COMISIÓN
PARA EL MERCADO
FINANCIERO

Regulador y Supervisor Financiero de Chile

Informe Normativo

Norma de Externalización de Servicios en Compañías de Seguros

Agosto 2025

www.CMFChile.cl

INDICE

I. INTRODUCCIÓN

En mayo de 2021 la Comisión para el Mercado Financiero, CMF, emitió la Norma de Carácter General N°454 que estableció los principios y conceptos de una correcta gestión del riesgo operacional y ciberseguridad, así como la realización periódica de autoevaluaciones en dichas materias.

En dicho contexto, se observa que la externalización de actividades, funciones o procesos es una práctica habitual dentro del mercado asegurador, asociada a la búsqueda de mayor eficiencia operativa, incorporación de tecnologías especializadas y mayor flexibilidad organizacional. No obstante, esta práctica también puede generar una exposición significativa a distintos tipos de riesgos, en particular al riesgo operacional, en aspectos tales como la continuidad operacional, la ciberseguridad, la protección de datos, la calidad del servicio, y el cumplimiento normativo.

La presente norma se enmarca dentro de la implementación del modelo de Supervisión Basada en Riesgo y se fundamenta en los principios de gestión prudencial establecidos en la Norma de Carácter General N°309 sobre Gobierno Corporativo, la Norma de Carácter General N°325 sobre Sistemas de Gestión de Riesgos y la Norma de Carácter General N°454 sobre Gestión de Riesgo Operacional y Ciberseguridad. En concordancia con estos cuerpos normativos, la presente norma establece los principios y requisitos mínimos que deberán observar las compañías para identificar, evaluar, monitorear y controlar los riesgos derivados de la externalización de servicios.

Esta norma establece, por una parte, criterios para la evaluación de la materialidad y criticidad de los servicios externalizados, lineamientos sobre los procesos de selección y contratación de proveedores, requisitos contractuales mínimos, medidas para la gestión de subcontrataciones, así como la necesidad de incorporar los servicios externalizados en los planes de continuidad del negocio y en los mecanismos de ciberseguridad de las compañías de seguros.

Finalmente, y reforzando las exigencias de trazabilidad y transparencia en la relación con los proveedores, se refuerza que la obligación de garantizar el acceso de la Comisión a la información relacionada con los servicios externalizados recae sobre la compañía de seguros, independiente de las condiciones contractuales establecidas con los proveedores. Esto implica que las compañías deberán adoptar todas las medidas necesarias para asegurar el cumplimiento de este principio, incluyendo cláusulas contractuales claras y mecanismos de supervisión efectivos, de forma tal que permita a la CMF el cumplimiento de su rol supervisor.

II. OBJETIVO DE LA PROPUESTA NORMATIVA

La presente propuesta normativa tiene como objetivo establecer un marco regulatorio claro y detallado para la externalización de servicios por parte de las compañías de seguros y reaseguros. Este marco busca asegurar que las compañías:

- Identifiquen y gestionen eficazmente los riesgos asociados a la externalización, incluyendo riesgos operacionales, estratégicos, reputacionales, de cumplimiento y de continuidad del negocio.
- Clasifiquen las actividades externalizadas según su criticidad y materialidad, considerando criterios cuantitativos y cualitativos, y apliquen controles proporcionales al impacto potencial en la organización.
- Implementen mecanismos robustos de supervisión y auditoría para garantizar la adecuada prestación de los servicios externalizados y el cumplimiento de las normativas vigentes.
- Aseguren la continuidad del negocio mediante planes propios de contingencia y la exigencia de que los proveedores y subcontratistas cuenten también con planes adecuados y probados frente a fallas en los servicios externalizados.
- Fortalezcan la seguridad de la información y la ciberseguridad, especialmente en servicios externalizados que manejan datos sensibles o críticos para la operación de la compañía.
- Incluyan cláusulas contractuales claras y exigibles, que definan niveles mínimos de servicio, condiciones de terminación anticipada de los contratos, acceso a la información, auditorías y otras garantías de control.
- Eviten y gestionen el riesgo de concentración y dependencia tecnológica, evaluando adecuadamente barreras de salida, propiedad de los datos, jurisdicción de procesamiento y alternativas de continuidad.
- Conserven la responsabilidad de la gestión de riesgos en la compañía, asegurando que la externalización no implique pérdida de control ni debilitamiento de los sistemas de gobierno y cumplimiento interno.
- Faciliten el acceso de la CMF a la información y operaciones externalizadas, incluyendo la supervisión remota o presencial en el extranjero, conforme a los requerimientos regulatorios establecidos.

III. DIAGNÓSTICO

En el marco de la adopción, planificación y desarrollo del modelo del Supervisión Basado en Riesgo en el mercado de seguros, la CMF emitió, en diciembre de 2011, la NCG N°325. Dicha norma establece instrucciones sobre el sistema de gestión de riesgos (SGR) de las compañías de seguros, basado en principios y buenas prácticas. En particular, para la gestión de riesgo operacional, establece una serie de aspectos que debería contemplar dicha gestión.

La norma señala que la aseguradora debe ser capaz de identificar las causas que generan los diferentes riesgos, su impacto en la compañía y las relaciones entre las distintas exposiciones, permitiéndole a la compañía identificar debilidades en sus sistemas operacionales, de gestión y de control y, a través de ello, perfeccionar sus procedimientos y técnicas para la administración de los riesgos.

No obstante lo anterior, se hacía necesario abordar aspectos adicionales y específicos incluidos en los principios y recomendaciones internacionales en materia de gestión de riesgo operacional y ciberseguridad.

En tal sentido, la CMF emitió, en mayo de 2021, la NCG N°454 que estableció los principios y conceptos de una correcta gestión del riesgo operacional y ciberseguridad, y la realización periódica de autoevaluaciones en ambas materias, por parte de las compañías de seguros.

Finalmente, en la hoja de ruta establecida por la CMF en relación con la gestión del riesgo operacional quedaba pendiente establecer una normativa que dictara los lineamientos que las compañías de seguros debieran considerar a la hora de externalizar servicios que involucren actividades significativas o estratégicas, lo que se establece en la presente propuesta normativa. Un ejemplo concreto de este tipo de actividades estratégicas, y con alta interacción sistémica, es el Sistema de Consultas y Ofertas de Montos de Pensión (SCOMP), utilizado tanto por las compañías de seguros que comercializan rentas vitalicias como por las Administradoras de Fondos de Pensiones (AFPs). La operación y correcta gestión de este sistema resulta fundamental para la transparencia, continuidad y estabilidad del proceso de jubilación de un número relevante de personas.

IV. EXPERIENCIA COMPARADA

1. Comisión para el Mercado Financiero, CMF.

La **RAN 20-7** establece el marco regulatorio para que las entidades financieras gestionen los riesgos asociados a la externalización de servicios. Dispone que la entidad contratante sigue siendo responsable de los procesos externalizados y que debe contar con políticas y procedimientos para la evaluación, selección, contratación, monitoreo y control de los proveedores. Requiere por parte de las entidades financieras la definición de actividades críticas o estratégicas, la mantención de un catastro actualizado, cláusulas contractuales claras, controles sobre subcontrataciones, y planes de continuidad del negocio tanto del proveedor, subcontratistas, como de la entidad.

También regula aspectos específicos como la seguridad de la información, el uso de servicios en la nube, las condiciones para la externalización con un proveedor internacional, y la obligación de asegurar el acceso de la CMF a la información procesada por terceros.

2. Office of the Superintendent of Financial Institutions, OSFI, Canadá.

En el caso de Canadá, el regulador integrado encargado de supervisar a las instituciones financieras, incluidas las compañías de seguros, es la Office of the Superintendent of Financial Institutions (OSFI). Este organismo ha emitido la **Guía B-10**, la cual establece expectativas prudenciales específicas para las entidades que externalizan funciones, procesos o actividades relevantes del negocio.
La guía enfatiza que las entidades mantienen la responsabilidad final por toda función externalizada, y que la OSFI no debe ver restringida su capacidad de supervisión por acuerdos de externalización con terceros.

El documento requiere, entre otros aspectos, que las entidades:

- Evalúen la materialidad de cada acuerdo de externalización.
- Implementen un programa de gestión de riesgos proporcional al nivel de criticidad del servicio.
- Desarrollen procesos de debida diligencia para seleccionar proveedores.
- Formalicen los acuerdos mediante contratos que incluyan medidas de continuidad del negocio, seguridad, auditoría, acceso a la información, y reglas sobre subcontratación.
- Monitoreen los servicios externalizados y mantengan una lista centralizada de los acuerdos materiales.

3. Australian Prudential Regulation Authority (APRA)

Por su parte, en Australia, la supervisión de las compañías de seguros recae en la Australian Prudential Regulation Authority (APRA), regulador encargado de velar por la estabilidad del sistema financiero. Esta autoridad ha establecido la norma prudencial **CPS 231**, que fija los lineamientos que deben seguir las instituciones reguladas al externalizar actividades de negocios materiales.
La norma exige que las entidades:

- Mantengan una política de externalización de servicios aprobada por el directorio.
- Realicen evaluaciones de materialidad y debida diligencia antes de externalizar.
- Formalicen los acuerdos con contratos legalmente vinculantes que regulen aspectos como la continuidad operativa, seguridad de la información, subcontratación, acceso de APRA y rescisión.
- Notifiquen a APRA tras firmar acuerdos y consulten previamente en caso de externalización internacional (offshoring).
- Monitoreen permanentemente el desempeño de los proveedores, incluyendo auditorías internas y reportes al directorio.

V. ANÁLISIS DE IMPACTO REGULATORIO

Efectos para las compañías de seguros y reaseguros

Impactos positivos:

- Fortalece la gestión del riesgo operacional y la administración de riesgos derivados de servicios tercerizados, dotando a las compañías de principios y criterios claros para la toma de decisiones.
- Mejora la resiliencia operativa al exigir planes de continuidad y controles específicos sobre los servicios externalizados.
- Contribuye a una mayor trazabilidad y claridad en las relaciones contractuales, garantizando que la supervisión interna y regulatoria pueda ejercerse de forma efectiva.
- La norma adopta un enfoque proporcional que permite ajustar las exigencias según el tamaño, complejidad y perfil de riesgo de cada entidad, minimizando impactos negativos en actores de menor escala.

Desafíos y costos asociados:

- Incremento en la carga operativa inicial para revisar y adecuar contratos, de ser necesario, establecer evaluaciones de materialidad, y gestionar relaciones con proveedores con nuevos estándares.
- Necesidad de invertir en capacitación, en el desarrollo de herramientas de monitoreo y en la actualización de políticas internas asociadas a la externalización.
- Costos relacionados con auditorías adicionales y mayor complejidad en la integración de controles de ciberseguridad y continuidad operativa.

Efectos para el regulador (CMF)

Beneficios esperados:

- Facilita una supervisión más proactiva y estandarizada, permitiendo identificar y evaluar con mayor precisión las exposiciones derivadas de la externalización.
- Refuerza la capacidad del regulador para exigir transparencia y acceso a la información relevante, lo que contribuye a una supervisión más eficaz.
- Potencia el enfoque de Supervisión Basada en Riesgo, ya que la CMF dispondrá de herramientas y criterios claros para monitorear los procesos de outsourcing y sus riesgos asociados.

Costos regulatorios potenciales:

- Se requerirá que la CMF desarrolle y fortalezca capacidades y herramientas internas especializadas para supervisar procesos de externalización complejos, en especial aquellos vinculados a tecnologías emergentes como, por ejemplo, computación en la nube (cloud computing).
- Podría incrementarse la carga de revisión y verificación de la información suministrada por las entidades supervisadas, lo que demandará mayores recursos en términos de personal y tecnología.

VI. PROYECTO NORMATIVO

REF: Imparte instrucciones en materia de externalización de servicios en el contexto de la gestión de riesgo operacional.

NORMA DE CARACTER GENERAL Nº BORRADOR

A todas las entidades aseguradoras y reaseguradoras

Esta Comisión, en uso de sus facultades legales, en especial lo dispuesto en el número 1 y 4 del artículo 5, el número 3 del artículo 20 y el número 1 del artículo 21 del DL N°3.538, de 1980, y la letra b) del artículo 3° del D.F.L. N°251, de 1931, y lo acordado por el Consejo de la Comisión para el Mercado Financiero en Sesión Ordinaria N° XX del XX de XX de 2025, ha resuelto impartir las siguientes instrucciones relativas al sistema de gestión del riesgo operacional, en lo referido a la externalización de servicios por parte de las entidades aseguradoras y reaseguradoras.

I. Introducción

La externalización de actividades, funciones o procesos se ha convertido en una práctica habitual dentro del mercado asegurador, asociada a la búsqueda de mayor eficiencia operativa, incorporación de tecnologías especializadas y mayor flexibilidad organizacional. No obstante, esta práctica también puede dar lugar a una exposición significativa a distintos tipos de riesgo, en particular al riesgo operacional, así como a riesgos de cumplimiento y reputacionales, entre otros.

Esta norma se enmarca en la implementación de un modelo de Supervisión Basada en Riesgo promovido por la Comisión para el Mercado Financiero (CMF) y, se fundamenta en los principios de gestión prudencial establecidos en la Norma de Carácter General N°309 sobre Gobierno Corporativo, la NCG N°325 sobre sistemas de gestión de riesgos y la NCG N°454 sobre gestión de riesgo operacional y ciberseguridad.

En concordancia con los mencionados cuerpos normativos, la presente norma establece los principios y requisitos mínimos que deberán observar las compañías a la hora de identificar, evaluar, monitorear y controlar los riesgos derivados de la externalización de servicios.

Entre otros elementos, la norma considera criterios para la evaluación de la materialidad y criticidad de los servicios externalizados, lineamientos sobre los procesos de selección y contratación de proveedores, requisitos contractuales mínimos, medidas para la gestión de subcontrataciones, así como la necesidad de incorporar los servicios externalizados en los planes de continuidad del negocio y en los mecanismos de ciberseguridad. Además, se refuerzan las exigencias de trazabilidad y transparencia en la relación con los proveedores, asegurando que la CMF mantenga, en todo momento, la capacidad de acceder a la información relevante para el cumplimiento de su rol supervisor.

II. Ámbito de Aplicación.

1. Alcance de la presente norma.

La presente norma se refiere a las contrataciones por parte de las compañías de seguros con proveedores de servicios externos, mediante las cuales se encomienda a terceros la realización de una o más actividades operativas que, en principio, podrían ser efectuadas directamente por la compañía con sus propios recursos, tanto humanos como tecnológicos.

En consecuencia, las disposiciones de esta normativa no son aplicables a aquellos servicios que una compañía no puede proveerse a sí misma, tales como los servicios básicos o aquellos donde una ley ha definido que deben ser prestados por entidades de giro exclusivo.

A su vez, la presente norma no contempla como actividades posibles de externalización las vinculadas a funciones de control al interior de la compañía.

Asimismo, debe tenerse en consideración que conforme a lo prescrito en el artículo 40 de la Ley N°18.046, las actividades encomendadas a terceros deben atender a la realización de objetos específicos especialmente determinados. En tal sentido, en ningún caso podrá externalizarse la ejecución de aquellas actividades respecto de las cuales una ley o cuerpo normativo aplicable disponga expresamente que deben ser realizadas directamente por la compañía o a través de terceros expresamente autorizados para dicho efecto.

En todo caso, dichos servicios deberán ser considerados por las compañías dentro de sus procesos de evaluación y gestión de riesgos en conformidad con lo establecido en el numeral 2.5 del capítulo III de la NCG N°325 y en la NCG N°454.

2. Definiciones.

Externalización de servicios (*Outsourcing*): es la ejecución por un proveedor externo de servicios o actividades en forma continua u ocasional, las que normalmente podrían ser realizadas directamente por la compañía contratante.

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

Cadenas de servicios externalizados: Son aquellas formadas por terceros subcontratados por el proveedor inicial de servicios para realizar parte importante de las actividades contratadas con éste (subcontrato de otros proveedores).

Persona relacionada: Se entenderá por persona relacionada lo definido en el artículo 100 de la ley N°18.045 y aquellas en que deba intervenir la sociedad y alguna de las personas señaladas en los numerales del artículo 146 de la Ley N°18.046.

Servicios en la nube (*cloud computing*): modelo de prestación de servicios configurable según demanda, para la provisión de servicios asociados a las tecnologías de la información a través de redes, basado en mecanismos técnicos como la virtualización, bajo diferentes enfoques o estrategias de suministro.

Nube Privada: infraestructura de nube provista para el uso exclusivo de una entidad, comprendiendo múltiples usuarios (por ejemplo, unidades comerciales). Puede ser de propiedad, administración y operación de la misma entidad, de un tercero o una combinación de ambos; y puede encontrarse tanto dentro como fuera de las instalaciones del contratante.

Nube Pública: infraestructura de nube provista para el uso de varias entidades. La infraestructura pertenece a un proveedor que otorga servicios de nube, y es administrada y operada por éste. Esta infraestructura se encuentra en las instalaciones del proveedor de nube.

Actividades significativas o estratégicas (críticas):

i. Actividades o servicios que al verse afectadas por una deficiente gestión pueden generar riesgos relevantes, tales como de seguridad o continuidad o riesgos de proceso, entre otros. Estas van a depender del modelo de negocio de cada entidad.

ii. Aquellas actividades de alta interacción sistémica en el mercado. Esto significa actividades cuya deficiente gestión puede tener un impacto más allá de la entidad individual, es decir, son actividades que tienen interconexiones o interdependencias relevantes con otros actores del mercado.

Infraestructura tecnológica: Conjunto de hardware y software que requiere una entidad para realizar las actividades necesarias para ejercer su giro.

Infraestructura de seguridad de la información: Conjunto de hardware y software dispuesto para resguardar la seguridad de la información, en particular en el ámbito de la Ciberseguridad.

III. Adecuada gestión de riesgos de la Externalización de Servicios.

Una sólida gestión de riesgos se basa en la existencia de una adecuada estructura de gobierno, un marco con políticas, normas y procedimientos, así como un entorno que permita identificar, evaluar, controlar, mitigar, monitorear y reportar los riesgos más relevantes asociados al outsourcing de actividades, proceso que en el caso del riesgo operacional debe cumplirse en concordancia con lo indicado en el numeral 2.5 del capítulo III de la NCG N°325 y en lo señalado por la NCG N°454.

Dentro de las evaluaciones de riesgo deben considerarse aquellos que se generan como consecuencia de la concentración de compañías de seguros u otras entidades financieras en un proveedor, ya que ante una eventual falla de éste, se podría generar una crisis a nivel de la industria; cuando se entreguen varias actividades significativas a un mismo proveedor; y al cuando se externalicen servicios en proveedores que generen barreras altas de salida, especialmente en términos de dependencia de la infraestructura tecnológica contratada, la posible pérdida de la pericia técnica interna, la localización de los datos y la propiedad de los mismos. Las compañías deben definir de manera fundada los criterios de concentración y barreras de salida.

IV. Condiciones que deben cumplirse en la Externalización de Servicios.

La compañía que decida externalizar alguna actividad, además de considerar los aspectos indicados en el Anexo N°1 para fines de la contratación de cada servicio en particular, debe dar cumplimiento a las siguientes condiciones:

1. Condiciones generales.

a) El Directorio, o quien haga sus veces, deberá pronunciarse sobre la tolerancia o el apetito al riesgo que está dispuesto a asumir en el caso de externalizar servicios.

b) Mantener una política debidamente aprobada por el Directorio, que regule las actividades asociadas a la externalización. Esta política debe pronunciarse, al menos, respecto de los elementos indicados en el N°2 siguiente.

c) Verificar que el proveedor cuenta con mecanismos que permitan prevenir que acciones realizadas por otros clientes afecten negativamente el servicio externalizado por la compañía.

d) Establecer procedimientos formales para la selección, contratación y monitoreo de proveedores.

e) Velar por que el proveedor y el personal a cargo de los servicios contratados posean adecuados conocimientos y experiencia en la actividad que se está externalizando. Asimismo, también deberá vigilar el debido cumplimiento de aquellos aspectos regulatorios y legales que pudiesen afectar la provisión de los servicios contratados (ej. leyes laborales).

f) Mantener un catastro actualizado de todos los servicios contratados con empresas externas, determinando claramente aquellos que, a su juicio, son estratégicos y de alto riesgo, de manera de establecer procedimientos de control y seguimiento en forma permanente de acuerdo con los niveles de criticidad que les asigne.

g) Establecer procedimientos que aseguren el cumplimiento oportuno y cabal de los compromisos que tiene con sus asegurados.

h) Velar por que existan auditorías independientes al proceso de selección, contratación y seguimiento de los proveedores, con personal especialista en los distintos riesgos auditados.

i) Asegurar que el proveedor realice periódicamente informes de auditoría interna o revisiones independientes de sus servicios, conforme con su estructura y el tamaño de su organización, debiendo compartir oportunamente con la compañía los hallazgos que le sean pertinentes.

j) Exigir a los proveedores de servicios que los procedimientos operacionales, administrativos y tecnológicos propios del servicio contratado, se encuentren debidamente documentados, actualizados y permanentemente a disposición de la compañía, la que deberá asegurar su disponibilidad para su revisión por parte de esta Comisión.

k) Considerar los riesgos que provienen de las cadenas de servicios externalizados, lo que debe quedar reflejado en el contrato respectivo en forma previa, señalándose que, en caso de subcontratación, la empresa subcontratada debe cumplir también con las condiciones pactadas entre la compañía y el proveedor de servicios inicial. Asimismo, deben quedar claramente establecidos, en los respectivos contratos, las responsabilidades y obligaciones que deben cumplir las empresas subcontratadas respecto del servicio externalizado por la compañía.

l) La compañía debe incorporar en sus reportes de riesgo operacional que elabora para el Directorio, o para quien haga sus veces, información respecto de la gestión que realiza la compañía para administrar los riesgos de externalización, incluyendo los cambios en el perfil de riesgos de los proveedores (como, por ejemplo, cambios relevantes en sus procesos y áreas geográficas de donde se prestan los servicios) y la exposición a aquellos servicios considerados críticos.

m) Los datos, plataformas tecnológicas y aplicaciones a utilizar en la externalización de los servicios deben encontrarse en sitios de procesamiento específicos y, para el caso de procesamiento en el extranjero, en una jurisdicción definida y conocida. Además de la jurisdicción, se debe conocer la ciudad donde operan los centros de datos.

n) Inclusión de niveles mínimos de servicios en los contratos, y acceso a información suficiente para hacer monitoreo continuo de los niveles de servicios.

2. Política de contratación y gestión de actividades relativas a la externalización de servicios

La política que corresponde ser sancionada por el Directorio de la compañía, debe abordar al menos las siguientes materias:

a) La definición de la estructura de gobierno y de los procedimientos a seguir para autorizar y gestionar la externalización de servicios, incluyendo las líneas de reporte y de responsabilidad.

b) La descripción de las herramientas específicas de evaluación de riesgos en esta materia y de su utilización.

c) Criterios para definir los umbrales o límites permitidos o de tolerancia o apetito al riesgo inherente y residual, así como los instrumentos y estrategias de mitigación y monitoreo.

d) Evaluación de materialidad del servicio a externalizar, la cual dependerá del potencial que tenga de influir, ya sea cuantitativa o cualitativa, en una línea de negocio significativa de las operaciones de la compañía.

e) Criterios particulares de contratación, cuando se trate de un proveedor que sea una entidad relacionada.

f) Elementos que serán considerados por la compañía para determinar aquellos servicios que, a su juicio, se encuentran asociados con actividades significativas o estratégicas.

g) La definición de aquellas actividades que solo pueden externalizarse previa aprobación del Directorio o de otra instancia de la administración que se defina.

h) Periodicidad de revisión de la política, especialmente cuando existan cambios relevantes en el perfil de riesgo de la compañía.

i) Los elementos mínimos que deberá incorporar el contrato de prestación de servicios.

j) Definición de los elementos relacionados a la gestión de riesgo que no les sean aplicables a cierto tipo de actividades o servicios que se realicen localmente, de acuerdo con lo dispuesto en el Anexo N°2.

3. Evaluación de materialidad

Toda compañía que decida externalizar una actividad deberá realizar una evaluación de materialidad de dicha actividad, la cual, como se mencionó anteriormente, dependerá del potencial que tenga de influir, ya sea cuantitativa o cualitativamente, en una línea de negocio significativa o estratégica de las operaciones de la compañía. Por lo tanto, la compañía deberá realizar una evaluación de los riesgos operacionales y su impacto en la continuidad del negocio asociado a dicha actividad.

Todas las actividades significativas o estratégicas (críticas), ya sea debido a su impacto significativo en la continuidad del negocio, el cumplimiento normativo, la seguridad de la información y la estabilidad del mercado, deben ser consideradas como materiales en la evaluación de externalización.

Por lo tanto, para efectos de control y monitoreo, las compañías deben clasificar las actividades externalizadas en función de su criticidad y materialidad, asegurando que cuenten con medidas reforzadas de supervisión, auditoría y continuidad del negocio.

La evaluación de materialidad de una actividad es a menudo subjetiva y depende de las circunstancias que enfrenta una compañía individual. Sin limitar el alcance de la evaluación de materialidad, los factores que la compañía debe considerar incluyen:

a) El impacto del acuerdo de externalización en los resultados, en la reputación y en las operaciones de la compañía, o en una línea de negocio significativa, particularmente si el proveedor de servicios, o un grupo de proveedores de servicios, no cumplen con su desempeño durante un período de tiempo determinado;
b) La capacidad de la compañía para mantener controles internos apropiados y cumplir con los requisitos regulatorios, especialmente si el proveedor de servicios experimentara problemas;

c) El costo del acuerdo (contrato) de externalización en relación con los costos totales;

d) El grado de dificultad y el tiempo requerido para encontrar un proveedor de servicios alternativo o para llevar la actividad comercial "internamente"; y

e) El potencial de que múltiples acuerdos de externalización proporcionados por el mismo proveedor de servicios puedan tener en conjunto una influencia importante en la compañía.

El anexo N°3 contiene preguntas específicas que una compañía podría considerar en la evaluación de materialidad de las actividades a externalizar.

Cambios significativos en el volumen o la naturaleza del negocio realizado deberían hacer que la compañía reevalúe la materialidad de una o más actividades. En los casos en que una o más actividades se reevalúen como materiales, deben cumplir con todas las directrices establecidas en esta normativa.

4. Proceso de debida diligencia

4.1 Consideraciones generales

La CMF espera que las compañías realicen una debida diligencia interna para determinar la naturaleza y el alcance de la actividad que se va a externalizar, su relación con el resto de las actividades de la compañía y cómo se gestiona la actividad.

Al seleccionar un proveedor de servicios, o al enmendar sustancialmente o renovar un contrato o acuerdo de externalización, se espera que las compañías lleven a cabo un proceso de debida diligencia que evalúe completamente los riesgos asociados con el acuerdo de externalización y aborde todos los aspectos relevantes del proveedor de servicios, incluidos los factores cualitativos (operativos) y cuantitativos (financieros).

Cuando se contemple la externalización fuera del país, las compañías deben prestar especial atención a los requisitos legales de esa jurisdicción, así como a las posibles condiciones y eventos políticos, económicos y sociales que puedan conspirar para reducir la capacidad del proveedor de servicios extranjero para proporcionar el servicio, así como a cualquier factor de riesgo adicional que pueda requerir un ajuste al programa de gestión de riesgos.

Los procesos de debida diligencia variarán según la compañía y la naturaleza del acuerdo de externalización que se esté contemplando. Por ejemplo, en el caso de renovaciones donde no ha ocurrido ningún cambio material que afecte la viabilidad de la relación de externalización, puede ser apropiado realizar una debida diligencia más simplificada.

4.2 Proceso de debida diligencia reforzada para servicios en la nube

La computación en la nube o *cloud computing* engloba la evolución de varios ámbitos de las tecnologías de la información, tales como las redes de telecomunicaciones y los microprocesadores, siendo la virtualización o abstracción del *hardware* una de las más relevante. Por la variedad de servicios que es posible acceder a través de la nube, como de infraestructura, plataforma o incluso de *software*, se advierte una modificación en la dinámica de los riesgos asociados a los actuales modelos tecnológicos aplicados en el mercado asegurador.

Para efectos de contratar cualquier tipo de servicio a través de la modalidad denominada nube, el Directorio de la compañía deberá pronunciarse anualmente sobre la tolerancia o apetito al riesgo que está dispuesto a asumir en este tipo de externalizaciones. Este pronunciamiento deberá considerar un análisis de los datos a almacenar o procesar bajo esta modalidad y su ubicación.

Sin perjuicio del debido cumplimiento de los distintos requerimientos contenidos en esta norma, las compañías podrán externalizar en la nube pública o privada sus servicios no críticos sin consideraciones adicionales a las ya mencionadas en los títulos precedentes.

En el evento que la compañía evalúe la contratación de un servicio en la nube para una actividad considerada estratégica o crítica, este también podrá ser efectuado en modalidad de nube pública o privada. No obstante, en estos casos la compañía deberá realizar una diligencia reforzada del proveedor y del servicio, que al menos considere lo siguiente:

a) El proveedor dispone de reconocido prestigio y experiencia en el servicio que otorga.

b) El proveedor contratado cuenta con certificaciones independientes, reconocidas internacionalmente, en términos de gestión de la seguridad de la información, la continuidad del negocio y la calidad de servicios que recojan las mejores prácticas vigentes.

c) Los contratos de externalización de servicios son celebrados directamente entre la compañía contratante y los proveedores, con la finalidad de minimizar los riesgos que podría aportar el rol de intermediarios en este tipo de servicios.

d) La compañía cuenta con informes legales respecto de la regulación sobre privacidad y acceso a la información existentes en jurisdicciones donde se esté llevando a cabo el servicio, y ha evaluado la resolución de contingencias legales en las jurisdicciones en las que opere.

e) La compañía se ha asegurado que el proveedor del servicio realiza informes de auditoría asociados a los servicios prestados y dichos informes se encuentran disponibles, para ser consultados en cualquier momento por la compañía contratante y esta Comisión, en las materias que resulten pertinentes.

f) Verificar que el proveedor cuenta con adecuados mecanismos de seguridad, tanto físicos como lógicos, que permitan aislar los componentes de la infraestructura nube que la compañía comparte con otros clientes del proveedor, de manera de prevenir fugas de información o eventos que puedan afectar la confidencialidad e integridad de los datos de la compañía.

g) Identificar los datos que, por su naturaleza y sensibilidad, deben contar con mecanismos fuertes de encriptación.

5. Plan de continuidad del negocio.

La compañía debe verificar que sus proveedores de servicios críticos cuenten con planes apropiados que aseguren la continuidad de los servicios contratados. De igual forma la compañía debe verificar que sus proveedores críticos se aseguran de que los servicios subcontratados por estos cuentan con apropiados planes de continuidad del negocio. Esos planes deben ser probados al menos una vez al año, debiendo la compañía tomar conocimiento de dicha actividad y verificar los resultados obtenidos. Adicionalmente, la compañía también debe disponer de planes, igualmente probados, para asegurar la continuidad operacional ante la contingencia de no contar con dicho servicio externo.

La compañía debe contar con planes de salida en el evento de incumplimientos de dichos proveedores, que consideren el término anticipado de la relación contractual y que permitan retomar la operación, ya sea por cuenta propia o mediante otro proveedor.

La compañía debe asegurarse que el proveedor cuente con un proceso formal y sistemático de gestión frente a los incidentes que pudieran interrumpir o afectar la provisión de los productos, servicios o actividades.

El plan de continuidad y los sistemas de respaldo deben ser proporcionales al riesgo de una interrupción del servicio. En particular, el plan de continuidad del negocio debe asegurar que la compañía tenga en su posesión, o pueda acceder fácilmente, a todos los registros necesarios para permitirle mantener las operaciones, cumplir con sus obligaciones legales y proporcionar toda la información que pueda ser requerida por la CMF para cumplir con su mandato, en caso de que el proveedor de servicios no pueda prestar el servicio.

6. Seguridad de la información propia y de sus asegurados, en los casos que corresponda.

La compañía debe cerciorarse que el proveedor del servicio mantiene un programa de seguridad de la información que le permita asegurar la confidencialidad, integridad, trazabilidad y disponibilidad de sus activos de información y la de sus clientes. Estas condiciones deben ser consistentes con las políticas y estándares adoptados por la compañía y quedar incorporadas en el contrato de prestación de servicios.

La compañía debe controlar y monitorear la infraestructura de seguridad de la información dispuesta por el proveedor, con el objeto de proteger los activos de información presentes en los servicios críticos externalizados, independiente de los controles dispuestos por el proveedor. De igual forma, debe controlar y monitorear la gestión de identidades y control de accesos a la información referida a dichos servicios críticos.

Las conexiones de comunicaciones entre la compañía contratante y el proveedor de servicios deben contar con un nivel de cifrado que asegure la confidencialidad y la integridad de los datos de punta a punta (*end to end*).

La compañía debe asegurarse que el proveedor disponga de medidas efectivas de control y protección sobre ataques externos que persigan la indisponibilidad de los servicios contratados, como, por ejemplo, los de denegación de servicios. Adicionalmente, para los servicios críticos externalizados, la compañía deberá controlar la realización periódica por parte del proveedor de evaluaciones de vulnerabilidad de su infraestructura tecnológica y testeos de penetración.

La información, una vez procesada, debe ser almacenada y transportada en forma encriptada, manteniéndose las llaves de desencriptación en poder de la compañía. Asimismo, se deben definir los procedimientos de intercambio de claves entre el proveedor de servicios y la compañía, además de establecerse los roles y responsabilidades de las personas involucradas en la administración de la seguridad.

En el caso del procesamiento de la documentación física, la compañía deberá contar con procedimientos de control que vele por el debido cumplimiento de las condiciones señaladas en este Título. Junto a lo anterior, se deben establecer los procedimientos que aseguren el adecuado traspaso de información a la compañía por parte del proveedor y que éste, en ningún caso, mantenga información en su poder después de finalizada la relación contractual.

7. Riesgo país.

Sólo se podrá externalizar servicios en jurisdicciones que cuenten con calificación de riesgo país en grado de inversión. No obstante, el Directorio o la instancia que haga sus veces podrá excepcionar este requisito, en la medida que el país en el que se externalizan los servicios cuente con leyes de protección y seguridad de datos personales adecuadas, debiendo dejar constancia formal del análisis realizado al efecto.

8. Responsabilidad por la gestión.

La compañía deberá mantener la responsabilidad por la gestión global de los riesgos y funciones de control en el país. Lo anterior es sin perjuicio que en algunas entidades internacionales existan, para efectos de una administración consolidada por parte de sus casas matrices, coordinaciones matriciales entre el personal establecido en el extranjero y el personal local.

Por otra parte, en cumplimiento de lo dispuesto en el capítulo VI de la NCG N°454, la compañía deberá comunicar a esta Comisión, en los términos definidos en dicho Capítulo, los incidentes operacionales que afecten un servicio externalizado en el país o en el exterior.

9. Acceso a la información por parte del supervisor.

La compañía contratante debe asegurarse que esta Comisión tenga acceso permanente, sea mediante visitas a las instalaciones de los proveedores de servicios o por vía remota, a todos los registros, datos e información que se procesen, mantengan y generen a través de un proveedor externo, ya sea establecido en el país o en el exterior.

Al tratarse de un proveedor de servicios establecido en el exterior, deberá prestarse especial atención a las restricciones legales del país anfitrión que pudieren impedir la visita de esta Comisión al proveedor o el acceso a la información y a los datos mencionados en el párrafo anterior.

10. Servicios externalizados en el extranjero

En el caso de que la compañía externalice servicios fuera del país, deberá disponer en todo momento de los antecedentes de la empresa contratada. En especial, deberá mantener aquellos antecedentes que respalden la solidez financiera del proveedor del servicio y que éste mantiene certificaciones de calidad, seguridad y apropiados sistemas de control.

La compañía debe disponer de los antecedentes del proyecto, del contrato de servicios y, en caso de existir subcontratos con terceros, estos también deben ser incorporados.

La compañía debe efectuar el control y monitoreo del servicio externalizado en el exterior, especialmente, en los aspectos relacionados con la seguridad de la información, continuidad del negocio y condiciones de operación del centro de procesamiento de datos. Dichas actividades deben estar debidamente fundamentadas de acuerdo con la gestión de riesgos realizada para el proveedor específico. Lo anterior, independientemente de las actividades propias de control y monitoreo que realice el proveedor del servicio.

Adicionalmente, el sistema de gestión de riesgos de la compañía debe incorporar cualquier preocupación adicional relacionada con el entorno económico y político, la sofisticación tecnológica y el perfil de riesgo legal y regulatorio de la(s) jurisdicción(es) extranjera(s).

V. Revisiones de esta Comisión

Esta Comisión podrá requerir que los servicios se realicen en el país, o sean ejecutados internamente por la compañía, según corresponda. En consideración a lo anterior, la compañía deberá mantener permanentemente actualizado un plan que posibilite cumplir con esos eventuales requerimientos.

SOLANGE BERSTEIN JÁUREGUI
PRESIDENTA
COMISIÓN PARA EL MERCADO FINANCIERO

Anexo N°1

Aspectos mínimos que deben considerarse para la externalización de servicios

1. Evaluación del riesgo.

Antes de decidir la externalización de una actividad, se debe efectuar una evaluación, que considere la participación de todos los agentes involucrados, respecto de los riesgos que esta decisión incorpora a la compañía, así como la cantidad de riesgo comprometido en razón de los montos pagados a la empresa externa, volumen de transacciones que se procesará, criticidad del servicio contratado, concentración de servicios con el mismo proveedor, concentración del sector financiero en un proveedor específico, entre otros.

En esta evaluación se debe considerar la opinión del área encargada de la gestión del riesgo operacional de la compañía fiscalizada, la que deberá encontrarse debidamente sustentada.

2. Selección del proveedor de servicios.

La compañía debe evaluar las propuestas recibidas de acuerdo con sus requerimientos y llevar a cabo un proceso de *debida diligencia* que sustente la información recibida de los posibles proveedores.

En el caso de que se contrate un servicio con una entidad relacionada, las condiciones económicas deben cumplir con principios de transparencia y equidad, aspectos que deben estar definidos en la política que regula la externalización de servicios.

3. Contrato.

La compañía debe asegurarse que el contrato defina claramente los derechos y obligaciones de ambas partes, conteniendo acuerdos de niveles claros y medibles de los servicios contratados, cláusulas de término anticipado de la relación contractual, así como también un método de fijación de precios adecuado para el contrato específico. En caso de que se adquiera más de un servicio por un precio único, debe tenerse el detalle del cobro por cada uno de tales servicios.

También se deben incluir cláusulas de continuidad del negocio y de seguridad de la información, especialmente aquella que se refiere a la propiedad y confidencialidad de la información, tanto propia como de sus clientes; restricciones sobre el uso de *software*; eliminación segura de los datos del cliente, cuando corresponda; además indicar claramente donde operan los centros de datos y establecer una autorización permanente que permita tanto a esta Comisión como a la compañía fiscalizada examinar *in situ*, o en forma remota, según se disponga, en cualquier momento, todos los aspectos relacionados con el servicio contratado.

Adicionalmente, la compañía deberá considerar cláusulas de veto en la selección de subcontratación de terceros por parte del proveedor principal.

Contractualmente debe quedar claramente establecido todo lo relacionado con la idoneidad y responsabilidad del personal de la empresa proveedora del servicio, así como también todos los aspectos legales y laborales que imperen en el país o en el extranjero, aplicables a estas contrataciones.

Por último, todos los contratos, subcontratos y sus respectivos anexos, deberán estar en idioma español, o bien traducidos a este idioma, y con las correspondientes rúbricas de las partes.

4. Control permanente.

Del proveedor: La compañía debe controlar el desempeño del proveedor y los posibles cambios en los requerimientos de la compañía durante la vigencia del contrato. El control debe comprender como mínimo: el conocimiento y análisis del último estado financiero del proveedor y aspectos tales como la observación del entorno de control general de la empresa externa.

Del servicio: La compañía debe contar con procedimientos que le permitan controlar el cumplimiento de las cláusulas estipuladas en los contratos. El monitoreo debe comprender al menos: acuerdos de niveles de servicios, disposiciones contractuales, gestión del riesgo operacional asociado al servicio contratado y posibles cambios a causa del entorno externo. Adicionalmente, se debe evaluar y probar, al menos anualmente, la existencia y suficiencia de los procedimientos de traspaso a producción y escalamiento de incidentes; así como definir y controlar los hitos relevantes de cada uno de estos servicios.

Anexo N°2

Externalización de servicios no estratégicos

El Directorio debe definir qué elementos de esta norma no serán aplicables a aquellos servicios contratados en el país, que comúnmente se vinculan con actividades que no tienen un carácter estratégico, material o sus riesgos son más acotados.

A continuación, a manera de referencia, se enumeran algunas categorías de servicios y actividades que podrían cumplir con dichas condiciones:

i. Servicios Generales: tales como vigilancia, limpieza, mantenimiento y reparaciones, mensajería, servicios públicos, entre otros.

ii. Actividades de apoyo administrativo: pago de sueldos, compras, facturación, capacitación, selección de personal, entre otros.

iii. Actividades de investigación de mercado y marketing: encuestas de productos y servicios, antecedentes de clientes y publicidad, entre otros.

    En cuanto a la comercialización de las pólizas de seguro ésta debe realizarse directamente por la compañía o a través de agentes de venta o corredores de seguros.

iv. Otros: Servicios de arrendamiento.

Sin perjuicio de lo señalado, para estas actividades la compañía deberá velar por el debido cumplimiento de cualquier aspecto legal o regulatorio que ponga en riesgo la adecuada provisión del servicio como, por ejemplo, las leyes laborales.

Asimismo, dependerá de cada compañía establecer las condiciones que deben ser ponderadas antes de exceptuar a un servicio o actividad de alguna de las medidas de gestión de riesgo de que trata esta norma, de acuerdo con las características particulares de cada compañía.

Anexo N°3

Preguntas tipo para la evaluación de materialidad

En la evaluación de materialidad de una actividad específica, la compañía puede considerar, entre otras, las siguientes preguntas:

1. Relación con el negocio principal

    - ¿Cuál es la relación entre la actividad externalizada y el negocio principal de la compañía?

2. Impacto potencial en áreas claves

    - ¿Cuál es el impacto potencial de la actividad en las ganancias, la solvencia, la liquidez, el financiamiento, el capital y otros indicadores financieros de la compañía?

    - ¿Qué impacto podría tener sobre la reputación de la compañía, la experiencia interna y las capacidades operativas de la compañía, el valor de la marca y el sistema de control interno?

3. Alineación con los objetivos y la estrategia de la compañía

    - ¿En qué medida esta actividad es relevante para el logro e implementación de los objetivos comerciales, la estrategia de negocio y los planes de corto y largo plazo de la compañía?

4. Exposición a proveedores de servicios

    - ¿Cuál es la exposición agregada de la compañía a un proveedor de servicios especifico?

    - ¿Está la compañía expuesta a un riesgo adicional de externalización debido a la concentración de acuerdos con un mismo proveedor?

5. Volumen de los compromisos contractuales

    - ¿Cuál es el tamaño de los gastos contractuales como parte de los gastos no relacionados con intereses de la compañía o de la línea de negocio?

6. Riesgos ante la incapacidad de cumplimiento por parte de un proveedor para entregar los servicios comprometidos.

    - En caso de que un proveedor de servicios no pueda cumplir con su compromiso durante un período de tiempo determinado, la compañía deberá evaluar:

        - ¿Cuál sería el impacto esperado sobre los servicios entregados?

        - ¿Cómo afectaría esto a la reputación de la compañía?

        - ¿Tendría un impacto material en el perfil de riesgo de la compañía?

        - ¿Cómo afectaría esto a la continuidad del negocio?

        - ¿La compañía podría contratar en tiempo y forma un proveedor de servicios alternativo?

        - ¿Cuánto tiempo y recursos, tanto financieros como operativos, serían necesarios para hacer frente a esta contingencia?

COMISIÓN
PARA EL MERCADO
FINANCIERO

REGULADOR Y SUPERVISOR FINANCIERO DE CHILE

www.cmfchile.cl