incidente. Se debe completar la fecha (DD/MM/AAAA) y la hora (HH:MM:SS) en que éste finalizó.

ANEXO N° 3: REPORTE DE PÉRDIDAS OPERACIONALES

A través del menú "INCIDENTES Y PERDIDAS OPERACIONALES" del canal oficial de comunicación y envío de información entre la Comisión y sus fiscalizados, la entidad deberá reportar al último día hábil de junio y diciembre de cada año el detalle de todos los eventos que materialicen individualmente en pérdidas operacionales mayores a 150 Unidades de Fomento. Además, se deberán reportar los montos de gastos y recuperaciones asociados a pérdidas operacionales asociados a un mismo evento.

INFORMACION	*DETALLE*
Número de identificación del incidente asignado por la CMF	
Fecha de descubrimiento	
Fecha de contabilización	
Tipo de monto	
Tipo de gasto	
Tipo de recuperación	
Monto	
Nombre y cargo del informante	

NUMERO DE IDENTIFICACIÓN DEL INCIDENTE ASIGNADO POR LA CMF
Corresponde al código que identifica en forma unívoca el incidente reportado, asignado por la CMF cuando se reportó el inicio del incidente a través del menú "INCIDENTES Y PÉRDIDAS OPERACIONALES" del canal oficial de comunicación y envío de información entre la Comisión y sus fiscalizados.

FECHA DE DESCUBRIMIENTO
Seleccionar el día y hora que se desplegará en este campo correspondiente a la fecha en la que se identificó el evento de pérdida.

FECHA DE CONTABILIZACIÓN
Seleccionar el día y hora que se desplegará en este campo correspondiente a la fecha en la que se imputa contablemente la pérdida o recupero en los estados financieros.

TIPO DE MONTO
Seleccionar el código que identifica el tipo de monto a reportar, de acuerdo a la siguiente codificación que se desplegará en este campo:

CODIGO	*TIPO DE MONTO*
1	*Pérdida (cargos directos en los estados de resultados)*
2	*Gastos (costos incurridos internos o externos con relación directa al evento operacional)*
3	*Recuperación*

TIPO DE GASTO
Seleccionar el código que identifica el principal tipo de gasto asociado al evento de pérdida, ya sea interno o externo directamente atribuible al evento operacional, de acuerdo a la siguiente codificación que se desplegará en este campo:

CODIGO	*TIPO DE GASTO*
1	*Legales*
2	*Proveedores*
3	*Asesorías*
4	*Internos*
5	*Otros*
9	*No aplica (debe reportarse cuando el campo "TIPO DE MONTO" toma valores 1 o 3)*

TIPO DE RECUPERACIÓN
Seleccione el código asociado a las causas de la recuperación operacional, de acuerdo a la siguiente codificación que se desplegará en este campo:

CODIGO	*TIPO DE RECUPERACIÓN*
1	*Compañías de seguros*
2	*Acciones judiciales*
3	*Otros (liberación de provisión)*
4	*No aplica*

MONTO
Corresponde al monto de las pérdidas, gastos o recuperaciones que deben reportarse en la fecha en la que se contabilicen.

NOMBRE Y CARGO DEL INFORMANTE
Corresponde a la persona que informa el incidente y su cargo.

ANEXO N° 4: DISPOSICIONES ADICIONALES RELATIVAS AL REPORTE DE INCIDENTES PARA SOCIEDADES ADMINISTRADORAS DE SISTEMAS DE COMPENSACIÓN Y LIQUIDACIÓN Y ENTIDADES DE DEPÓSITO Y CUSTODIA DE VALORES

Las Sociedades Administradoras de Sistemas de Compensación y Liquidación de Instrumentos Financieros y las Entidades de Depósito y Custodia a los que se refiere la ley N° 18.876 deberán considerar como parte de los incidentes a reportar definidos en la sección I.D.1:

- *Eventos que provoquen la falta de disponibilidad de uno o más servicios por, al menos, 15 minutos.*
- *Eventos que impliquen la solicitud de una extensión horaria, se haga o no ésta efectiva, al Banco Central de Chile en su calidad de administrador del Sistema de Liquidación Bruta en Tiempo Real.*

Esta Comisión deberá ser informada de toda solicitud de extensión horaria al Banco Central de Chile tan pronto ésta ocurra, y ser incluida como destinatario en el caso de boletines electrónicos u otras comunicaciones a sus depositantes u otras entidades que tengan por objetivo informar acerca de esta materia.

En caso de incidentes que no hayan sido resueltos luego de transcurridos 30 minutos desde su ocurrencia, la entidad afectada deberá comunicar al menos a sus usuarios, a las entidades no afectadas y al Banco Central de Chile esta situación, indicando la siguiente información:

- *Ocurrencia de un incidente.*
- *Tiempo previsto para resolver incidente.*
- *Tiempo de extensión horaria otorgado por el Banco Central de Chile, en caso de haber sido solicitado.*
- *Recomendaciones para los usuarios.*

En el mismo momento, la referida comunicación deberá ser enviada a esta Comisión a través del menú "INCIDENTES Y PERDIDAS OPERACIONALES" del canal oficial de comunicación y envío de información entre la Comisión y sus fiscalizados.

Si el incidente se prolongara por sobre el tiempo previsto para resolverlo, se deberá remitir una nueva comunicación en los mismos términos descritos anteriormente, con la información requerida actualizada y enviar copia de esta comunicación a esta Comisión a través del menú "INCIDENTES Y PERDIDAS OPERACIONALES".

La entidad deberá implementar y ejecutar procedimientos para identificar el problema que originó el incidente y prevenir su ocurrencia futura. Para la fase de identificación del problema deberá documentarse con precisión la metodología a emplear, la cual deberá ser una de amplia utilización en el ámbito de tecnologías de información y comunicación, validada por estándares internacionales en la materia. La información de incidentes y pérdidas operacionales a la que se refiere la sección I.D deberá remitirse al Comité de Riesgos (y al Comité de Vigilancia, cuando corresponda) de las Sociedades Administradoras de Sistemas de Compensación y Liquidación de Instrumentos Financieros y las Entidades de Depósito y Custodia, dentro de los plazos previstos en dicha sección.

V. EVALUACIÓN DE IMPACTO REGULATORIO

La implementación de un adecuado marco de gestión de riesgo operacional obedece, entre otras, a las siguientes razones:

- La rápida evolución de la infraestructura tecnológica en los últimos años (hardware y software) genera obsolescencia de las medidas de seguridad de información de una entidad, haciéndola vulnerable a brechas de seguridad de datos y ataques cibernéticos. Desde la pandemia, los ataques cibernéticos se incrementaron considerablemente: se estima que el malware creció 358% y el ramsomware, 435% a nivel mundial en 2020, con un impacto potencial significativo en entidades de menor tamaño[5]. También los ataques cibernéticos crecieron un 24% en América Latina durante los primeros ocho meses de 2021[6]. En este contexto, los efectos de un incidente operacional local o internacional podrían transmitirse rápidamente entre entidades del sector financiero en forma sistémica.
- La transición hacia la automatización de tareas, el procesamiento de datos en servidores y nube y las modalidades de trabajo remoto incrementan los riesgos derivados de un incidente operacional, planteando la necesidad de establecer lineamientos regulatorios para la actualización periódica de los planes de continuidad de negocio y respuesta ante incidentes de las entidades fiscalizadas.
- La externalización de servicios en la nube y otros de estas entidades requieren una adecuada política de contratación y monitoreo de proveedores que esté acorde con las políticas de seguridad de la información y ciberseguridad, y los planes de continuidad y respuesta a incidentes.
- La aparición de nuevos servicios financieros que utilizan la tecnología, contemplados en la reciente Ley N° 21.521 (Ley Fintec), lo cual requiere tener la capacidad operacional para soportar el procesamiento de las transacciones que se realice mediante los sistemas o infraestructura de las entidades.

Al respecto, se observa que los fiscalizados han ido internalizando previamente los costos de incorporar formalmente la gestión de riesgo operacional:

- La Norma de Carácter General N° 480[7] establece la obligatoriedad de que las Bolsas de Valores tengan una unidad de dedicación exclusiva, destinada a la función de Gestión de Riesgos, y otra unidad, también de dedicación exclusiva, destinada a la función de Auditoría Interna de Riesgos). Dentro de los riesgos que deben gestionar, se encuentra la gestión de riesgo operacional.
- La Circular N° 1939 establece la obligatoriedad de que las Sociedades Administradoras de Sistemas de Compensación y Liquidación (SCLI) y Entidades de Depósito Central de Valores (DCV) tengan una unidad de evaluación "permanente e independiente" de la gestión de riesgo operacional, así como matrices de riesgo operacional.
- La Bolsa de Valores de Santiago cuenta con certificación de normas ISO de gestión de riesgo operacional.
- La Bolsa de Productos en su reglamento general establece que el sistema de transacciones, en los planes de trabajo que se elaboren, deberá considerar respecto de

[5] Global Risks Report (World Economic Forum, 2022)
[6] Panorama de Amenazas de América Latina (Kaspersky, 2021)
[7] NCG N° 480 (CMF, 2022)

sus corredores, la evaluación y seguimiento de los sistemas de control interno para riesgo operacional.
- Las AGF (Circular N° 1869) ya cuenta con funciones de gestión de riesgos y auditoría interna, que deben velar por la gestión del riesgo operacional.

La propuesta normativa establece requisitos destinados a garantizar la gestión de riesgo operacional en los ámbitos de seguridad de la información, continuidad del negocio y externalización de servicios, atendido el volumen y complejidad de las operaciones de cada entidad, el tipo de negocio que desarrolla y el impacto sistémico que una interrupción de sus operaciones pudiera tener en el mercado financiero local e internacional.

Asimismo, la propuesta requiere que todas las entidades lleven dos registros: Incidentes Operacionales y Pérdidas Operacionales. No obstante, dichas funciones podrán ser desempeñadas por una persona que ya forma parte del staff de tecnologías de información de la entidad, siempre que posea los conocimientos y experiencia adecuados.

Dentro de los beneficios de la propuesta destacamos los siguientes:

- La prevención y monitoreo de incidentes operacionales evitaría brechas de seguridad de la información que podrían significar un perjuicio económico para la entidad y sus clientes producto de delitos informáticos que deriven en una pérdida de información o recursos y pudieran afectar la viabilidad financiera de la entidad en el mediano plazo.
- La reanudación temprana de las operaciones de la entidad ante incidentes fortalecería la confianza de los clientes, mitigando el riesgo reputacional. Lo anterior se traduciría en indicadores de liquidez, rentabilidad, solvencia y cobertura financiera más robustos. Asimismo, permitiría mitigar el riesgo legal derivado de incidentes que pudieran afectar la integridad y exactitud de la información que maneja la entidad para fines de cumplimiento regulatorio.
- Un marco regulatorio integrado para la gestión de riesgos operacionales a nivel de industria permitiría reconocer externalidades positivas derivadas de la gestión coordinada de fallas operacionales o filtraciones de datos que tengan el potencial de generar riesgos de contagio en todo el sistema financiero.
- La implementación de un registro y análisis de incidentes operacionales contribuiría al establecimiento de controles mitigantes de riesgo operacional.

Por último, en relación a la propia CMF, la propuesta:

- Permitiría un fortalecimiento de la supervisión de la gestión de riesgo operacional de estas entidades y una mejor focalización de los recursos del Supervisor al homogeneizar los requerimientos de gestión de riesgos entre diferentes industrias, en línea con el marco de Supervisión Basada en Riesgos de la CMF.
- Adecuaría la regulación local a los estándares internacionales de gestión de riesgo operacional.
- Tendría costos adicionales de supervisión, destacándose el incremento en horas-hombre destinadas al monitoreo del cumplimiento de los planes de acción anuales comprometidos por las entidades para mitigar sus riesgos (aunque en el caso de Administradoras Generales de Fondos ya se supervisan dichos planes).
- Implica que la CMF deberá destinar recursos para poder diseñar e implementar el sistema informático que permita que las entidades puedan reportar sus incidentes y pérdidas operacionales.

ANEXO A: PRINCIPIOS Y RECOMENDACIONES INTERNACIONALES

Comité de Basilea sobre Supervisión Bancaria

Se destaca la emisión de los Principios de Continuidad de Negocio, los Principios de Manejo de Riesgo Operacional y los Principios de Resiliencia Operacional.

Principios de Continuidad del Negocio (2006)

Principio 1: Los participantes de la industria financiera y las autoridades financieras deben contar con enfoques integrales para la gestión de la continuidad del negocio. El Directorio y la Alta Administración son responsables en conjunto de la continuidad de negocio de la organización.

Principio 2: Los participantes de la industria financiera y las autoridades financieras deben incorporar el riesgo de una interrupción operativa importante en sus enfoques para la gestión de la continuidad del negocio. La gestión de la continuidad del negocio de la Alta Administración debe abordar cómo responder a una interrupción operativa importante que afecte las operaciones de los participantes de la industria financiera o del sistema financiero en su área de influencia.

Principio 3: Los participantes de la industria financiera deben desarrollar objetivos de recuperación que reflejen el riesgo que dichos participantes representan para el funcionamiento del sistema financiero. Según corresponda, dichos objetivos pueden ser establecidos en consulta con las autoridades financieras pertinentes.

Principio 4: Los participantes de la industria financiera y las autoridades financieras deben incluir en sus planes de continuidad del negocio procedimientos para comunicarse en su organización y con otras organizaciones externas en caso dentro de una interrupción operativa importante.

Principio 5: Los procedimientos de comunicación de los participantes de la industria financiera y las autoridades financieras debe abordar las comunicaciones con las autoridades financieras de otras jurisdicciones en el caso de una interrupción operativa importante con implicaciones transfronterizas.

Principio 6: Los participantes de la industria financiera y las autoridades financieras deben testear sus planes de continuidad de negocio, evaluarlos y actualizarlos según corresponda.

Principio 7: Las autoridades financieras deben incorporar revisiones de la gestión de la continuidad del negocio en sus marcos para la evaluación continua de los participantes de la industria financiera bajo su supervisión.

Principios de Manejo de Riesgo Operacional (2021)

Principio 1: El Directorio debe liderar el establecimiento de una sólida cultura de gestión de riesgos, implementada por la Alta Administración. El Directorio y la Alta Administración deben establecer una cultura corporativa guiada por una sólida gestión de riesgos, establecer estándares e incentivos para profesionales y comportamiento responsable, y garantizar que el personal reciba una formación adecuada en gestión de riesgos y ética.

Principio 2: Los bancos deben desarrollar, implementar y mantener un marco de gestión de riesgos operacionales que esté completamente integrado en los procesos generales de gestión de riesgos del banco. El sistema de manejo de riesgo operacional adoptado por un banco

individual dependerá de una serie de factores, incluidos la naturaleza, el tamaño, la complejidad y el perfil de riesgo del banco.

Principio 3: El Directorio debe aprobar y revisar periódicamente el marco de gestión del riesgo operacional, y asegurarse de que la Alta Administración implemente las políticas, procesos y sistemas del marco de gestión del riesgo operacional de manera efectiva en todos los niveles de decisión.

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

Principio 5: La Alta Administración debe desarrollar para la aprobación del Directorio una estructura de gobierno clara, eficaz y sólida con líneas de responsabilidad bien definidas, transparentes y coherentes. La Alta Administración 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 importantes del banco de acuerdo con la declaración de tolerancia y apetito por el riesgo del banco.

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

Principio 7: La Alta Administración debe asegurarse de que el proceso de gestión del cambio del banco sea integral, cuente con los recursos adecuados y esté adecuadamente articulado entre las líneas de defensa pertinentes.

Principio 8: La Alta Administración debe implementar un proceso para monitorear regularmente los perfiles de riesgo operacional y las exposiciones operativas materiales. Deben existir mecanismos de información adecuados a nivel del Directorio, la Alta Administración y las unidades de negocio para respaldar la gestión proactiva del riesgo operacional.

Principio 9: Los bancos deben 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.

Principio 10: Los bancos deben implementar un programa sólido de gestión de riesgos alineado con su marco de gestión de riesgos operacionales.

Principio 11: Los bancos deben contar con planes de continuidad del negocio para garantizar su capacidad de operar de forma continua y limitar las pérdidas en caso de una interrupción grave del negocio. Los planes de continuidad del negocio deben estar vinculados al marco de gestión del riesgo operacional del banco.

Principio 12: Las comunicaciones públicas de información de un banco deben permitir que las partes interesadas evalúen su enfoque para la gestión y el grado de exposición al riesgo operacional.

Principios de Resiliencia Operacional (2021)

Principio 1: Los bancos deben utilizar su estructura de gobierno existente para establecer, supervisar e implementar un enfoque de resiliencia operacional eficaz que les permitan responder y adaptarse, así como recuperarse y aprender de los eventos disruptivos para minimizar su impacto en la entrega de operaciones críticas en caso de interrupción.

Principio 2: Los bancos deben aprovechar sus respectivas funciones de gestión del riesgo operacional para identificar de forma continua amenazas externas e internas, y fallas potenciales en personas, procesos y sistemas.

Principio 3: Los bancos deben contar con planes de continuidad del negocio y realizar ejercicios de continuidad del negocio en una variedad de escenarios severos pero plausibles para probar su capacidad para entregar operaciones críticas en caso de interrupción.

Principio 4: Una vez que un banco ha identificado sus operaciones críticas, debe mapear las interconexiones e interdependencias internas y externas que son necesarias para la entrega de operaciones críticas consistentes con su enfoque de resiliencia operativa.

Principio 5: Los bancos deben administrar sus dependencias en las relaciones, incluidas las de terceros o entidades de su grupo empresarial, para la entrega de operaciones críticas.

Principio 6: Los bancos deben desarrollar e implementar planes de respuesta y recuperación para gestionar incidentes que puedan interrumpir la entrega de operaciones críticas en línea con el apetito de riesgo del banco y la tolerancia a la interrupción. Asimismo, deben mejorar continuamente sus planes de recuperación y respuesta a incidentes incorporando las lecciones aprendidas de incidentes anteriores.

Principio 7: Los bancos deben garantizar Sistemas de Información, Comunicación y Tecnología resilientes, incluida la seguridad cibernética, que esté sujeta a programas de protección, detección, respuesta y recuperación que se prueben regularmente, incorporen una cultura de riesgos adecuada y transmitan información oportuna para la gestión de riesgos y los procesos de toma de decisiones en las operaciones críticas del banco.

Autoridad Europea de Bancos

Se destaca la emisión de las guías: Guía para el manejo de Riesgos Operacionales en actividades de mercado; Guía de Gestión de Riesgos de Seguridad en Sistemas de Información, Comunicación y Tecnología; y Guía de Acuerdos de Subcontratación.

Guía para el manejo de Riesgos Operacionales en actividades de mercado (2010)

Principio 1: La Alta Administración debe ser consciente de los riesgos operacionales, reales o potenciales, que afecten a las actividades de mercado. Debe desarrollar y mantener una estructura organizativa, controles internos y un sistema de información adecuados para la identificación, evaluación, control y seguimiento de los riesgos operacionales en las actividades de mercado.

Principio 2: La Alta Administración debe promover, en particular en el front office, una cultura diseñada para mitigar los riesgos operacionales en las actividades de mercado.

Principio 3: El Directorio debe asegurarse de que ellos y el personal en las funciones de control tengan la comprensión, la habilidad, la autoridad y el incentivo apropiados para desafiar de manera efectiva las actividades de los comerciantes.

Principio 4: El riesgo operacional debe tenerse en cuenta al establecer objetivos y evaluar el desempeño de una persona o unidad de negocios en actividades de mercado.

Principio 5: El comportamiento proactivo frente a acciones fraudulentas en actividades de mercado debe ser un elemento clave de los sistemas de control interno y de información.

Principio 6: Los traders deben iniciar transacciones solo cuando cumplan con sus términos de referencia establecidos. Se deben seguir estándares mínimos para el inicio y conclusión de transacciones.

Principio 7: Los requisitos de documentación para las actividades comerciales deben estar adecuadamente definidos. Deben minimizarse las incertidumbres jurídicas, de manera que los contratos sean exigibles en la medida de lo posible.

Principio 8: Como regla general, las operaciones deberán iniciarse y concluirse en la sala de operaciones y durante el horario de operaciones.

Principio 9: Cada posición y flujo de efectivo asociado con una transacción debe registrarse claramente en el sistema contable de la institución, con un rastro de auditoría documentado.

Principio 10: Las instituciones deben asegurarse de contar con un marco adecuado de controles sobre las relaciones entre los traders y sus contrapartes del mercado.

Principio 11: Los procesos de confirmación, liquidación y conciliación deben diseñarse y ejecutarse adecuadamente.

Principio 12: Las instituciones deben asegurarse de que sus procesos de marginación funcionen correctamente y que cualquier cambio se concilie con las posiciones relevantes en sus libros.

Principio 13: Las fuentes de riesgos operacionales en las actividades de mercado deben identificarse y monitorearse adecuadamente con el nivel apropiado de escrutinio, intensidad y oportunidad.

Principio 14: El valor nominal de las transacciones/posiciones debe mantenerse bajo estricto control para el seguimiento de los riesgos operacionales y de contraparte, mediante la definición de los límites pertinentes y/o la participación en iniciativas de novación de contratos.

Principio 15: Los sistemas de información en el área de negociación deben diseñarse, implementarse y mantenerse adecuadamente para garantizar un alto nivel de protección en las actividades de mercado.

Principio 16: El sistema de reporte de riesgo operacional para actividades de mercado debe estar diseñado para generar alertas adecuadas y debe alertar a la gerencia cuando se detecten operaciones sospechosas o incidentes materiales.

Principio 17: Las entidades deberán velar por la calidad y consistencia de sus informes internos y que sean adecuados a las necesidades de los destinatarios a los que están destinados.

Guía de gestión de Riesgos de Seguridad en Sistemas de Información, Comunicación y Tecnología (2019)

Establece recomendaciones relativas a la gestión de Riesgos de Seguridad en Tecnologías de Información y Comunicación (TIC):

- Proporcionalidad: Las políticas de gestión de riesgo de TIC deben implementarse acorde con el tamaño de la institución financiera, su organización interna y la naturaleza y complejidad de sus actividades.
- Gobernanza: La Alta Administración debe establecer funciones y responsabilidades claras para la gestión de riesgos de seguridad de la información y la continuidad del negocio. Debe garantizar que todo el personal reciba la capacitación adecuada en riesgos de TIC.
- Contratos con proveedores: Deben incluir los requisitos mínimos de ciberseguridad; especificaciones del ciclo de vida de los activos de información; cifrado de datos, seguridad de red y ubicación de los datos competidos; procedimientos de gestión de incidentes, incluidos el escalamiento y la notificación.

- Administración de riesgos de TIC: Asignada a una función separada de los procesos operativos de TIC, que responda directamente a la Alta Administración y que no realice labores de auditoría.
- Función de auditoría interna: Asignada a una función separada de los procesos operativos de TIC, debe revisar el cumplimiento de las políticas y procedimientos de gestión de riesgos de TIC. Los planes de auditoría deben ser aprobados por la Alta Administración.
- Marco de Gestión de Riesgos de Seguridad de la Información: Las entidades deben asignar roles, responsabilidades y líneas de reporte que garanticen la efectividad del marco de gestión de riesgos de TIC. Este marco debe estar alineado con la política comercial, el apetito por riesgo y el diseño de controles, y revisado por la Alta Administración al menos una vez al año.
- Política de Seguridad de la Información: Las entidades deben desarrollar y documentar una Política de Seguridad de la Información que incluya una descripción de las principales funciones y responsabilidades y los requisitos del personal a cargo. Dicha política debe identificar y clasificar las funciones comerciales, los activos de información y los procesos de soporte en base a consideraciones de confidencialidad, integridad y disponibilidad de los datos y el monitoreo continuo de posibles vulnerabilidades. La evaluación de riesgos de seguridad de información debe ser comunicada a la Alta Administración de manera clara y oportuna.

Seguridad lógica:

- Definir, documentar e implementar procedimientos para el control de acceso lógico (gestión de identidad y acceso).
- Usuarios deben tener derechos de acceso mínimos estrictamente necesarios para ejecutar sus funciones (principio de privilegio mínimo) y para evitar el acceso injustificado a un gran conjunto de datos (principio de segregación de funciones). Se deben registrar y monitorear las actividades de usuarios con privilegios de administrador.
- Los derechos de acceso a activos de información deben ser otorgados o retirados de manera oportuna y en función de los procesos comerciales de la entidad.
- Monitoreo de la Seguridad de la Información y del Sistema TIC: Las entidades deben contar con procedimientos aprobados por la Alta Administración para el monitoreo de riesgos de TIC, incluyendo:
    - Procedimientos de registro y monitoreo de operaciones críticas de TIC para la detección de actividades anómalas que puedan afectar la seguridad de la información y brechas de seguridad. Por ejemplo, fugas de información, códigos maliciosos y otras vulnerabilidades. En estos casos debe estar contemplada una actualización periódica de software y hardware, incluyendo parches de seguridad.
    - Inventario actualizado de activos de TIC para garantizar que continúen respaldando los requisitos comerciales y de gestión de riesgos.
    - Sistemas de segmentación de red, prevención de pérdida de datos y encriptación del tráfico de red, acorde con la clasificación de activos de información realizada por la entidad.
    - Estándares de seguridad predefinidos antes de otorgar el acceso a la red corporativa, a los servidores y a las estaciones de trabajo (idealmente con cifrado de datos de extremo a extremo).
    - Procedimientos de seguridad física de las instalaciones.
    - Realización de pruebas de seguridad, incluyendo revisión de código fuente y pruebas de penetración. Estas pruebas deben realizarse periódicamente por personal independiente y con experiencia. Para servicios críticos, se recomienda que sean al

menos una vez por año, y para servicios no críticos al menos cada 3 años. Los resultados de las pruebas deben informarse a la Alta Administración.

- Procedimientos de respaldo de datos: Las entidades deben definir e implementar procedimientos de respaldo y restauración de datos y sistemas de TIC. Las copias de seguridad deben almacenarse de forma segura y lo suficientemente alejadas del sitio principal.
- Manejo de incidentes: Las entidades deben establecer una política de gestión de incidentes con los siguientes elementos:
  - Identificación, registro y clasificación de incidentes con base en la criticidad de los procesos del negocio.
  - Roles y responsabilidades para diferentes escenarios de incidentes.
  - Procedimientos de análisis de causas de incidentes.
  - Planes de comunicación interna, incluidos los procedimientos de notificación y escalamiento de incidentes a la Alta Administración y a las partes interesadas.

- Análisis de Impacto del Negocio (BIA) y Plan de Continuidad del Negocio (BCP):
  - El BIA debe considerar la criticidad de las funciones comerciales, los procesos de soporte, los activos de información y sus interdependencias.
  - Las entidades deben establecer un Plan de Continuidad del Negocio aprobado por la Alta Administración. Estos planes deben proteger la confidencialidad, integridad y disponibilidad de las funciones comerciales, procesos de soporte y activos de información.
  - Las entidades deben coordinarse con las partes interesadas para garantizar que puedan reaccionar adecuadamente ante posibles escenarios de interrupción y poder recuperar las operaciones comerciales críticas dentro de un objetivo de tiempo de recuperación (RTO, el tiempo máximo dentro del cual un sistema o proceso debe ser restaurado después de un incidente) y un objetivo de punto de recuperación (RPO, el período de tiempo máximo durante el cual es aceptable que se pierdan datos en caso de un incidente).
  - El BCP debe incluir un conjunto adecuado de escenarios severos pero plausibles sobre cambios en funciones comerciales críticas, procesos de soporte y activos de información.

- Planes de Respuesta y Recuperación: Sobre la base de los BIA, las entidades deben desarrollar planes de respuesta y recuperación que deben centrarse en la recuperación de las operaciones de las funciones comerciales críticas, los procesos de apoyo, los activos de información y sus interdependencias con terceros. Estos planes deben actualizarse en función de los incidentes pasados y las pruebas realizadas.

Guía de Acuerdos de Subcontratación (2019)

Establece lineamientos generales para el desarrollo de acuerdos de externalización de servicios con proveedores:

<u>Alta Administración</u>

La Alta Administración es responsable de:

- Asignar claramente las responsabilidades y recursos para la documentación, gestión y control de los riesgos asociados a los acuerdos de subcontratación.

- Establecer una función de externalización o designar a un miembro de la Alta Administración que sea responsable de supervisar los riesgos de los acuerdos de externalización.
- Establecer políticas para el manejo de posibles conflictos de interés.

Proporcionalidad

Las entidades pequeñas y con tareas menos complejas deben garantizar al menos una división clara de tareas y responsabilidades para la gestión de riesgos de subcontratación, pudiendo asignar la función de externalización a un miembro de la Alta Administración.

Qué no debería considerarse como parte de una política de externalización

- Auditoría legal.
- Servicios de información de mercado.
- Infraestructuras de pagos globales.
- Acuerdos de compensación y liquidación entre Cámaras de Compensación y Contrapartes Centrales.
- Infraestructuras de mensajería financiera global.

Qué debería considerarse como una función subcontratada crítica

- Aquella cuya interrupción perjudique seriamente la resiliencia operacional, la continuidad del negocio, la viabilidad financiera de la entidad y/o afecte de manera importante a sus clientes o perjudique su reputación a largo plazo.
- Aquella relacionada con procesos comerciales complejos o importantes.
- Aquella que no pueda transferirse rápidamente a otro proveedor de servicios, considerando los costos y el tiempo para hacerlo.
- Aquella cuya interrupción tenga impacto potencial en la confidencialidad e integridad de los datos entregados al proveedor.

Política de externalización

La política debiera incluir al menos lo siguiente:

- Responsabilidades de la Alta Administración.
- Responsabilidad de las áreas comerciales.
- Identificación de funciones críticas y gestión de los riesgos asociados.
- Verificaciones de diligencia debida sobre proveedores de servicios
- Capacidad de supervisión continua sobre proveedores contratados.
- Manejo de posibles conflictos de interés (ej. proveedor que forme parte del grupo empresarial de la entidad).
- Planes apropiados de continuidad del negocio con respecto a las funciones críticas subcontratadas, teniendo en cuenta el posible evento de que la calidad de la prestación de la función crítica se deteriore a un nivel inaceptable o falle; el impacto potencial de la insolvencia financiera de un proveedor; o los riesgos políticos en la jurisdicción en que éste opera.
- Procedimientos para ser notificado y responder ante los cambios en un acuerdo de subcontratación o en la situación financiera de un proveedor.
- Auditoría independiente del cumplimiento de las políticas de gestión de riesgo operacional de la función subcontratada.
- Mantenimiento de un Registro de Subcontratación.

- Estrategia en caso de término de contrato con un proveedor, con un plan de salida documentado para cada función crítica subcontratada.

Contratación de proveedores

Previo a cualquier acuerdo de subcontratación, las entidades deben:

- Evaluar si el acuerdo de externalización se refiere a una función crítica o importante.
- Evaluar si se cumplen las condiciones de supervisión para la subcontratación.
- Identificar y evaluar todos los riesgos relevantes del acuerdo de subcontratación, incluyendo:
  - Riesgos de concentración de la función subcontratada en un proveedor no fácilmente sustituible.
  - Riesgo de intervención, la posibilidad de que se tenga que prestar apoyo financiero al proveedor y hacerse cargo de la función subcontratada.
  - Riesgos legales, regulatorios y reputacionales.
  - Riesgos derivados de que el proveedor subcontrate a su vez la función, reduciendo la capacidad de la entidad de supervisar la función subcontratada.

- Llevar a cabo la debida diligencia sobre los posibles proveedores de servicios. En este sentido, la entidad debe asegurarse que tenga la reputación comercial, la experiencia y los recursos suficientes para prestar la función. Asimismo, debe considerar su actual situación financiera, su estructura de grupo empresarial y si está supervisado por las autoridades competentes.
- Existencia de acuerdos de confidencialidad apropiados con respecto a los datos, considerando las consecuencias de la ubicación geográfica del proveedor (por ej., la posibilidad que las autoridades competentes puedan acceder a documentación de la función subcontratada en terceros países).
- Posibilidad de transferir la función a proveedores de servicios alternativos o a la propia entidad.

El contrato debe contemplar:

- Una descripción clara de la función subcontratada y la fecha de finalización.
- Las obligaciones financieras de las partes.
- La ubicación geográfica donde se proporcionará la función crítica subcontratada.
- Disposiciones relativas a la disponibilidad, integridad, privacidad y seguridad de los datos, incluyendo el derecho de la entidad y las autoridades a auditar al proveedor con respecto a la función crítica subcontratada.
- Las obligaciones de información del proveedor para con la entidad, incluida la comunicación de cualquier acontecimiento que pueda tener un impacto material en la capacidad para llevar a cabo la función crítica.
- La posibilidad de que el proveedor a su vez subcontrate la función. Si éste fuera el caso, la entidad debe tener los mismos derechos contractuales de auditoría que los concedidos por el proveedor del servicio.
- Las causales de término de la relación contractual, por ej. cuando haya cambios materiales que afecten la calidad del servicio provisto, la adecuada gestión de la confidencialidad de los datos o la situación financiera del proveedor. En este caso el contrato debe contemplar un período de transición apropiado, durante el cual el proveedor continúe brindando la función subcontratada.

Supervisión de la función subcontratada

La entidad debe garantizar que el proveedor cumpla con los estándares de desempeño y calidad apropiados, para lo cual debe:

- Evaluar el desempeño del proveedor a través de herramientas tales como indicadores de desempeño, informes de prestación de servicios, auto certificación y revisiones independientes.
- Definir los niveles inaceptables de indicadores que deberían desencadenar el término anticipado de la relación.
- Implementar planes de salida que sean integrales, documentados y suficientemente probados mediante un análisis de costos de recursos y tiempo necesarios para transferir el servicio a un proveedor alternativo.

Registro de Subcontratación

Las entidades deben mantener un registro actualizado de todos los acuerdos de externalización, distinguiendo entre la subcontratación de funciones críticas y otras. El registro debe incluir al menos la siguiente información:

- La fecha de inicio, renovación o finalización del contrato.
- Una breve descripción de la función subcontratada, incluidos los datos que se subcontratan. Asimismo, una justificación de porqué se considera una función crítica o no.
- El país donde se realizará el servicio y la ubicación geográfica de los datos.
- En el caso de la subcontratación de servicios en la nube, los modelos de implementación (público, privado, mixto).
- En el caso de la subcontratación de funciones críticas, cuáles son las entidades que hacen uso del servicio externalizado; si el proveedor es parte del grupo empresarial de la entidad; una evaluación de riesgos del servicio provisto; las fechas de las auditorías programadas del servicio; las entidades a las que el proveedor subcontratará a su vez todo el servicio o parte de éste, indicando la ubicación geográfica de los datos respectivos; una calificación cualitativa de la posibilidad de reemplazar al proveedor (fácil, difícil, imposible).

Group of Seven

Se destaca la emisión de Elementos fundamentales de Ciberseguridad para el Sector Financiero.

Fundamental elements of Cybersecurity for the Financial Sector (2016)

Elemento 1: Estrategia y Marco de Ciberseguridad

Establecer un marco de seguridad cibernética adaptado a riesgos cibernéticos específicos y bajo estándares internacionales, locales y de la industria.

Elemento 2: Gobernanza

Definir y facilitar el desempeño de funciones y responsabilidades del personal que implementa o supervisa el marco de seguridad cibernética; proporcionar los recursos adecuados y el acceso a la Alta Administración o la autoridad regulatoria.

Elemento 3: Evaluación de riesgos y controles

Identificar funciones, actividades, productos y servicios, incluidas interconexiones, dependencias y terceros, priorizar su importancia relativa y evaluar los respectivos riesgos cibernéticos. Identificar e implementar controles, incluidos sistemas, políticas, procedimientos y capacitación, para proteger y administrar esos riesgos dentro del nivel de tolerancia establecido por el Directorio.

Elemento 4: Monitoreo

Establecer procesos de monitoreo sistemáticos para detectar rápidamente incidentes cibernéticos y evaluar periódicamente la efectividad de los controles, incluso a través del monitoreo, las pruebas, las auditorías y los ejercicios de red.

Elemento 5: Respuesta oportuna

- Evaluar la naturaleza, el alcance y el impacto de un incidente cibernético.
- Solucionar el incidente y mitigar su impacto.
- Notificar a las partes interesadas internas y externas (los reguladores, accionistas, proveedores de servicios y clientes, según corresponda).
- Coordinar las actividades de respuesta conjunta según sea necesario.

Elemento 6: Recuperación

- Reanudar las operaciones de manera responsable.
- Restaurar sistemas y datos a la normalidad y confirmar dicho estado.
- Identificar y mitigar todas las vulnerabilidades que fueron explotadas.
- Remediar vulnerabilidades para prevenir incidentes similares.
- Comunicarse apropiadamente con las partes interesadas.

Elemento 7: Intercambio de información

Participar en el intercambio oportuno de información de seguridad cibernética con partes interesada (autoridades, otras entidades, clientes) sobre amenazas, vulnerabilidades, incidentes y respuestas para limitar el impacto potencial de futuros incidentes, aumentar la conciencia situacional y ampliar el aprendizaje.

Elemento 8: Aprendizaje Continuo

Revisar el marco de seguridad cibernética regularmente y cuando los eventos lo justifiquen, incluidos sus componentes de gobernanza, evaluación de riesgos y control, monitoreo, respuesta, recuperación e intercambio de información, para asignar recursos, identificar y remediar brechas e incorporar lecciones.

International Organisation of Securities Commissions

Se destacan los Mecanismos para el Manejo de Riesgos de Transacciones Electrónicas y Planes de Continuidad de Negocio de Bolsas; Planes de Continuidad de Negocio y Recuperación de Intermediarios; los Principios de Subcontratación; y la Resiliencia Operacional de Bolsas e Intermediarios durante el Covid-19.

Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business Continuity (2015)

IOSCO identifica algunos riesgos asociados al Plan de Continuidad de Negocios en el caso de Bolsas de Valores:

- Mal funcionamiento de TI y fallas del sistema/red: Esto puede incluir una falla de hardware o software que afecte las transacciones, el flujo de mensajes entrantes y salientes, los sistemas de transmisión de datos y las redes de conectividad, incluyendo proveedores de servicios.
- Ataques cibernéticos.
- Riesgo legal y reputacional de fallas o interrupciones prolongadas en los sistemas.
- Riesgos de liquidez derivados de la interrupción de transacciones, cuando éstas se trasladan a otras Bolsas.
- Riesgos relacionados con la ocurrencia de desastres naturales o terrorismo.

Dentro de los sistemas críticos de una Bolsa, se pueden considerar:

- Sistemas de entrada y ejecución de órdenes, cuya falla impide realizar transacciones
- Sistemas de enrutamiento de pedidos.
- Sistemas de difusión de datos históricos y en tiempo real relacionados con las operaciones, cuya falla impide tomar una decisión informada a los participantes.
- Sistemas de infraestructura de red, gestión de bases de datos, almacenamiento, cortafuegos y conexiones de red.
- Sistemas de vigilancia.
- Sistemas de Gestión de Riesgos para monitoreo de límites y márgenes.

IOSCO recomienda a los reguladores exigir que las Bolsas cuenten con los siguientes mecanismos para garantizar la resiliencia, la confiabilidad y la integridad de los sistemas críticos:

- Implementar pruebas de estrés, controles de aplicaciones, metodologías de desarrollo de sistemas, métricas de desempeño relacionada con la seguridad de los sistemas.
- Que la Alta Administración o el Directorio retengan un rol general de toma de decisiones con respecto a los sistemas críticos.
- Revisar al menos una vez al año los sistemas críticos a través de un auditor interno independiente que informe los resultados a la Alta Administración y notifique a los reguladores, cuando corresponda, de las deficiencias identificadas y las medidas adoptadas para abordarlas.
- Establecer procedimientos de gestión de incidentes con protocolos de comunicación a los clientes y reguladores.

- Monitorear el cumplimiento de las políticas relativas al funcionamiento de la Bolsa, tales como medidas para restringir operaciones frente a movimientos de precios anómalos y controles de entrada, seguimiento y cancelación de transacciones.
- Medidas contra ataques cibernéticos, tales como control de acceso a usuarios, pruebas de penetración y vulnerabilidad, salvaguardas de integridad y almacenamiento de datos, detección de intrusos, cifrado y contraseñas de red.
- Desarrollar un Plan de Continuidad de Negocios que incluya la asignación de recursos adecuados para su actualización y prueba periódica; evaluaciones de impacto de eventuales interrupciones operativas en sistemas críticos; protocolos de comunicaciones y escalamiento de incidentes; mantenimiento de registros; redundancia de software y hardware; obligaciones de proveedores de servicios. El Plan de Continuidad de Negocios debe ser revisado regularmente por el Directorio.

Market Intermediary Business Continuity and Recovery Planning (2015)

Principio 1: Responsabilidad del Directorio y la Alta Administración

Los Intermediarios y las autoridades deben tener enfoques efectivos e integrales para la gestión de la continuidad del negocio. El Directorio y la Alta Administración son colectivamente responsables de la continuidad del negocio de la organización.

Principio 2: Interrupciones operativas importantes

Los Intermediarios y las autoridades deben incorporar el riesgo de una interrupción operativa importante en sus enfoques para la gestión de la continuidad del negocio. La gestión de la continuidad del negocio de las autoridades financieras también debe abordar cómo responderán a una interrupción operativa importante que afecte la operación de los participantes de la industria financiera o el sistema financiero del que son responsables.

Principio 3: Objetivos de recuperación

Los Intermediarios deben desarrollar objetivos de recuperación que reflejen el riesgo que representan para la operación del sistema financiero. Según corresponda, dichos objetivos de recuperación pueden establecerse en consulta con las autoridades financieras pertinentes.

Principio 4: Comunicaciones

Los Intermediarios deben incluir en sus planes de continuidad comercial procedimientos para comunicarse dentro de sus organizaciones y con partes externas relevantes en caso de una interrupción operativa importante.

Principio 5: Comunicaciones transfronterizas

Los procedimientos de comunicación de los Intermediarios y las autoridades deben abordar las comunicaciones con las autoridades financieras en otras jurisdicciones en caso de interrupciones operativas importantes con implicaciones transfronterizas.

Principio 6: Pruebas

Los Intermediarios y las autoridades deben probar sus planes de continuidad comercial, evaluar su eficacia y actualizar la gestión de la continuidad comercial, según corresponda.

Principio 7: Revisiones de la gestión de la continuidad del negocio por parte de las autoridades financieras

Las autoridades deben incorporar revisiones de gestión de la continuidad del negocio en sus marcos para la evaluación continua de los participantes de la industria financiera.

Principles for Outsourcing (2021)

Principio 1: Una entidad regulada debe llevar a cabo procesos de diligencia debida para seleccionar un proveedor de servicios adecuado y monitorear su desempeño en forma continua.

Principio 2: Una entidad regulada debe celebrar un contrato escrito legalmente vinculante con cada proveedor de servicios, cuya naturaleza y detalles deben ser apropiados a la materialidad o criticidad de la tarea subcontratada en el negocio de la entidad regulada.

Principio 3: Una entidad regulada debe tomar las medidas apropiadas para garantizar que tanto la entidad regulada como cualquier proveedor de servicios establezcan procedimientos y controles para proteger la información y el software de su propiedad o propiedad del cliente, y para garantizar la continuidad del servicio, incluyendo un plan de recuperación ante desastres con pruebas periódicas de las instalaciones de respaldo.

Principio 4: Una entidad regulada debe tomar las medidas apropiadas para garantizar que los proveedores de servicios protejan la información confidencial y los datos relacionados con la entidad regulada y sus clientes, de la divulgación no autorizada intencional o involuntaria a terceros.

Principio 5: Una entidad regulada debe ser consciente de los riesgos planteados, y debe gestionarlos de manera efectiva, cuando dependa de un solo proveedor de servicios para tareas subcontratadas importantes o críticas o cuando sea consciente de que un proveedor de servicios proporciona servicios subcontratados importantes o críticos a múltiples entidades reguladas, incluida ella misma.

Principio 6: Una entidad regulada debe tomar las medidas apropiadas para garantizar que su regulador, sus auditores y ella misma puedan obtener rápidamente, previa solicitud, información sobre las tareas subcontratadas que sea relevante para el cumplimiento contractual y/o la supervisión regulatoria, incluida, según sea necesario, acceso a los datos, sistemas informáticos, instalaciones y personal de los proveedores de servicios en relación con las tareas subcontratadas.

Principio 7: Una entidad regulada debe incluir disposiciones escritas relacionadas con la terminación de tareas subcontratadas en su contrato con proveedores de servicios y garantizar que mantiene estrategias de salida adecuadas.

La pandemia de COVID-19 destacó ciertos aspectos de los Principios sobre la subcontratación. En particular, las entidades reguladas deben considerar:

- Con respecto a los Principios 1 y 2, si los proveedores de servicios y las entidades reguladas han identificado sus procesos críticos y tomado medidas para mitigar los riesgos asociados.
- Con respecto al Principio 3, los desafíos que plantea un entorno de trabajo remoto por un mayor uso de tecnología y las crecientes amenazas de ciberseguridad. Asimismo, el desarrollo de pruebas que utilizan escenarios severos pero plausibles con múltiples eventos concurrentes.
- Con respecto a los Principios 3 y 4, evaluar la continuidad y calidad de las tareas provistas por terceros en forma remota. Esto podría incluir el establecimiento de nuevos procedimientos para salvaguardar la seguridad y accesibilidad de la conexión de red remota utilizada por el personal y la realización de nuevas pruebas.
- Con respecto al Principio 5, incrementar la medición y evaluación de la función subcontratada desde una perspectiva de tecnología e infraestructura (por ejemplo, proveedores de servicios en la nube), así como la ubicación física del proveedor de servicios.
- Con respecto al Principio 6, en el caso de un proveedor situado en otro país, la posibilidad de obtener información del servicio subcontratado a través del regulador de dicho país cuando existan dificultades para organizar inspecciones in situ o extra situ.
- Con respecto al Principio 7, la incorporación de estrategias de salida adecuadas.

Operational resilience of trading venues and market intermediaries during the COVID-19 (2022)

La Resiliencia Operativa se refiere a la capacidad de una entidad para realizar operaciones críticas durante una interrupción. Implica incorporar procesos, instalaciones y personal adecuado en el Plan de Continuidad del Negocio.

Para las Bolsas, las operaciones críticas incluyen procesos relacionados con los sistemas de enrutamiento y ejecución de órdenes, la difusión de datos, la infraestructura de red y similares. Para los Intermediarios, las operaciones críticas son más diversas y dependen de la naturaleza de los productos y servicios ofrecidos (ej. un Market Maker vs. un corredor de bolsa minorista).

Los Comités 2 y 3 de IOSCO plantean que los reguladores debieran exigir a las Bolsas e Intermediarios contar con Planes de Continuidad de Negocios que consideren todos los procesos comerciales y las interconexiones entre distintos sistemas para garantizar la resiliencia, confiabilidad e integridad de las operaciones críticas en caso de una interrupción. Estos Planes debieran actualizarse en caso de cualquier cambio importante en variables como la estructura organizacional, el negocio o la ubicación geográfica. Asimismo, debieran revisarse anualmente con la realización de pruebas en distintos escenarios severos.

ANEXO B: MARCO NORMATIVO EXTRANJERO

Australia

El marco general de Gestión de Riesgos viene dado por el estándar AS/NZS 4360:1999, la AS/NZS ISO 31000:2009 y las guías RG 104 ("*Licenciamiento: Obligaciones Generales*") y RG 269 ("*Sistemas de Manejo de riesgos de entidades responsables*") de la Australian Securities and Investment Commission (ASIC), los cuales establecen principios generales para la adecuada identificación, evaluación y mitigación de riesgos para todo tipo de entidades. En particular, la RG 104 regula los requisitos para obtener la licencia "Australian Financial Services" y la RG 259 sobre la implementación de un Sistema de Gestión de Riesgos.

Otras guías regulatorias específicas para entidades del mercado financiero son la RG 172 ("*Mercados financieros: operadores nacionales y extranjeros*" y RG 265 ("*Reglas de integridad del mercado para participantes de los mercados de valores*").

En lo que respecta a Riesgo Operacional, los Intermediarios y las Bolsas deben:

- Identificar las funciones críticas de su negocio y contar con recursos tecnológicos suficientes para el establecimiento de controles en dichas funciones, de manera que aseguren su resiliencia ante fallas en los sistemas de TI o frente a brechas de seguridad.
- Notificar al regulador los incidentes de ciberseguridad que detecten. Adicionalmente, en el caso de los Intermediarios de Valores, deben notificar toda conducta que a su juicio les parezca sospechosa en relación a la integridad de las operaciones del mercado (ej. movimientos anómalos de precios y órdenes).
- Registrar sus incidentes operacionales en una Base de Incidentes, incluyendo incidentes relacionados con servicios críticos externalizados.
- Contar con Planes de Continuidad de Negocios y de Recuperación ante Desastres que involucren el respaldo de datos y la realización de pruebas de estrés, de manera tal que minimicen el impacto de incidentes que afecten el funcionamiento de las operaciones críticas del negocio y aseguren el cumplimiento de la regulación financiera. Estos planes deben ser revisados regularmente, aunque no hay un requerimiento específico sobre su periodicidad.
- Realizar pruebas periódicas de vulnerabilidad y capacidad para el monitoreo continuo de los sistemas críticos, acorde al Plan de Continuidad de Negocio.
- Contar con una función que supervise el Plan de Continuidad del Negocio y el funcionamiento de los Sistemas de Información. Dicha función debe ser realizada por personas con las calificaciones y experiencia adecuadas; no obstante, pueden ser llevadas a cabo eventualmente por una sola persona en función de la naturaleza, tamaño y complejidad de las operaciones de la entidad.
- Enviar al regulador un Informe de Auditoría Interna de sus sistemas tecnológicos. El regulador puede designar un auditor propio que participe en dicha auditoría o, en el caso de servicios críticos externalizados, en una auditoría del proveedor de servicios.
- Llevar a cabo una verificación de diligencia debida de potenciales proveedores de servicios críticos. El proveedor elegido debe ser autorizado por el regulador.
- Mantener una Base de Registro de Proveedores.

Colombia

En materia de Gestión de Riesgos, la Superintendencia Financiera de Colombia (SFC) toma como referencia el estándar australiano AS/NZS 4360:1999, la ISO 31000 (Gestión de Riesgos – Directrices) y las recomendaciones del Comité de Supervisión Bancaria de Basilea.

Para temas de Seguridad de la Información y Ciberseguridad, los referentes son las ISO/IEC 27001 (Sistemas de Gestión de Seguridad de la Información - Requisitos), 27017, 27018, 27032 (Directrices para la Ciberseguridad), SP 800 y1800 del National Institute of Standards and Technology (NIST) y las recomendaciones del Information Security Forum, los Critical Security Controls y Cobit 5.

En lo que respecta a la regulación de riesgo operacional de entidades supervisadas por la SFC, se destaca lo siguiente:

- Todas las entidades deben mantener un Sistema de Administración de Riesgo Operacional acorde a su estructura, tamaño, objeto social y actividades de apoyo, el cual debe ser aprobado por el Directorio. Los requisitos se encuentran en las "Instrucciones Generales aplicables a las Entidades Vigiladas", Título IV de la Circular Básica Jurídica de SFC. En particular, se enfatiza la prevención de riesgos de seguridad de la información y ciberseguridad (Capítulo IV del Título IV).
- Las actividades significativas de cada entidad supervisada son definidas por la propia SFC en base a una metodología que considera: importancia de la actividad en la generación de ingresos operacionales, uso intensivo de recursos de la entidad, fuente de riesgos operacionales, n° de clientes atendidos, complejidad del producto/servicio ofrecido, externalización, reclamos de clientes.
- La evaluación de las actividades significativas de la SFC se materializa en una matriz de riesgos que se presenta a la propia entidad, con sugerencias de mejora que pueden incorporar en su Plan de Continuidad del Negocio. Todas las entidades deben contar con este Plan y realizar pruebas de vulnerabilidad de sus sistemas.
- La Circular Externa 033 (2020) establece el envío de la siguiente información trimestral por todas las entidades financieras:
  - Gestión de incidentes: Las entidades deben mantener un Registro de Eventos de Riesgo Operacional, clasificándolo en dos tipos: Ciberseguridad y Otros. Se deben reportar al regulador las fallas en los sistemas que afecten o tengan el potencial de afectar la prestación de los servicios o generen errores en la información financiera puesta a disposición del público. La SFC realiza un análisis el evento reportado y monitorea los planes de mejora comprometidos por la entidad.
  - Nivel de madurez de la gestión del Sistema de Información y Ciberseguridad: Las entidades deben realizar una autoevaluación de controles de Ciberseguridad en función del grado de automatización y sofisticación, basada en una escala cualitativa de 5 categorías. Regularmente la SFC realiza auditorías de estos sistemas y elabora un reporte que entrega a la entidad con recomendaciones de mejora en sus controles.
  - Tiempo promedio de detección y respuesta a incidentes.
  - Gestión de vulnerabilidades.
  - Política de Capacitación en gestión de riesgos.
  - Evaluación de gestión de riesgos: Incluye una evaluación de las pérdidas asociadas a la materialización de riesgos operacionales, incluyendo sanciones económicas.
  - Presupuesto de la función de Gestión de Riesgos.

Estados Unidos

La Securities Exchange Act de 1934 de la Comisión de Bolsa y Valores de Estados Unidos (SEC) establece lineamientos generales de Gestión de Riesgos de Intermediarios y Bolsas a través de la Regulación de Sistemas de Cumplimiento e Integridad (SCI).

La sección 404 de la Ley Sarbanes-Oxley de 2002 regula la emisión de informes de Control Interno en los balances de las entidades financieras.

La regla 17Ad22 de Cámaras de Compensación requiere la identificación de fuentes de riesgo en la compensación o liquidación de operaciones, materializada en un Plan de Continuidad Operacional que contenga procedimientos para la recuperación oportuna de sus operaciones. Las Cámaras deben tener una Unidad de Gestión de Riesgos y una Unidad de Auditoría Interna independientes que respondan al Directorio.

La Commodity Futures Trading Commission (CFTC) requiere para sus supervisados la elaboración de informes de evaluación de riesgos y una actualización de los límites de tolerancia al riesgo aprobados por el Directorio y la Alta Administración. Cualquier cambio material relevante en las operaciones o en los riesgos del negocio debe ser informado dentro de las 24 horas.

El National Institute of Standards and Technology (NIST) tiene un estándar mínimo para el manejo de riesgos de Ciberseguridad que considera el monitoreo de activos de información, la asignación de responsabilidades del personal de TI, el control de acceso a redes, las políticas de respaldo de información, la actualización de hardware y software y los planes de respuesta ante incidentes.

No existe actualmente una ley de Riesgos de Ciberseguridad de aplicación general. Se puede mencionar la ley federal de Modernización de Servicios Financieros (1999), que establece la obligatoriedad de contar con un Plan de Seguridad de la Información. Actualmente, se encuentra en consulta una regla de la SEC para el manejo de los riesgos de Ciberseguridad para empresas del sector público.

En lo que respecta a la Gestión de Riesgo Operacional, se destacan los siguientes requisitos para Intermediarios y Bolsas:

- El Directorio y la Alta Administración deben capacitarse en Gestión de Riesgos.
- Se deben identificar las funciones críticas del negocio.
- Se contará con Planes de Continuidad del Negocio y Recuperación ante Desastres, que incluyan capacidades de respaldo resilientes y geográficamente diversas para la reanudación de las operaciones al día hábil siguiente (o en dos horas, en el caso de servicios críticos de SCI). Asimismo:

  - Para el caso de operaciones de swaps, el Plan de Continuidad de Negocios debe contener un detalle de los datos, instalaciones, infraestructura, comunicaciones, respaldo de datos y competencias esenciales para la continuidad de las operaciones del operador y participantes principales.
  - El Plan de Continuidad de Negocios debe contemplar la realización de pruebas de vulnerabilidad, penetración y cumplimiento periódicas, incluyendo escenarios severos tales como huracanes, terremotos, incendios y contingencias sanitarias.

- Notificación al regulador de los incidentes de ciberseguridad detectados. Esta función puede estar a cargo de una sola persona, no siendo necesario llevar una Base de Registro de Incidentes.
- Elaboración de un informe de auditoría de sistemas TI.
- La SEC está facultada para auditar todo servicio subcontratado, aunque no obliga a las entidades a mantener una Base de Registro de Proveedores.

México

La Comisión Nacional Bancaria y de Valores (CNBV) utiliza el estándar regulatorio del Comité de Supervisión Bancaria de Basilea y establece lineamientos generales de Gestión de Riesgos en la Ley del Mercado de Valores.

En materia de gestión de riesgo operacional, se destaca la emisión de las "*Disposiciones de Carácter General aplicables a las Casas de Bolsa*" (2004) y la "*Guía aplicable a las solicitudes de autorización para la organización y cooperación de Casas de Bolsa*" (2015) de Intermediarios. Los principales requisitos son los siguientes:

- A diferencia del regulador australiano, no se considera un criterio de proporcionalidad, sino que las normas mencionadas se aplican a todos los Intermediarios, independientemente de su tamaño.
- Las entidades deben llevar a cabo un Análisis e Impacto al Negocio que incluya la totalidad de los servicios, procesos y participantes, identificando aquellos procesos críticos indispensables para la continuidad de las operaciones.
- Las entidades deben contar con un Plan de Continuidad de Negocio y someterlo al menos una vez al año a pruebas de efectividad de controles, seguridad de red y seguridad física y ejercicios de gestión de crisis, entre otros. El regulador no requiere el envío de los resultados de estas pruebas, pero puede solicitarlo a petición.

En lo que respecta al Sistema de Gestión de Riesgos, los Intermediarios deben contar con:

- Programas semestrales de revisión de límites de exposición y niveles de tolerancia al riesgo aprobados por el Directorio.
- Una Unidad de Administración Integral de Riesgos independiente, encargada de identificar y evaluar los riesgos que enfrenta la entidad. La metodología de evaluación se materializa en un Manual de Administración Integral de Riesgos aprobado por el Comité de Riesgos (los riesgos se clasifican en tecnológico, de crédito, liquidez, de mercado, legal y riesgos no cuantificables).
- Un Comité de Riesgos encargado de la administración de los riesgos de la entidad. Está integrado por un miembro del Directorio, el Gerente General, el responsable de la Unidad de Administración Integral de Riesgos y el responsable de la Unidad de Auditoría Interna. Sesiona al menos mensualmente.
- Un Área de Auditoría Interna independiente, encargada de la evaluación del cumplimiento de las políticas de Gestión de Riesgos y Control Interno de la entidad.
- Un Comité de Auditoría encargado del seguimiento de las actividades de auditoría interna y externa. Está integrado con al menos dos y no más de cinco miembros del Directorio, uno de los cuales debe ser independiente. Sesiona al menos trimestralmente.

- Un Manual de Administración de Riesgo Operacional, que contiene las políticas y procedimientos para:
  - Mantenimiento de una Base de Datos de Eventos por Pérdida de Riesgo Operacional.
  - Reporte de incidentes operacionales (Reporte R28). Este reporte contiene información del tipo de riesgo operacional de acuerdo a una clasificación de la CNBV, el monto de la pérdida financiera y las áreas de negocio, productos y clientes afectados.
  - Procedimientos de gestión de riesgo operacional.
  - Cálculo del requerimiento de Capital por Riesgo Operacional.
  - Procedimientos de seguridad de instalaciones físicas y seguridad lógica.

- Procedimientos de gestión de incidentes y reclamaciones realizadas por los clientes.
- Políticas de externalización de servicios de bases de datos y otros procesos operativos:
  - Antes de externalizar el servicio, las entidades deben asegurarse de contar con esquemas de registro, redundancia, continuidad y monitoreo de la calidad del servicio.
  - Designar a un Oficial de Seguridad independiente que realizará el monitoreo del servicio.
  - Tomar medidas para el control y vigilancia de acceso a los Sistemas de Información. Por ejemplo, cifrado de datos, control de perfiles de acceso a usuarios y auditorías de TI.

Perú

La Superintendencia del Mercado de Valores (SMV) ha utilizado como estándares para el desarrollo de la normativa de gestión de Riesgo Operacional las ISO 31000, 27001, 22301 (Sistemas de Gestión de Continuidad del Negocio - Requisitos), 27032 y el Marco para la mejora de la Ciberseguridad en infraestructuras críticas de NIST.

Los requisitos para la gestión del Riesgo Operacional están en el "*Reglamento de Gestión del Riesgo Operacional*" para todas las entidades financieras supervisadas por SMV. Se destaca lo siguiente:

- Las exigencias son acordes al tamaño de la entidad, el volumen de transacciones y la complejidad de sus operaciones (principio de Proporcionalidad).
- La entidad debe determinar sus servicios críticos en base a una identificación de las actividades del negocio y el posible impacto financiero y regulatorio que una interrupción tendría en la propia entidad, en los clientes y el público general.
- La metodología de gestión de riesgo operacional comprende el Sistema de Gestión de Seguridad de la Información y el Sistema de Gestión de la Continuidad del Negocio. Dicha metodología es aprobada por el Directorio.
- La entidad debe contar con una Función de Gestión de Seguridad de la Información y Ciberseguridad encargada del Sistema de Gestión de la Seguridad de la Información. Reportará al Directorio o al Comité de Riesgos con una periodicidad no mayor a 6 meses.
- La entidad debe contar con una Función de Continuidad del Negocio encargada del Sistema de Gestión de la Continuidad del Negocio. Reportará al Directorio o al Comité de Riesgos con una periodicidad no mayor a un año.
- La entidad debe remitir un informe a la SMV en caso de Cambios Significativos en sus Sistemas de Gestión, con una descripción del cambio, los procesos asociados, los riesgos identificados (diferenciados por tipos de riesgo) y las medidas implementadas.
- La entidad debe remitir un Reporte de Indicadores Clave de Gestión de Riesgo Operacional a la SMV en forma trimestral, semestral y anual. Dentro de este Reporte se incluye un "Reporte de Planes de Continuidad del Negocio" en donde la entidad debe

informar el número de planes probados (Plan de Gestión de Crisis, Plan de Emergencia, Plan de Continuidad del Negocio y Plan de recuperación de servicios de TI) y la cantidad de pruebas realizadas a estos dos últimos.

- En caso de ocurrencia de eventos de interrupción significativa de operaciones, esta deberá ser comunicada a la SMV al día siguiente hábil, incluyendo una descripción general del evento ocurrido. Si el incidente corresponde a la gestión de la Continuidad del Negocio, la Superintendencia Adjunta de Riesgos de la SMV evaluará el impacto generado y eventualmente instruirá al fiscalizado sobre las medidas a adoptar.
- La entidad debe mantener una Base de Eventos de Pérdida por Riesgo Operacional y registrar incidentes que signifiquen una pérdida superior a tres mil soles. No obstante, la entidad podrá establecer un monto mínimo inferior en función del tamaño, volumen de transacciones y complejidad de sus operaciones (y la SMV podrá modificar dicho monto):
  - No hay una exigencia de remitir periódicamente esta base de datos al regulador.
  - Los incidentes deben ser clasificados de acuerdo a la siguiente tipología:

    - Fraude Interno
    - Fraude Externo
    - Relaciones laborales y seguridad en el puesto de trabajo
    - Prácticas relacionadas con los clientes, los productos y el negocio
    - Daños a activos físicos
    - Interrupción del negocio por fallas en la tecnología de información
    - Deficiencia en la ejecución, entrega y gestión de procesos

- Las pruebas deben realizarse periódicamente y cuando existan cambios significativos. Deberán estar basadas en escenarios planificados y tener un reporte interno que resuma los resultados alcanzados y las acciones de mejora a implementar. Este reporte no debe ser enviado a la SMV a menos que ésta solicite esta información.
- El Plan de continuidad del negocio deberá ser probado cuando menos una vez al año.
- La Política de Subcontratación debe seguir los siguientes lineamientos:

  - Contar con procedimientos para evaluar el nivel de riesgo del servicio subcontratado, selección del proveedor, monitoreo del servicio, planes de continuidad y estrategias de salida.
  - La entidad asume plena responsabilidad por el servicio subcontratado, y en el caso de un servicio crítico deberá considerarlo como un Cambio Significativo. No hay exigencias más específicas sobre el manejo de los datos entregados al proveedor y la gestión de incidentes.
  - La entidad debe mantener un registro actualizado de información de todos los servicios subcontratados, con información del tipo de subcontratación (significativa y no significativa), la fecha de inicio y término, y la descripción de las modificaciones realizadas al contrato.
  - En el caso de servicios en la nube que involucren un Cambio Significativo, se deberá realizar una diligencia reforzada del proveedor y del servicio, considerando los permisos de acceso, la seguridad de datos y sistemas, localización y procesamiento de datos y el caso en que el proveedor a su vez subcontrate todo o parte del servicio.

Singapur

El marco general de Gestión de Riesgos viene dado por el estándar AS/NZS ISO 31000:2009, el "*Enterprise Risk Management – Integrated Framework*" del Committee of Sponsoring Organizations (COSO) y la ISO 31000:2009 y las guías regulatorias específicas de la

Autoridad Monetaria de Singapur (MAS): "*Guía de prácticas de manejo de riesgo – Controles Internos"* y "*Guía de prácticas de manejo de riesgo para entidades aseguradoras*".

En lo que respecta a Riesgo Operacional de Intermediarios y Bolsas, se establece lo siguiente:

- El Directorio debe aprobar la Política de Gestión de Riesgos. Los integrantes del Directorio deben certificarse en gestión de riesgos.
- La entidad debe realizar un Análisis de Impacto del Negocio e identificar los sistemas críticos para asegurar la resiliencia, confiabilidad e integridad de los mismos. Se entiende por sistema crítico:
  - Aquel cuya falla cause una interrupción significativa en las operaciones de la entidad o afecte materialmente el servicio provisto a los clientes.
  - Un sistema que procesa transacciones que son críticas en cuanto al tiempo o proporciona servicios esenciales a los clientes.
- La entidad debe contar con un marco de Gestión de Riesgos Tecnológicos, incluido una Base de Registro de Riesgos, que facilite la gestión del cambio tecnológico y la respuesta ante incidentes. Se espera que los Intermediarios mantengan una alta disponibilidad y capacidad de recuperación del sistema, incluyendo el desarrollo de redundancias integradas para reducir los puntos de falla de red, y el mantenimiento de hardware, software y componentes de red en espera.
- La información confidencial y la seguridad física de los centros de datos donde se mantienen los sistemas críticos deben protegerse.
- El regulador debe ser notificado tan pronto como sea posible y más tardar en una hora sobre el descubrimiento de un incidente importante. Dentro de los 14 días siguientes, la entidad debe presentar un Informe con el análisis del incidente, su impacto y las medidas correctivas adoptadas.
- Enviar un Plan de Continuidad de Negocios al MAS y mantenerlo actualizado.
- Realizar pruebas de control de inventario, seguridad, vulnerabilidad y penetración.
- Enviar un Plan de Recuperación de Incidentes que incluya a los proveedores de servicios externalizados.
- Contar con reportes de evaluación de impacto de Subcontratación de funciones críticas. Está prohibido subcontratar proveedores por períodos inferiores a 6 meses. El MAS está facultado para efectuar una auditoría sobre los mismos.

COMISIÓN
PARA EL MERCADO
FINANCIERO

Regulador y Supervisor Financiero de Chile

www.cmfchile.cl