Capítulo 4
Riesgos operacionales

Vicente Lazen
Jefe de la División de Custodia y Liquidación de Valores de la Superintendencia de Valores y Seguros de Chile

1. Introducción
2. Riesgo operacional
3. Riesgo tecnológico
4. Continuidad operacional o de negocios
5. Situación en Iberoamérica

1. Introducción

El riesgo operacional se puede definir como el riesgo de pérdida debido a la inadecuación o a la falla de los procesos, del personal, y de los sistemas internos y/o de los controles internos aplicables que podrían perjudicar la prestación de servicios, lo que podría repercutir en la exposición del mercado a un riesgo sistémico, en caso de afectar una entidad de depósito y custodia de valores, o una entidad de compensación y liquidación. Dichas fallas pueden perjudicar la reputación y la percepción sobre la fiabilidad de una entidad, derivando en consecuencias legales y pérdidas financieras para las entidades y sus participantes.

De acuerdo con el actual borrador del documento sobre Principios CPSS – IOSCO para las Infraestructuras del Mercado Financiero[1], el Principio 17: Riesgo operativo establece que:

"Una Infraestructura de Mercados Financieros (FMI) deberá identificar todas las fuentes plausibles de riesgo operativo, tanto internas como externas, y minimizar su impacto a través del uso de sistemas, controles y procedimientos adecuados. Los sistemas deberán disponer de un alto grado de seguridad y fiabilidad operativa, y tendrán una capacidad adecuada y versátil. Los planes de continuidad del servicio deberán tener como objetivo la recuperación oportuna de las operaciones y el cumplimiento de las obligaciones de la FMI, incluso en caso de que se produzcan alteraciones a gran escala".

Asimismo, estos estándares indican que las Infraestructuras del Mercado Financiero deben:

[1] Ver Capítulo 8 de este Estudio

- *Contar con un sólido marco de gestión del riesgo operativo que disponga de los sistemas, políticas, procedimientos y controles oportunos para identificar, controlar y gestionar los riesgos operativos.*

- *Definir claramente las funciones y responsabilidades con relación al riesgo operativo, y su marco de gestión del riesgo operativo deberá contar con el respaldo del consejo de administración de la FMI.*

- *Contar con unos objetivos de fiabilidad operativa claramente definidos y disponer de políticas que sean proporcionales a dichos objetivos. Una FMI deberá contar con una capacidad y versatilidad adecuadas, así como con las herramientas y procedimientos necesarios para controlar el rendimiento de la FMI.*

- *Disponer de políticas de seguridad de la información y de seguridad física debidamente definidas. Todas las vulnerabilidades y amenazas potenciales deberán ser investigadas, evaluadas y documentadas.*

- *Contar con un plan de capacidad y continuidad de servicio que aborde acontecimientos que representen un riesgo importante de alteración de sus actividades, como también, acontecimientos de gran escala.*

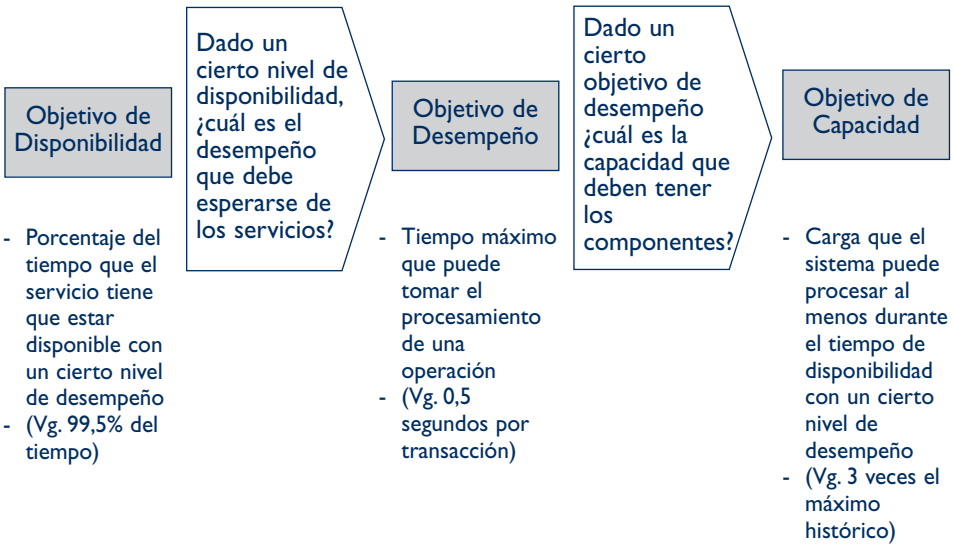
- *Identificar, controlar y gestionar los riesgos que los principales participantes, las otras FMI y los proveedores de servicios podrían representar para sus actividades. Asimismo, una FMI deberá identificar, controlar y gestionar los riesgos que sus actividades puedan representar para otras FMI.*

De acuerdo a lo mencionado, estas infraestructuras deben adquirir fiabilidad operativa en su función, controlando los riesgos operativos y tecnológicos producto del uso intensivo de tecnologías de información, capacidad operativa, seguridad de la información, y continuidad de negocios y recuperación ante desastres.

A continuación se detallan dichos riesgos y se definen los estándares internacionales que están asociados para su control.

Disponibilidad, desempeño y capacidad en las entidades de custodia, compensación y liquidación

Existe una estrecha relación entre los conceptos de disponibilidad, desempeño y capacidad de los sistemas tecnológicos. Particularmente en las entidades de custodia, compensación y liquidación. Esta interconexión de los tres elementos es esencial para desarrollar la estrategia y determinar la adecuación de las entidades a los objetivos que les impone el mercado.



Fuente: Superintendencia de Valores y Seguros – Chile. Informe "Estado y evaluación del Sistema de Compensación, Custodia y liquidación de valores 2009/2010"

2. Riesgo operacional

Para gestionar los riesgos operacionales y cumplir con los principios mencionados en el apartado anterior, las infraestructuras del mercado financiero pueden emplear diversos estándares internacionales. En particular, el estándar COSO (*Committee of Sponsoring Organizations of the Treadway Commission*) es un modelo integrado de control interno que permite a las entidades un mejor tratamiento de los riesgos.

Bajo este estándar, las prácticas internacionales definen que, en el marco de la gestión de riesgo operacional, se debe identificar, medir, controlar y monitorear el riesgo operacional que pueda afectar de forma adversa la consecución de sus obligaciones establecidas en el marco legal. Para ello, se deben establecer procedimientos documentados que deben considerar al menos:

- Una política de gestión de riesgo aprobada por el directorio de la entidad.

- Un manual de gestión de riesgo operacional que detalle los procedimientos formales para gestionar los riesgos de la entidad.

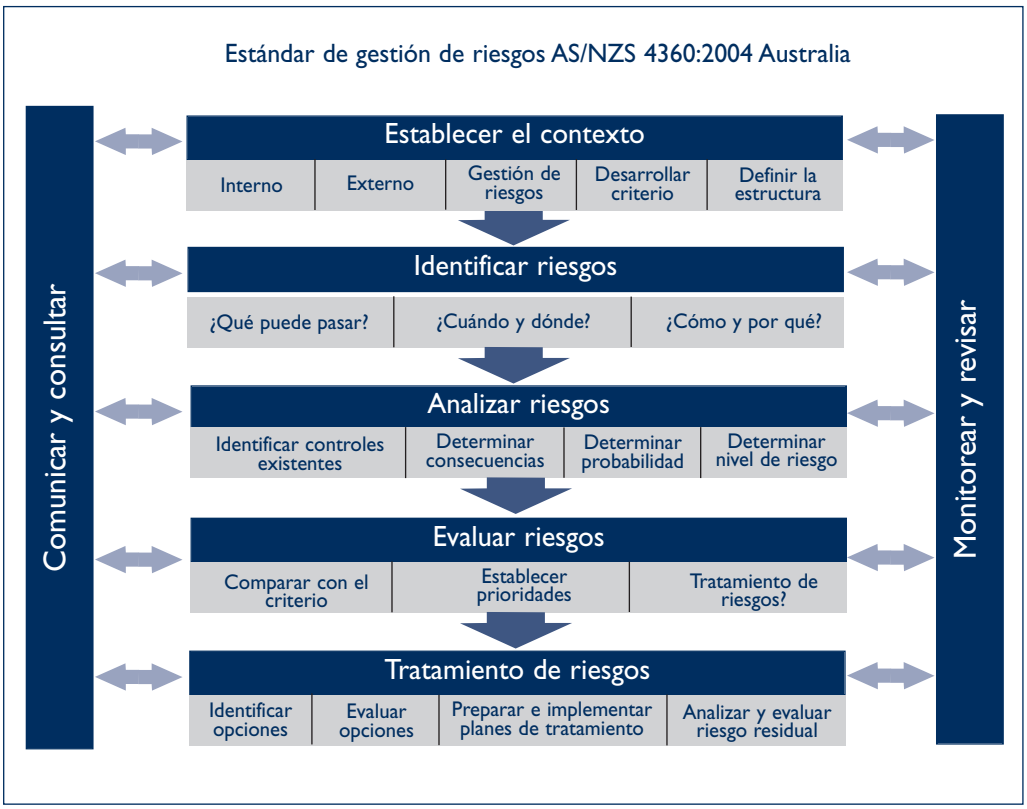
- Identificar los riesgos y factores que influyen en los procesos, definiendo el nivel de riesgo inherente, impacto y probabilidad de ocurrencia. A partir de ello se debe estimar el riesgo residual o nivel de riesgo expuesto.

- Analizar las opciones para el tratamiento de riesgos establecidas en la política, de acuerdo a las que se debe elaborar un plan de acción.

- El monitoreo de dichos riesgos y actividades de control, debe ser permanente de modo de definir la efectividad de las medidas implementadas.

- Toda la organización, en general, debe ser constantemente informada de la gestión de riesgo que se lleva a cabo y el monitoreo realizado.

Este estándar se enmarca en un proceso, cuyas etapas se muestran en el siguiente esquema del estándar australiano – semejante a COSO y a la norma ISO 31.000 –:



3. Riesgo tecnológico

El riesgo tecnológico toma relevancia en la gestión de riesgo operacional, debido al uso de los sistemas de información (TI) dentro de los procesos de negocio. Las entidades de infraestructura de mercado son altamente intensivas en el uso de sistemas de información, por lo que la correcta gestión de los riesgos asociados al uso de las tecnologías de información (recursos tecnológicos), resulta de suma importancia y es necesario que deban estar bajo un adecuado control. Los recursos tecnológicos son: 1) Las aplicaciones, 2) La información; 3) La infraestructura y 4) Las personas (que operan estos recursos).

Para garantizar un adecuado control de los recursos tecnológicos, se utilizan los estándares Cobit (*Control Objectives for Information and related Technology*), ITIL (*Information Technology Infrastructure Library*) e ISO 27001, que pasaremos a comentar a continuación:

Cobit

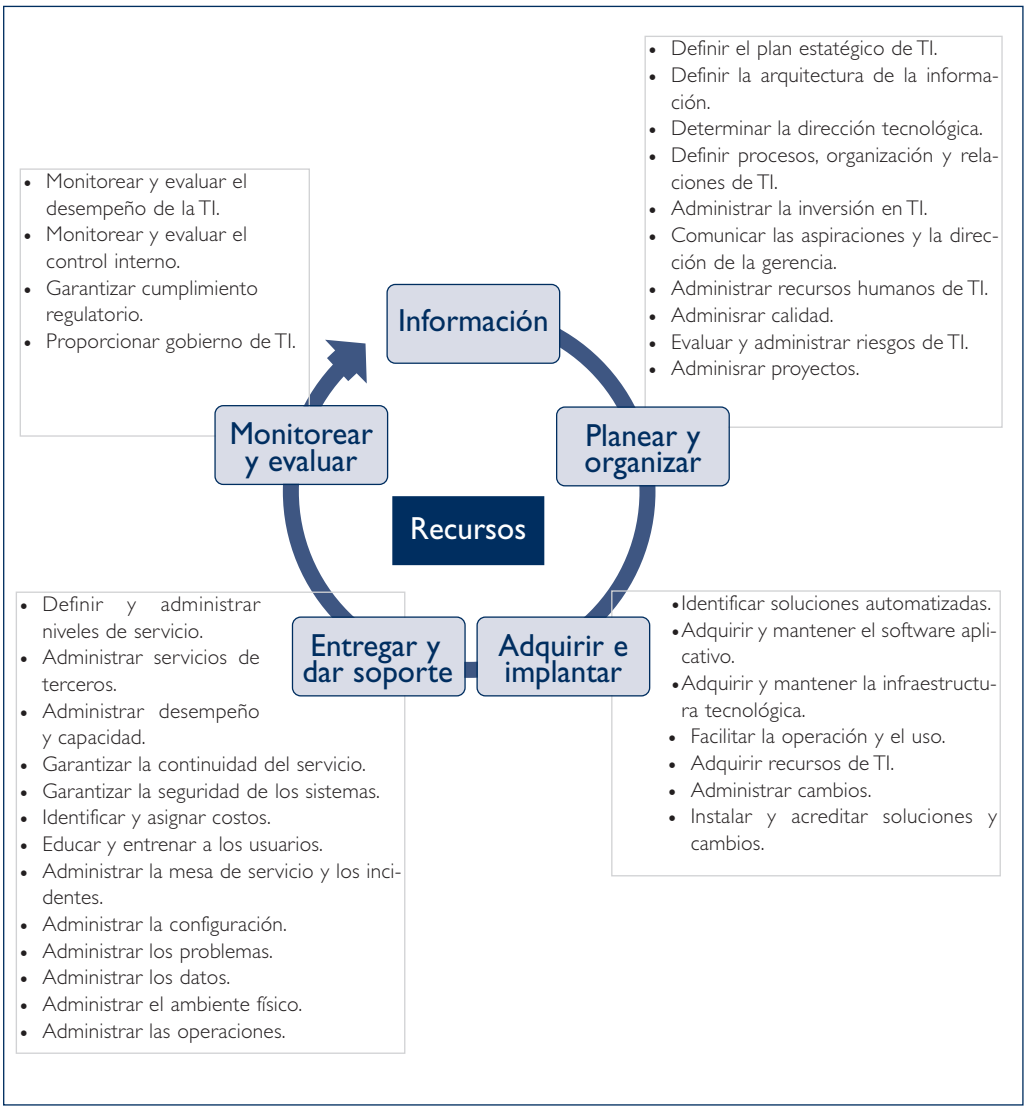
Es un marco de trabajo de control interno de TI para las empresas, que permite a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio. En este contexto, provee de un marco de buenas prácticas para definir y alinear los objetivos de TI con los requerimientos y objetivos del negocio. Dichas prácticas se enmarcan en un modelo de procesos que está enfocado en los aspectos que se requieren para lograr una administración y un control adecuado para todos los procesos de TI, constituyendo una guía integral para la gerencia y para los responsables de los procesos de negocio.

El principio clave de Cobit es que la empresa necesita invertir, administrar y controlar los recursos de TI, usando un conjunto estructurado de procesos que provean los servicios de tecnología requeridos para que la empresa logre sus objetivos. De esta manera, Cobit permite describir los procesos, definir los objetivos, generar las métricas, y medir el estado de madurez en el que se encuentran dichos procesos, enfocándose en satisfacer los objetivos del negocio conforme a criterios de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

Cobit entrega al gobierno de TI herramientas enfocadas en: la alineación estratégica, garantizar la entrega de valor, la administración de recursos críticos de TI, la administración de riesgos y medición del desempeño de los recursos de TI.

El ciclo de Cobit consta de cuatro dominios, estos son:

- Planear y organizar.
- Adquirir e implantar.
- Entregar y dar soporte.
- Monitorear y evaluar.



En el contexto de gestión de riesgo operacional, Cobit define los siguientes aspectos a ser considerados:

- Integrar el gobierno, la administración de riesgos y el marco de control de TI, al marco de trabajo de administración de riesgos de la organización.

- Establecimiento del contexto en el cual, el marco de trabajo de evaluación de riesgos, se aplica para garantizar resultados apropiados.

- Identificación de eventos (amenazas y vulnerabilidades) con un impacto potencial sobre las metas o las operaciones de la empresa, aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos.

- Evaluación de la posibilidad e impacto de todos los riesgos identificados, cualitativa y cuantitativamente.

- Identificación de los responsables de controlar los riesgos y a los dueños de procesos afectados, y elaborar y mantener respuestas que permitan la mitigación continúa de los riesgos. La respuesta a los riesgos debe identificar estrategias de riesgo tales como evitar, reducir, compartir o aceptar.

- Mantenimiento y monitoreo de un plan de acción de riesgos. Esto significa asignar prioridades y planear las actividades de control a todos los niveles para implantar las respuestas a los riesgos, identificadas como necesarias, costos, beneficios, responsables y riesgo residual aceptado. Además se deben realizar evaluaciones de riesgo periódicas con los gerentes senior y con el personal clave.

ITIL

Provee un marco de trabajo de mejores prácticas para la gestión de servicios de TI, y se enfoca en la medición y mejoramiento continuo de la calidad del servicio entregado desde la perspectiva del negocio y del cliente. A través de una aproximación sistemática a la planificación, desarrollo, entrega y soporte de los servicios TI para el negocio, aúna la comunidad dedicada al negocio y el departamento de TI. Su fundamento es la calidad y mejora continua del ciclo de vida del servicio, el cual es iterativo y multidimensional.

ITIL divide las actividades en procesos, proporcionando un marco eficaz para lograr una gestión de servicios TI más madura, al objeto de optimizar y mejorar la coordinación de los procesos. De este modo, provee estructura, estabilidad y fuerza a la administración de los servicios TI, con el fin de proteger las inversiones y proveer la base necesaria para la medición, aprendizaje y mejora de los servicios de TI.

El ciclo de vida del servicio comprende 5 aspectos:

- Estrategia de servicios: diseño, desarrollo e implementación de la administración como un activo estratégico.

- Diseño del servicio: diseño y desarrollo de servicios y de procesos de administración de servicios para convertir objetivos estratégicos en portafolios de servicios.

- Operación del servicio: gestión de operaciones que permite alcanzar la eficiencia y eficacia en la prestación y soporte garantizando el valor al cliente.

- Transición de servicio: guía para el desarrollo y mejora de la transición de servicios nuevos o modificados a operaciones controlando los riesgos asociados.

- Mejoramiento continúo del servicio: creación y mantención del valor a través de un mejor diseño, combinando principios, prácticas y métodos de gestión de la calidad, gestión de cambios y mejoramiento de capacidad.

ISO 27001

La seguridad de la información es otro elemento de importancia en la gestión de la seguridad tecnológica. Este objetivo de control involucra tres componentes: la integridad de la información, la seguridad de la información y la confidencialidad. Los elementos de seguridad tecnológica son analizados en base a diversos estándares de la materia. Destaca el estándar ISO 27001, que corresponde a un estándar de seguridad de la información que

especifica los requerimientos necesarios para establecer, implementar, operar, monitorear, revisar, mantener, y mejorar continuamente el sistema de gestión de seguridad de la información, para así preservar la integridad, confidencialidad y disponibilidad de la información. Para ello se adopta una aproximación de procesos que permite:

- Comprender los requerimientos de seguridad de la información y la necesidad de establecer políticas y objetivos para seguridad de la información.
- Implementar y operar controles para gestionar los riesgos de seguridad de la información en el contexto de todos los riesgos de negocios.
- Monitorear y revisar el rendimiento y efectividad del sistema de gestión.
- Desarrollar un proceso de mejora continua basada en medición de objetivos.

Este estándar establece como requerimientos para gestionar la seguridad de la información lo siguiente:

- La administración debe establecer una política de seguridad de la información, indicando roles y responsabilidades: se debe desarrollar una metodología que permita identificar los riesgos para analizar y evaluar el riesgo aceptado.
- Desarrollo de un plan de tratamiento de riesgos, además de implementar controles: se deben definir las métricas, y se debe considerar la documentación de procedimientos ante incidentes y la capacitación.
- Ejecución de un monitoreo y revisiones regulares de la efectividad del sistema: se deben revisar los niveles de riesgo residual y aceptado y conducir auditorías internas con periodicidad. La administración debe actualizarse constantemente en función de la experiencia real frente a eventos de impacto.
- Implementar las mejoras identificadas en un proceso de mejora continua que debe comprobar la efectividad de la gestión de seguridad de la información.
- Realizar auditorías internas para evaluar la conformidad de los objetivos, controles, procesos y procedimientos respecto a los estándares y la regulación.

4. Continuidad operacional o de negocios

Como continuidad operacional se entiende el garantizar la continuidad de un proceso ante un evento que afecte o interrumpa su normal funcionamiento, como puede ser un terremoto, una pandemia, etc., sucesos en los que puede existir una pérdida temporal o permanente de la infraestructura o de recursos de la entidad.

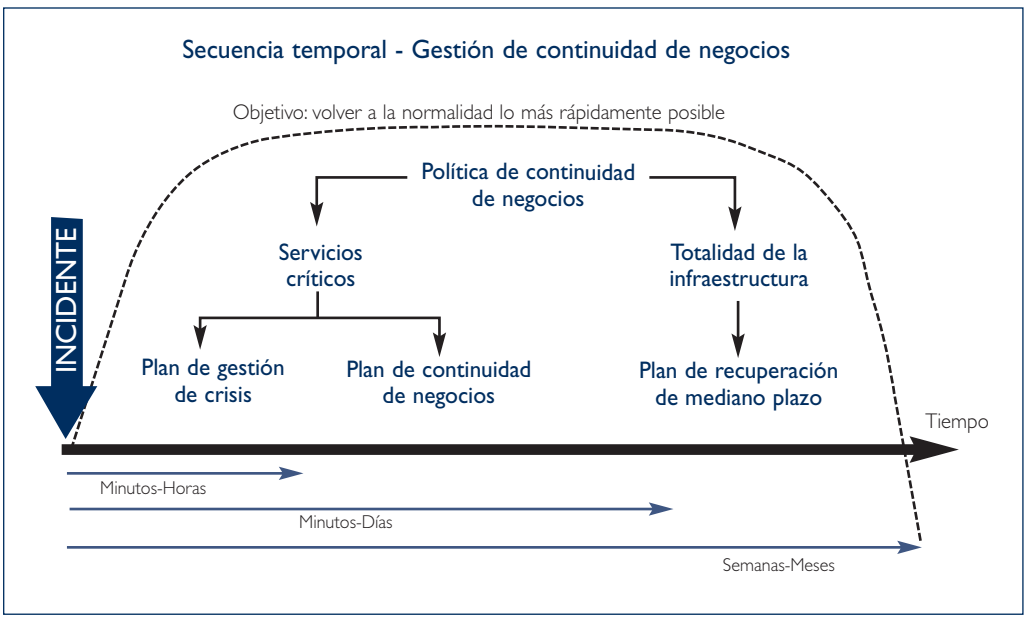
La suspensión o el atraso prolongado por parte de las entidades de infraestructura de mercado en la prestación de servicios críticos, tendría consecuencias operacionales y financieras sobre todos sus usuarios, a raíz de la incertidumbre e imposibilidad de continuar operando en los mercados hasta el reinicio de los servicios, los cuales son esenciales para la propia continuidad de negocio y sustentabilidad de sus usuarios.

En el mundo, las organizaciones adoptan estándares que establecen mejores prácticas, recomendaciones y actividades específicas para garantizar la continuidad de negocio tales como el BS 25999. Este estándar exige a las entidades el desarrollo de una política de continuidad de negocio donde se defina el alcance de la gestión de continuidad, sus lineamientos, objetivos y principales roles y responsabilidades. Además, establece que los servicios externalizados deben cumplir con las disposiciones de estos estándares.

- Se deben identificar los servicios críticos para la entidad, considerando las amenazas que pueden tener efectos sobre la disponibilidad, capacidad financiera, desempeño, cumplimiento normativo y reputación.

- Se debe desarrollar un plan de gestión de crisis, el cual debe comprender al menos los siguientes elementos: listado de tareas, personal responsable, contactos relevantes, estrategias de comunicación frente a un escenario crítico. Asimismo, se exige un tiempo de recuperación objetivo para los servicios críticos de las entidades.

- Se debe generar un plan de continuidad de negocios, cuyo fin es documentar las estrategias de respuesta y sus planes de recuperación de los servicios para reducir el impacto



de una amenaza, ya sea terrorismo, terremoto, incendio, etc. Dicho plan debe definir la respuesta de las personas mediante documentación y capacitación apropiadas, debe considerar la existencia de infraestructuras tecnológicas alternativas distanciadas geográficamente, oficinas alternativas y la posibilidad de ejecución remota de actividades criticas, replicación de toda la información necesaria para reiniciar los servicios críticos de la entidad, dos conexiones a Internet con distintos ISPs, infraestructura alternativa, entidades relacionadas y proveedores externos.

- Finalmente, debe desarrollarse un plan de recuperación de mediano plazo encaminado al reestablecimiento total de la infraestructura y la reposición de recursos de acuerdo a condiciones normales de operación, un manual de coordinación que indique los servicios críticos, protocolo de comunicación y coordinación para recuperar los servicios críticos y el personal clave.

- Se exigen pruebas periódicas de los planes mencionados, además de sistemas de comunicación alternativos con los clientes, personal clave y autoridades supervisoras.

5. Situación en Iberoamérica

La heterogeneidad del desarrollo organizacional de la gestión de riesgo operacional en Iberoamérica es notoria en los resultados del estudio. Por una parte, en los sistemas de Chile, Portugal y Perú existe el desarrollo de una unidad que coordina la gestión de riesgo además de otra unidad independiente que audita la implementación de los planes de gestión de riesgo operacional. En el caso particular de Chile, tanto la organización de la entidad de depósito, como la del sistema de compensación, comprenden ambas unidades. Por otra parte, en España, Costa Rica y Panamá existe una sola unidad – comité – responsable de la gestión de riesgo operacional. Dicha unidad está conformada por miembros de la junta directiva.

En México existe una Dirección de administración de riesgos que realiza las tareas de administración, coordinación y supervisión, mientras que en Ecuador se establece una unidad de riesgos. En Bolivia y Ecuador se contempla la existencia de un oficial de cumplimiento. En el resto de los países, también se han implementado políticas de manejo de riesgos que incluyen detección, manejo y supervisión de riesgos, no obstante, no se explicitan unidades establecidas en el organigrama que cumplan el rol de coordinar dicha gestión.

Debido a que la estructura organizacional enfocada a la gestión de riesgo operacional difiere entre los países, las directrices y políticas de gestión de riesgo también son diferentes. En este contexto, existen desarrollos de reglas de buena conducta y confidencialidad – realizados en Panamá y Argentina –, en tanto en países como Brasil y Nicaragua principalmente se enfocan en la continuidad de negocios. En Bolivia existe una política de gestión de riesgos, y en Ecuador se han desarrollado normas de seguridad y manuales, mientras que en España existe un control de capacidad técnica.

En Portugal, Perú, Costa Rica y Chile, las políticas y normas desarrolladas han dado origen a procedimientos, roles, responsabilidades y definiciones de riesgos, análisis de impacto de los riesgos en el negocio, riesgos aceptados, manuales, medidas de mitigación, errores y planes de contingencia, monitoreo y auditorías externas. Los planes de seguridad en Perú y Bolivia emplean la metodología COBIT y las normas ISO 27001.

Respecto a continuidad de negocios en Argentina, Bolivia, Brasil, Chile, Costa Rica, España, México, y Panamá, se consideran políticas y procedimientos de contingencia, pruebas periódicas y la disponibilidad de sitios alternativos y de respaldo a una distancia geográfica que permita garantizar la reposición rápida del funcionamiento del sistema frente a desastres, empleando diversos estándares tecnológicos. Dichos estándares incluyen, entre otras características, sitios de respaldo actualizados en tiempo real, generadores, grupos electrógenos y planes de contingencia. Por su parte, en Nicaragua y Ecuador existen políticas y procedimientos de contingencia. En Portugal el plan de continuidad de negocios se encuentra en desarrollo.