COMISIÓN PARA EL MERCADO FINANCIERO

Regulador y Supervisor Financiero de Chile

Informe Normativo

Norma de Externalización de Servicios en Compañías de Seguros y Reaseguros

Agosto 2026

www.CMFChile.cl

Contenido

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 en entidades aseguradoras y reaseguradoras, así como la realización periódica de autoevaluaciones en dichas materias.

En este 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 aseguradoras y reaseguradoras para identificar, evaluar, monitorear y controlar los riesgos derivados de la externalización de servicios.

En particular, la norma establece principios y lineamientos para la gestión de riesgos en la externalización de servicios por parte de compañías de seguros y reaseguros. Incluye directrices sobre los procesos de selección y contratación de proveedores, requisitos contractuales mínimos tales como cláusulas de continuidad del negocio, seguridad de la información y niveles de servicio, así como medidas para la gestión de subcontrataciones. Además, requiere incorporar los servicios externalizados en los planes de continuidad operativa y en los mecanismos de ciberseguridad, reforzando la trazabilidad, la transparencia y el acceso a la información por parte de la CMF.

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 CMF a la información relacionada con los servicios externalizados recae sobre la compañía de seguros o reaseguros, 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 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 significancia[1], considerando criterios cuantitativos y cualitativos, y apliquen controles proporcionales al impacto potencial en la organización.
- Implementen mecanismos de supervisión y auditoría proporcionales al perfil de riesgo del servicio externalizado, para velar por 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 el requerimiento de que los proveedores y subcontratistas cuenten también con planes 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, en consistencia con la Ley N°21.719 sobre Protección de Datos Personales y la Ley N°21.663, Ley Marco de Ciberseguridad.[2]
- Incluyan cláusulas contractuales que definan niveles mínimos de servicio, condiciones de terminación anticipada de los contratos, acceso a la información, auditorías y otras garantías de control, reconociendo los resguardos alternativos aplicables en contratos de adhesión.
- Gestionen el riesgo de concentración y dependencia tecnológica, evaluando adecuadamente barreras de salida, propiedad de los datos, jurisdicción de procesamiento y alternativas de continuidad.[3]
- Conserven la responsabilidad última e indelegable 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 de las operaciones externalizadas, canalizado a través de la propia compañía como responsable última de garantizar dicho acceso.

---

[1] Modificado en normativa definitiva para consistencia con los términos de actividades significativas o principales.

[2] Modificado tras la segunda consulta pública considerando los nuevos marcos legales que se indican.

[3] Modificado en normativa definitiva para ajuste de términos de la normativa definitiva.

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.

IV. EXPERIENCIA COMPARADA

1. Comisión para el Mercado Financiero, CMF

El Capítulo **20-7** de la RAN de bancos 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 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 del año 2023, 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 del año 2017**, 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 (REVISADO POR NORMA DEFINITIVA)

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 y gestionar relaciones con proveedores con nuevos estándares. No obstante, la norma adopta un enfoque basado en Principios, correspondiendo a cada compañía definir los criterios específicos en su política de externalización conforme al principio de proporcionalidad. Este carácter gradual se ve reforzado por el plazo de entrada en vigencia diferido de un año y las reglas de transitoriedad, que permiten adecuar los contratos vigentes en la primera oportunidad disponible.
- 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. Con todo, en aplicación del principio de proporcionalidad, corresponde a cada compañía determinar la frecuencia, el alcance y la profundidad de dichas auditorías en función de la criticidad del servicio y del perfil de riesgo del proveedor, las que podrán ser ejecutadas por personal interno o por entidades externas, lo que permite moderar estos costos.

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 externalización de servicios 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. COMENTARIOS DE LA PRIMERA CONSULTA PÚBLICA

El 14 de agosto de 2025 la CMF dio inicio al proceso de consulta pública de la propuesta normativa, contenida en el Informe normativo puesto en consulta, que imparte instrucciones en materia de Externalización de Servicios en el contexto de la Gestión de Riesgo Operacional.

Los comentarios a la propuesta normativa se recibieron hasta el 30 de septiembre de 2025. En total se recibieron 14 documentos con comentarios, los cuales de desglosan de la siguiente forma:

- Compañías de seguros: 11.
- Asociaciones gremiales: 2.
- Personas naturales: 1.

El resumen de los principales comentarios recibidos y las respuestas de la CMF a los mismos, se presentan a continuación:

1. **Comentario:** Se solicita un plazo de implementación gradual de 1 a 2 años que permita la adecuación de los contratos vigentes.

Respuesta CMF: Se establece vigencia diferida de 1 año desde la publicación de la normativa con el objetivo de que las compañías puedan adecuar sus procesos de gestión a los lineamientos establecidos en la norma.

2. **Comentario:** En la sección "Consideraciones generales" se propone reemplazar el término "verificar" por "realizar una debida diligencia" en lo relacionado a la verificación de los proveedores por parte de las compañías de seguros, puesto que las aseguradoras no tienen facultades ni medios técnicos para comprobar mecanismos internos de los proveedores.

   Respuesta CMF: Se ajusta la redacción de esta sección, estableciéndose criterios generales que deben ser considerados por las compañías en los procesos de externalización de servicios, precisando que éstas, deben velar por el cumplimiento de los criterios establecidos.

3. **Comentario:** La facultad de la CMF de exigir que ciertos servicios se realicen en Chile o internamente podría reducir la competencia, excluir proveedores especializados y favorecer la concentración en pocos actores grandes o extranjeros.

   Respuesta CMF: Se recoge el comentario, eliminándose dicha exigencia.

4. **Comentario:** Se propone aplicar principios de proporcionalidad también a los proveedores, clasificándolos según su tamaño, criticidad y capacidad operativa.

   Respuesta CMF: Se recoge el comentario. El enfoque planteado en la nueva propuesta normativa considera el principio de proporcionalidad, en consistencia con la NCG N°325, lo que se hace explícito en la introducción de la propuesta y en algunas secciones de la misma.

5. **Comentario:** Exigir el mismo nivel de cumplimiento a toda la cadena de subcontratación excluirá pymes y encarecerá los servicios.

   Respuesta CMF: Se recoge el comentario, y se elimina exigencia, ajustando la redacción en términos generales y proporcionales.

6. **Comentario:** Solicitan aclarar si la CMF establecerá un listado de cláusulas mínimas obligatorias (continuidad, información, término, subcontratación) que deban incluirse en los contratos.

   Respuesta CMF: Se mantiene un enfoque de principios generales. Cada compañía define las cláusulas mínimas que corresponda incorporar en el contrato de

externalización. Dichos principios, al menos, deben buscar asegurar la continuidad operacional y la seguridad de la información.

7. **Comentario:** Se propone que se permitan auditorías conjuntas coordinadas por la AACH, para reducir costos y evitar duplicidad, en forma similar a la práctica observada en la industria bancaria.

   Respuesta CMF: La propuesta normativa no excluye lo planteado en el comentario recibido.

8. **Comentario:** Se solicita que se defina la periodicidad mínima para realizar auditorías y aplicar criterios de materialidad, enfocándose en proveedores críticos.

   Respuesta CMF: La periodicidad debe ser fijada por las propias compañías en concordancia con los principios establecidos, así como el criterio de proporcionalidad indicado en la normativa.

9. **Comentario:** Se señala que los planes de salida requeridos a los proveedores externos ante incumplimientos resultan impracticables dada la alta especialización de los proveedores.

   Respuesta CMF: Se ajusta la propuesta normativa, incorporando criterios de razonabilidad y proporcionalidad en los planes de continuidad requeridos.

10. **Comentario:** Se menciona que es imposible garantizar el acceso directo de la CMF a proveedores extranjeros, generándose conflictos con leyes de confidencialidad.

    Respuesta CMF: Se recoge el comentario, se ajusta la redacción, precisando que el acceso de la CMF a la información requerida es a través de la compañía de seguros.

11. **Comentario:** Se señala que se plantean exigencias excesivas para la externalización de servicios en la nube.

    Respuesta CMF: Se recoge el comentario y se ajusta la redacción de la sección "Proceso de debida diligencia reforzada para servicios en la nube" adecuándose algunas exigencias específicas.

12. **Comentario:** Se señala que la evaluación de materialidad es ambigua y subjetiva.

    Respuesta CMF: Se recoge el comentario y se elimina la evaluación de materialidad, manteniéndose el enfoque en criticidad.

13. **Comentario:** Se señala que la prohibición de externalizar funciones de control es excesiva. De igual forma, se solicita permitir la externalización de la función de cumplimiento.

    Respuesta CMF: Se ajusta la redacción, indicándose que no se contemplan como actividades posibles de externalización las vinculadas a funciones de gestión de riesgo, así como la función de auditoría interna realizadas por entidades no relacionadas a la compañía.

14. **Comentario:** Se indica que en el título "Seguridad de la información propia y de sus asegurados, en los casos que corresponda." se estima inadecuado solicitar a las compañías "controlar y monitorear la infraestructura de seguridad de la información del proveedor".

    Respuesta CMF: Se adecuan las exigencias de esa sección, tanto para los servicios externalizados en Chile como en el extranjero.

15. **Comentario:** En relación con la exigencia de una política debidamente aprobada por el Directorio, señalan que la CMF no debería restringir la regulación interna de las compañías a través de una política, debiera ser cualquier documentación interna o incorporarse a políticas ya existentes.

    Respuesta CMF: No obstante, los ajustes con foco en principios y criterios de proporcionalidad realizados a la propuesta normativa, se mantiene la exigencia de política aprobada por el directorio, en línea con lo establecido en la NCG N°325.

16. **Comentario:** Se señala que las cláusulas de veto en la selección de subcontratación que deben incluirse en los contratos de externalización son impracticables.

    Respuesta CMF: Se recoge el comentario, se elimina dicha exigencia.

17. **Comentario:** Para el caso de los contratos de externalización de proveedores en el exterior, ¿cómo se pretende que se incluyan todas las exigencias cuando hay contratos de adhesión, en los que no se permiten negociar cláusulas específicas?

    Respuesta CMF: Se ajusta la redacción, precisándose que las compañías deben tomar los resguardos que sean relevantes en el caso de contratos de adhesión.

18. **Comentario:** En relación a la externalización de servicios no estratégicos, señalan que la exigencia que el Directorio defina 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, debiera reemplazarse por "El Directorio será informado...".

Respuesta CMF: Se ajusta redacción. El Directorio deberá aprobar la política donde se defina qué elementos de esta norma no serán aplicables a aquellos contratos de servicios que comúnmente se vinculan con actividades que no tienen un carácter estratégico o sus riesgos son más acotados.

19. **Comentario:** En relación a los señalado en el Título IV, punto 1, letra h). "Velar por que existan auditorías independientes al proceso de selección..." se consulta si dichas auditorías podrán ser realizadas por la función de auditoría interna?

    Respuesta CMF: Puede ser cualquiera independiente del proceso (interno o externo). La compañía debe establecerlo en su política.

20. **Comentario:** Se señala que debiera clarificarse que la prohibición de externalizar actividades sujetas a ejecución directa por mandato legal no afecta figuras como la liquidación de siniestros por un liquidador oficial y la venta de seguros a través de agentes de venta o corredores.

    Respuesta CMF: La propuesta normativa no prohíbe que ambas actividades puedan externalizarse, en consideración a la normativa específica aplicable, Decreto Supremo N° 1.055, DFL N° 251 y normas asociadas.

En razón de los comentarios recibidos en el primer proceso de consulta pública, la CMF decidió poner en consulta pública, por un segundo periodo, una nueva propuesta normativa. Este proceso se presenta a continuación.

VII. PROCESO DE SEGUNDA CONSULTA PÚBLICA

Entre el 26 de enero y el 9 de marzo de 2026 se puso en consulta, por un segundo periodo, la propuesta normativa contenida en el Informe normativo puesto en consulta. Al respecto, se recibieron 67 comentarios de 10 entidades de la industria aseguradora (Asociación de Aseguradoras de Chile y 9 compañías de seguros). Adicionalmente, se recibió un oficio de la Agencia Nacional de Ciberseguridad (ANCI) con comentarios del proyecto normativo.

A continuación se presenta un resumen de los principales comentarios recibidos en esta etapa junto con la respuesta a los mismos:

1. En el contexto de que la norma deja al criterio de cada entidad la identificación de actividades estratégicas y críticas, sin entregar criterios mínimos ni ejemplos orientadores, lo que podría generar heterogeneidad entre compañías, se sugiere que la norma incorpore un catálogo mínimo transversal de actividades que, por su naturaleza, deban considerarse críticas para todas las compañías (e.g. SCOMP o infraestructura de TI crítica), sin perjuicio del análisis adicional que cada entidad deba efectuar.

Respuesta: La definición de "Actividades significativas o estratégicas (críticas)" contenida en el Título II.2 se alinea con la noción de "actividades significativas o principales" establecida en la NCG N°325. En este sentido, no se considera necesario incorporar a la norma un catálogo mínimo transversal.

2. Unas compañías indicaron que actualmente existe una definición de "Actividad Significativa" en la NCG N°325 que podría entrar en conflicto con la nueva definición que propone la norma. Adicionalmente, indican que el criterio de "alta interacción sistémica en el mercado" es difícil de aplicar para compañías de menor escala. Se sugiere mantener una definición única en todo el marco regulatorio, alineando la nueva norma con la NCG N°325. Además, se propone que la CMF aclare que el criterio de interacción sistémica aplica a nivel de mercado agregado y no genera obligaciones adicionales para compañías de menor participación. Finalmente, se solicita aclarar expresamente si los requisitos i y ii de la definición de actividades significativas o estratégicas son copulativos o alternativos.

Respuesta: La definición de "Actividades significativas o estratégicas (críticas)" contenida en el Título II.2 se alinea con la noción de "actividades significativas o principales" establecida en la NCG N°325, ajustando aquello en la normativa definitiva. De esta forma, no aplican los requisitos i y ii de la definición puesta en consulta.

3. Existe una definición de "Actividad Significativa" en la NCG N°325 que podría entrar en conflicto con la nueva definición. Adicionalmente, el criterio de "alta interacción sistémica en el mercado" es difícil de aplicar para compañías de menor escala.

Respuesta: Ver respuesta de la letra anterior.

4. La norma establece que la compañía mantendrá la responsabilidad por la gestión global de los riesgos y funciones de control. La redacción podría interpretarse como una restricción a la externalización de funciones de riesgo o control. Se solicita precisar la redacción indicando que la responsabilidad se mantiene en la compañía, lo que no impide que el servicio, función de riesgo o control se pueda externalizar (e.g. ejecución técnica de actividades de soporte o monitoreo especializado).

Respuesta: La Comisión acoge esta observación. Con el objeto de precisar que la responsabilidad irrenunciable de la compañía es compatible con la externalización de la ejecución técnica de servicios, se ajusta la redacción del Título IV.7 dejando en claro que el hecho de encomendar dicha ejecución a un proveedor externo no exime a la compañía de su obligación de supervisión, ni de su responsabilidad frente a esta Comisión por los resultados de la gestión externalizada.

Cabe señalar que, como indica el Título II.1 de la norma, no se contemplan como actividades posibles de externalización las vinculadas a funciones de gestión de riesgo y la función de auditoría interna realizadas por entidades no relacionadas a la compañía.

5. La norma propone regular las cadenas de servicios externalizados sin distinguir entre subcontrataciones materiales y dependencias tecnológicas accesorias propias del modelo *cloud*, lo que genera exigencias de difícil aplicación práctica. Se solicita precisar que las obligaciones se refieren a subcontrataciones materiales que incidan de forma relevante en la prestación del servicio, continuidad operacional o tratamiento de datos críticos, distinguiéndolas de dependencias accesorias del modelo *cloud*. Se sugiere además exigir al proveedor notificar sobre elementos tercerizados e informar mecanismos para suplir cambios.

Respuesta: Bajo el principio y objetivo de proporcionalidad que rige esta norma, corresponde a cada compañía determinar, en función de la criticidad del servicio y su perfil de riesgo, qué subcontrataciones dentro de la cadena de servicios externalizados requieren controles reforzados, incluyendo mecanismos de notificación por parte del proveedor ante cambios relevantes. Dicha determinación deberá quedar reflejada en la política aprobada por el Directorio y en los contratos respectivos, si correspondiera, sin perjuicio del deber general de monitoreo y del principio de responsabilidad indelegable de la compañía sobre el servicio externalizado.

6. La redacción de la norma sobre servicios en la nube, confidencialidad de la información y ciberseguridad difiere de las definiciones ya establecidas en la NCG N°510 (aplicable a AGF y Corredores de Bolsa), generando riesgo de asimetrías normativas entre industrias supervisadas.

Respuesta: Respecto de la definición de servicios en la nube (*cloud computing*), se adopta la propuesta presentada por la Agencia Nacional de Ciberseguridad, ANCI, en su carta con comentarios remitida a esta Comisión. Respecto de las definiciones de confidencialidad de la información y ciberseguridad, la Comisión estima que no corresponde incorporarlas en el glosario de la presente norma, sino remitirse a los cuerpos legales que las regulan de manera general para todo el mercado financiero. En consecuencia, las materias relativas a la protección y tratamiento de datos personales se regirán por lo dispuesto en la Ley N°21.719, sobre Protección y Tratamiento de Datos Personales, y las materias relativas a ciberseguridad se regirán por lo dispuesto en la Ley N°21.663, Ley Marco de Ciberseguridad.

7. La norma exige conocer la ciudad donde operan los centros de datos. Por razones de seguridad, muchos proveedores no revelan la ubicación específica de sus servidores. Se solicita aclarar cómo debe interpretarse este requisito en el contexto de proveedores hyperscalers que operan con arquitecturas distribuidas, redundantes y dinámicas dentro de una misma región, y si el conocimiento de la jurisdicción debe ser considerado suficiente.

Respuesta: Tal información debiera ser de acceso a la compañía. No obstante, los principios y conceptos de gestión del riesgo operacional de externalización de servicios señalados en la presente norma serán considerados en la evaluación de la CMF, de acuerdo con la realidad de cada compañía, reconociendo la existencia de diferentes prácticas de gestión de riesgo

operacional en la externalización de servicios dependiendo del tamaño, naturaleza, alcance y complejidad de sus operaciones, estrategia y perfil de riesgo de la compañía.

8. La norma exige procesos de debida diligencia a los proveedores sin contemplar mecanismos alternativos para proveedores tecnológicos globales o estandarizados. Para proveedores en la nube (*cloud*) certificados internacionalmente, la *due diligence* tradicional puede ser desproporcionada. Se solicita que la revisión de debida diligencia pueda basarse en certificaciones independientes, reportes de aseguramiento y estándares reconocidos internacionalmente.

Respuesta: Se acoge el comentario y se agrega indicación en la norma, señalándose que la compañía podrá justificar el cumplimiento de los requerimientos establecidos en dicho proceso a través de mecanismos alternativos, siempre que se adopten los resguardos necesarios para la adecuada gestión de los riesgos derivados de la externalización. Lo anterior deberá quedar documentado en la Política, con su debida justificación, especificando los elementos de debida diligencia que se sustituyen.

9. La norma exige una debida diligencia completa al seleccionar un proveedor y también al enmendar sustancialmente o renovar un contrato, sin distinguir según criticidad del servicio ni si ya se realizó una debida diligencia previa. Se solicita prescindir de la debida diligencia completa en renovaciones contractuales cuando ya se haya realizado previamente. Se propone establecer claramente el Enfoque Basado en Riesgo, dejando fuera del perímetro de due diligence completo las renovaciones y enmiendas de servicios no críticos o no materiales.

Respuesta: En el caso de renovaciones contractuales en que no existan cambios materiales en las condiciones del servicio ni en el perfil de riesgo del proveedor, no se exige un proceso de debida diligencia equivalente al de una contratación nueva, siendo suficiente la aplicación de los mecanismos de seguimiento y control continuo del proveedor que la compañía haya establecido en su política interna de gestión del riesgo de externalización, los cuales deben ser proporcionales a la criticidad del servicio contratado.

10. La debida diligencia reforzada para servicios en la nube exige un pronunciamiento sobre la tolerancia o apetito al riesgo respecto de los datos a almacenar o procesar, sin especificar el tipo de riesgo al que se refiere. Se solicita especificar el tipo de riesgo involucrado. Se entiende que, al tratarse de almacenamiento y procesamiento de datos, la referencia corresponde al Riesgo Tecnológico y al Riesgo de Seguridad de la Información.

Respuesta: La norma mantiene una referencia amplia sobre los riesgos derivados del procesamiento y almacenamiento de datos, sin restringirla a categorías específicas como riesgo tecnológico o riesgo de seguridad de la información, por cuanto el pronunciamiento del Directorio sobre tolerancia y apetito al riesgo en el contexto de servicios en la nube debe abarcar el conjunto de riesgos que dicho procesamiento y almacenamiento puede generar, incluyendo, pero no limitándose a, los riesgos de confidencialidad, integridad, disponibilidad y continuidad de la información.

11. La norma indica como buena práctica que el proveedor cuente con adecuados mecanismos de seguridad físicos y lógicos, sin precisar estándares mínimos para evaluaciones de seguridad. Se solicita precisar si existe un estándar mínimo esperado respecto de *vulnerability assessments* y *penetration tests* exigibles a proveedores externalizados, indicando periodicidad, alcance, metodologías y estándares internacionales de referencia.

Respuesta: La determinación de la periodicidad, alcance, metodologías y estándares de referencia aplicables corresponde a cada compañía, en función de la criticidad de la actividad externalizada y del perfil de riesgo del proveedor, en el marco de su política interna de gestión del riesgo de externalización.

12. La norma se refiere a "adecuados mecanismos de seguridad, tanto físicos como lógicos", sin especificar si esto implica una estructura formal de gestión de seguridad ni cómo deben tratarse los datos en otras jurisdicciones. Se solicita: a) Aclarar si la referencia implica que el proveedor cuente con una estructura mínima formal de gestión de seguridad proporcional a la criticidad del servicio externalizado. b) Aclarar si, en casos de tratamiento transfronterizo de datos, el proveedor debe cumplir con estándares equivalentes al marco normativo local de protección de datos personales.

Respuesta: Respecto de la letra a), la determinación de los mecanismos de seguridad físicos y lógicos exigibles al proveedor corresponde definirlos a cada compañía en función de la criticidad de la actividad externalizada y del perfil de riesgo del proveedor, en el marco de su política interna de gestión del riesgo de externalización. Respecto de la letra b), la compañía deberá velar que el proveedor trate los datos de sus asegurados bajo condiciones equivalentes al marco normativo local de protección de datos personales.

13. La norma exige que la compañía se cerciore de que el proveedor "mantiene y cumple efectivamente" un programa de seguridad de la información. Esta exigencia resulta de difícil aplicación en contratos de adhesión.

Respuesta: La norma ya contempla una excepción para los contratos de adhesión, caso en el cual la compañía deberá mantener a disposición de esta Comisión los antecedentes que acrediten los mecanismos adoptados para resguardar la confidencialidad, integridad, trazabilidad y disponibilidad de los activos de información.

14. La norma establece el deber de encriptación de datos sin precisar cuáles son los mecanismos técnicos aceptables.

Respuesta: El nivel de encriptación exigible corresponde a cada compañía determinarlo en función de la criticidad y clasificación de la información que se trate, en el marco de su política interna de gestión del riesgo de externalización.

15. En el primer proceso consultivo, la Comisión indicó que la "auditoría independiente" puede ser tanto interna como externa. Esta respuesta genera ambigüedad respecto del real alcance y estándar esperado.

Respuesta: Esta Comisión mantiene el criterio señalado en el proceso consultivo anterior. La auditoría exigida es "independiente" cuando quien la ejecuta tiene la facultad de desafiar objetivamente la calidad de la gestión de riesgos de externalización, independientemente de si pertenece a la plantilla de la compañía o a una entidad externa, en los términos establecidos en las NCG N°309, NCG N°325 y NCG N°454. Con todo, corresponde a cada compañía establecer en su política interna el tipo de auditoría que aplicará en cada caso, en función de la criticidad del servicio y del perfil de riesgo del proveedor.

16. Para servicios prestados bajo modalidad nube o SaaS, las limitaciones prácticas de acceso hacen que las auditorías in situ sean técnicamente imposibles o excesivamente costosas.

Respuesta: La propuesta normativa no exige auditorías in situ ni prohíbe el uso de certificaciones internacionales como mecanismo de acreditación. La letra h) del Título IV.1 establece una obligación de medio respecto de la existencia de auditorías independientes, sin prescribir una modalidad específica de ejecución. Adicionalmente, el Título IV.3.2 reconoce expresamente las certificaciones independientes reconocidas internacionalmente como elemento válido del proceso de debida diligencia reforzada, por lo que su utilización es plenamente compatible con las exigencias de la norma.

17. La norma exige que los proveedores realicen periódicamente informes de auditoría o revisiones independientes, aplicando esta obligación a todos los servicios externalizados sin distinción de criticidad.

Respuesta: La Comisión estima que la exigencia establecida en la letra i) del Título IV.1 se encuentra en la línea correcta. No obstante, corresponde a la propia compañía evaluar, conforme al criterio de proporcionalidad, la frecuencia, alcance y profundidad de esta exigencia respecto de cada proveedor, en función de su criticidad y perfil de riesgo.

18. La norma exige que la compañía evalúe si los proveedores críticos cuentan con "planes apropiados" de continuidad del negocio, implicando una valoración sobre la idoneidad de planes de terceros externos.

Respuesta: Se elimina la palabra "apropiados" del texto de la norma. Lo anterior, sin perjuicio de la responsabilidad indelegable de la compañía ante esta Comisión por la continuidad de los servicios externalizados y de su obligación de contar con su propio plan de continuidad.

19. La norma exige que la compañía disponga de planes propios para asegurar la continuidad operacional ante la indisponibilidad del servicio externalizado, asumiendo que la actividad puede ser realizada internamente, lo que no siempre es el caso.

Respuesta: La presente norma aplica a aquellas actividades que, en principio, podrían ser efectuadas directamente por la compañía con sus propios recursos humanos y tecnológicos, por lo que la obligación de contar con un plan propio de continuidad del negocio resulta inherente a su ámbito de aplicación.

20. La norma prohíbe externalizar servicios en jurisdicciones sin calificación de riesgo país en grado de inversión, sin precisar agencia calificadora ni metodología. Esta restricción puede limitar el acceso a proveedores globales especializados y genera inseguridad operativa ante cambios de calificación soberana.

Respuesta: Se especifica en la norma. La calificación de riesgo soberano debe haber sido asignada por una clasificadora de reconocido prestigio internacional (estándar objetivo y verificable). Respecto de la solicitud de incorporar excepciones basadas en controles contractuales y tecnológicos equivalentes, la Comisión estima que el mecanismo de excepción por parte del Directorio ya contemplado en la norma satisface esta inquietud, toda vez que dicha facultad presupone necesariamente que el Directorio haya realizado una evaluación completa y fundada de los riesgos asociados a la jurisdicción del proveedor, incluyendo la suficiencia de los controles contractuales y tecnológicos disponibles, antes de aprobar la excepción.

21. La norma exige que la compañía asegure que la CMF tenga acceso permanente a "todos los registros, datos e información" que se procesen a través de un proveedor externo. Esta exigencia es de difícil cumplimiento en contratos de adhesión.

Respuesta: La responsabilidad de garantizar el acceso de esta Comisión a la información reside en la compañía, independientemente de las condiciones pactadas con terceros, siendo dicho acceso canalizado siempre a través de la propia compañía, evitando conflictos directos de jurisdicción o confidencialidad con proveedores extranjeros. La aplicación de esta exigencia puede adoptar modalidades distintas según el tamaño, naturaleza y complejidad de las operaciones de cada compañía, y para los casos de proveedores con contratos de adhesión que no admitan negociación, la normativa faculta a la aseguradora para definir en su política de externalización los resguardos que estime pertinentes para satisfacer el objetivo de supervisión cuando la inclusión de cláusulas de acceso irrestricto no sea contractualmente factible.

22. La norma exige mantener permanentemente actualizado un plan que posibilite cumplir con los eventuales requerimientos de la CMF, incluyendo la sustitución del proveedor. No contempla los casos en que esto no sea posible.

Respuesta: Los principios y conceptos de gestión del riesgo operacional de externalización de servicios señalados en la presente norma serán considerados en la evaluación de la CMF, de acuerdo con la realidad de cada compañía, reconociendo la existencia de diferentes prácticas de gestión de riesgo operacional de la externalización de servicios dependiendo del tamaño, naturaleza, alcance y complejidad de sus operaciones, estrategia y perfil de riesgo de la compañía. De esta manera, la aplicación de estos principios o conceptos pueden adoptar modalidades distintas en cada aseguradora, lo que será tomado en cuenta por la Comisión en su evaluación.

23. La norma establece que al externalizar servicios fuera del país, la compañía deberá disponer en todo momento de los antecedentes de la empresa contratada y efectuar el monitoreo del servicio externalizado en el exterior. El acceso a estos antecedentes

depende de que el proveedor los proporcione. Se solicita: i) aclarar que la obligación se entiende cumplida mediante la realización de los procesos de debida diligencia y la solicitud de información al proveedor en la medida en que sea efectivamente entregada; ii) aclarar si la obligación de monitoreo aplica aun cuando el servicio no soporte procesos significativos.

Respuesta: La obligación de disponer en todo momento de los antecedentes del proveedor extranjero no puede quedar supeditada a la voluntad de éste, siendo responsabilidad de la compañía asegurar su obtención mediante sus procesos de debida diligencia, evaluando además la idoneidad de la legislación de protección de datos de la jurisdicción del proveedor. Respecto de la letra ii), el monitoreo de servicios externalizados en el extranjero es obligatorio, con independencia de si el servicio soporta o no procesos estratégicos, por cuanto el riesgo país y jurisdiccional introduce variables de naturaleza económica, política y legal que deben ser gestionadas independientemente de la criticidad del servicio. Si bien la aplicación de estos principios puede adoptar modalidades distintas según la complejidad de cada compañía, ello flexibiliza el cómo se realiza el control, pero no exime del cumplimiento de los requisitos mínimos de disponibilidad de información para esta Comisión.

24. Para contratos de adhesión, puede existir la imposibilidad de verificar el cumplimiento de todos los elementos de la política de contratación si el proveedor no entrega la documentación requerida. La norma tampoco especifica cómo debe quedar constancia de la revisión efectuada.

Respuesta: La política de externalización de la compañía (del Título IV.2) debe definir los elementos mínimos de los contratos o, en su defecto, los resguardos que se consideren relevantes para los casos de contratos de adhesión, debiendo la compañía dejar constancia formal de la revisión efectuada y de los resguardos adoptados, documentación que debe mantenerse permanentemente actualizada y a disposición de esta Comisión. Con todo, se perfecciona la condición de resguardo que debe tomarse en los contratos de adhesión.

25. La norma exige que los procedimientos operacionales, administrativos y tecnológicos del servicio contratado estén debidamente documentados y permanentemente a disposición de la compañía y la CMF. Algunos proveedores no entregarán esta información por considerarla protegida.

Respuesta: La letra j) del Título IV.1 se refiere específicamente a los procedimientos propios del servicio contratado y no a la documentación interna general del proveedor. Adicionalmente, la Política de contratación y gestión de externalización contemplada en el mismo Título IV.1 faculta a la compañía para definir los resguardos que estime relevantes en el caso de contratos de adhesión, lo que permite atender adecuadamente los casos en que el proveedor no entregue documentación por considerarla protegida.

26. La norma exige la inclusión de niveles mínimos de servicio (SLAs, en inglés) en los contratos y acceso a información para monitorearlos, sin aclarar si esto aplica a todas las externalizaciones o solo a aquellas con proveedores significativos.

Respuesta: La normativa establece principios generales, por lo que corresponde a cada compañía definir las cláusulas mínimas a incorporar en sus contratos de externalización, y la profundidad de los niveles de servicio aplicables, en función de la criticidad del proceso que el proveedor soporta. Adicionalmente, se faculta al Directorio para aprobar una Política que defina, conforme al Anexo N°2, los elementos que no resulten aplicables a contratos vinculados con actividades no estratégicas o de riesgos más acotados.

27. El Anexo N°1 de la normativa propuesta exige que todos los contratos en idioma extranjero cuenten con copia traducida al español. Para contratos de adhesión con grandes proveedores tecnológicos globales, esta exigencia implica costos excesivos sin un beneficio proporcional.

Respuesta: Se acoge el comentario, señalando en la norma que la exigencia de la traducción al español será a requerimiento de esta Comisión para fines de supervisión y sin expresión de causa.

28. La norma exige mantener un catastro actualizado de todos los servicios contratados con terceros, sin distinguir el nivel de detalle requerido según criticidad del servicio. Se solicita aclarar que el catastro de servicios no estratégicos puede mantenerse de forma simplificada, reservando el nivel de detalle exigido únicamente para aquellos servicios calificados como críticos.

Respuesta: La letra f) del Título IV.1 establece con claridad que la compañía debe mantener un catastro de todos los servicios contratados con terceros, determinando aquellos que, a su juicio, son estratégicos y de alto riesgo, y aplicando procedimientos de control y seguimiento de acuerdo con los niveles de criticidad que les asigne. En consecuencia, la norma ya contempla un tratamiento diferenciado del catastro en función de la criticidad del servicio, correspondiendo a la compañía determinar el nivel de detalle aplicable en cada caso.

29. La norma exige evaluar el riesgo de concentración en proveedores, pero actualmente no existe un registro centralizado de proveedores que permita determinarlo. Las cláusulas de confidencialidad contractual dificultan el análisis y existen riesgos en materias de libre competencia.

Respuesta: Los principios y conceptos de gestión del riesgo operacional de externalización de servicios señalados en la presente norma serán considerados en la evaluación de la CMF, de acuerdo con la realidad de cada compañía, reconociendo la existencia de diferentes prácticas de gestión de riesgo operacional de la externalización de servicios, dependiendo del tamaño, naturaleza, alcance y complejidad de sus operaciones, estrategia y perfil de riesgo de la compañía. De esta manera, la aplicación de estos principios o conceptos pueden adoptar modalidades distintas en cada aseguradora, lo que será tomado en cuenta por la Comisión en su evaluación. No obstante lo anterior, las compañías podrían hacer un catastro y levantamiento de aquellos proveedores considerados como críticos para efectos de cumplimiento de la evaluación del riesgo de concentración que requiere la normativa.

30. La norma establece como objetivo que las compañías "eviten y gestionen" el riesgo de concentración y dependencia tecnológica. En ocasiones el riesgo de concentración no puede evitarse por depender de condiciones de mercado no controlables.

Respuesta: Se elimina el término "evitar" del objetivo normativo relativo al riesgo de concentración y dependencia tecnológica, manteniéndose únicamente la obligación de gestionar dicho riesgo.

31. La norma establece una vigencia diferida de 1 año desde su publicación, plazo que resulta insuficiente para exigencias de mayor complejidad operativa: modificación de cláusulas contractuales, desarrollo y prueba de planes de continuidad, implementación de monitoreo continuo. Adicionalmente, no queda claro si el período aplica solo a nuevos contratos o también a los vigentes. Se propone una implementación gradual en plazos de 12 y 24 meses en función de los distintos requerimientos normativos.

Respuesta: Se establece vigencia diferida de un año desde la publicación de la normativa con el objetivo de que las compañías puedan adecuar sus procesos de gestión a los lineamientos establecidos en la norma. Los contratos suscritos a partir de la fecha de entrada en vigencia deberán cumplir íntegramente con los requisitos establecidos en esta norma. Por su parte, los contratos celebrados con anterioridad a la fecha de entrada en vigencia deberán adecuarse en la primera oportunidad disponible, tal como su renovación, prórroga o ante enmiendas sustanciales a sus términos y condiciones. En cualquier caso, deberán adecuarse a más tardar dentro del plazo de un año contado desde la entrada en vigencia.

32. La norma exige que el Directorio se pronuncie sobre el apetito y niveles de tolerancia al riesgo, indicando que niveles cuantificables aportan a un mejor control, sin especificar el tipo de riesgo al que se hace referencia.

Respuesta: La normativa establece que es responsabilidad del Directorio definir el apetito y la tolerancia al riesgo mediante una combinación de medidas cuantitativas (límites y umbrales) y definiciones cualitativas detalladas que permitan una administración adecuada de los riesgos de externalización de servicios a los que la aseguradora se ve expuesta. Estas métricas deben ser consistentes con el perfil de riesgo de la entidad, sirviendo además como indicadores para el escalamiento oportuno de incidentes a la alta administración.

33. El conjunto de exigencias de la norma implica una carga regulatoria y operativa significativa lo que podría desincentivar la externalización, ampliar responsabilidades y generar asimetrías normativas.

Respuesta: La propuesta normativa no impone un modelo rígido y se sustenta en Principios para la adecuada externalización. De esta forma, la CMF ponderará el cumplimiento según el tamaño, naturaleza y complejidad de cada aseguradora. Por su parte, se establece que el Directorio puede definir qué elementos de la norma no serán aplicables a servicios no estratégicos o de bajo riesgo, reduciendo la carga operativa donde no es crítica.

34. La norma utiliza expresiones que requieren precisión: i) no queda claro si el alcance de la norma considera factores como costos o disponibilidad de capacidades internas al evaluar si un servicio "podría ser efectuado directamente" por la compañía; ii) la expresión "personal a cargo de los servicios contratados" genera ambigüedad sobre si se refiere al personal del proveedor o al de la compañía.

Respuesta: Respecto del alcance de la expresión "podría ser efectuada directamente" contenida en el Título II.1, se aclara que dicha referencia alude exclusivamente a la capacidad operativa de la compañía para ejecutar la actividad con sus propios recursos humanos y técnicos; en consecuencia, una actividad queda comprendida en el ámbito de la norma cuando la compañía dispone de las capacidades técnicas u operativas para ejecutarla directamente, independientemente de consideraciones de costo o conveniencia económica. Por lo mismo, la compañía debe incorporar principios para velar por la continuidad operacional.

Respecto de la expresión "personal a cargo de los servicios contratados" contenida en la letra e) del Título IV.1, se precisa que ésta se refiere al personal especialista del proveedor que ejecuta materialmente las tareas externalizadas, y no al personal interno de la aseguradora que supervisa o recibe los entregables del servicio, siendo esta distinción relevante para efectos de los requisitos de calificación y experiencia que la norma exige acreditar respecto de quienes ejecutan directamente las actividades externalizadas.

35. Se sugiere ajustar distintas definiciones de la sección II.2 con relación a la Ley Marco de Ciberseguridad, así como pronunciarse respecto a la compatibilidad con la Ley indicada.

Respuesta: Se ajustan diferentes definiciones relacionadas con el servicio de nube.

En caso de que el proveedor se encuentre calificado como operador de importancia vital, o si le corresponde dicho estatuto conforme a la Ley N°21.663 (Ley Marco de Ciberseguridad) y su normativa complementaria, deberá cumplir las obligaciones propias de dicho régimen. Lo anterior resulta especialmente relevante cuando el servicio externalizado sea una actividad significativa o principal que pueda afectar la continuidad operacional, la seguridad de la información o la provisión regular de su servicio financiero.

Asimismo, en los procesos de debida diligencia, contratación, seguimiento y continuidad del negocio, la compañía deberá considerar, sobre la base de sus políticas de externalización y cuando corresponda, que el proveedor puede estar sujeto al estatuto de operador de importancia vital. De ser así, esta exigencia debe entenderse como un resguardo adicional frente a riesgos de ciberseguridad, continuidad operacional y dependencia tecnológica, particularmente en servicios de nube, infraestructura digital, servicios digitales o servicios de tecnología de la información gestionados por terceros.

VIII. NORMA DEFINITIVA

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

[XX] de [XX] de 2026

NORMA DE CARACTER GENERAL Nº [XX]

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, todos del D.L. 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 agosto de 2026, ejecutado mediante Resolución Exenta N°XXXX de XX de agosto de 2026, 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 riesgos, en particular al riesgo operacional, así como a riesgos de cumplimiento y reputacionales, entre otros.

Esta norma se enmarca en la implementación del modelo de Supervisión Basada en Riesgo promovido por la Comisión para el Mercado Financiero (CMF) y, se basa en los principios de gestión prudencial establecidos en la NCG N°454 sobre gestión de riesgo operacional y ciberseguridad, la que a su vez descansa en los principios establecidos por las Normas de Carácter General N°309 sobre gobierno corporativo y N°325 sobre sistemas de gestión de riesgos.

Los principios y conceptos de gestión del riesgo operacional de externalización de servicios señalados en la presente norma serán considerados en la evaluación de la CMF, de acuerdo con la realidad de cada compañía, reconociendo la existencia de diferentes prácticas de gestión de riesgo operacional de la externalización de servicios dependiendo del tamaño, naturaleza, alcance y complejidad de sus operaciones, estrategia y perfil de riesgo de la compañía. De esta manera, la aplicación de estos principios o conceptos pueden adoptar

modalidades distintas en cada aseguradora, lo que será tomado en cuenta por la Comisión en su evaluación.

El directorio y la alta gerencia son los responsables del cumplimiento de los principios establecidos en esta norma. De esta forma, el directorio deberá aprobar las políticas que implementan los principios detallados en esta norma en la compañía y monitorear el cumplimiento de estos principios. Por su parte, la administración deberá establecer los procedimientos para una correcta implementación de dichos principios conforme a la realidad de cada compañía.

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 lineamientos sobre los procesos de selección y contratación de proveedores, requisitos contractuales, 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 normativa 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 o norma ha definido que deben ser prestados por entidades de giro exclusivo.

La presente norma no contempla como actividades posibles de externalización las vinculadas a funciones de gestión de riesgo, así como tampoco la función de auditoría interna realizadas por entidades no relacionadas a la compañía.

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.

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 las definidas en el artículo 100 de la ley N°18.045 y todas aquellas personas señaladas en los numerales del artículo 146 de la Ley N°18.046.

Servicios en la nube (*cloud computing*): servicios de infraestructura tecnológica y aplicaciones, en modalidad física o virtual, administrados total o parcialmente por un proveedor externo. Generalmente son desplegados en múltiples ubicaciones geográficas y entregados bajo demanda de recursos o con mecanismos de auto 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 principales: toda línea de negocios o actividad que sea fundamental para el modelo de negocios de la aseguradora y en la que cualquier debilidad o falla en su provisión o ejecución pueda tener un efecto significativo sobre el cumplimiento normativo, la continuidad del negocio, la seguridad de la información propia o de sus asegurados, la calidad de sus servicios y productos, o la solvencia de la compañía, considerando su naturaleza, tamaño y complejidad.

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 por la compañía para resguardar la seguridad de la información.

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 a la externalización 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 por parte de numerosas compañías de seguros u otras entidades financieras en un solo 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 tal proveedor; cuando se externalicen servicios en proveedores que contemplen 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. En base a lo anterior, las compañías deben evaluar a cada proveedor y definir de manera fundada los criterios de contratación, tomando en consideración aspectos como la concentración y barreras de salida.

IV. Elementos que deben considerarse 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 considerar los elementos que se presentan a continuación:

1. Criterios generales

a) El Directorio, o quien haga sus veces, deberá pronunciarse sobre el apetito y los niveles de tolerancia al riesgo que está dispuesto a asumir en el caso de externalizar servicios. En este contexto, niveles de apetitos y tolerancias cuantificables aportan a un mejor control del riesgo.

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) Realizar una debida diligencia al proveedor, de acuerdo con lo indicado en el N°3 siguiente, resguardando que éste cuente 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.

f) Mantener un catastro actualizado de todos los servicios contratados con terceros, 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 que la externalización de servicios regulada por esta norma no afecte el cumplimiento oportuno y cabal de los compromisos que la compañía tiene con sus asegurados.

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

i) Velar por 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, que aborden aspectos tales como la calidad del servicio, la continuidad operacional y la seguridad de la información, debiendo compartir oportunamente con la compañía los hallazgos que le sean pertinentes.

j) Velar por 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. Asimismo, deben quedar claramente establecidas, 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 los reportes de riesgo operacional que ponga a disposición del Directorio, 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, entre otros contenidos que estime necesarios.

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 definidos por la compañía en los contratos, y acceso a información suficiente para hacer monitoreo de los niveles de servicios.

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

La Política que deberá ser aprobada 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) Criterios particulares de contratación, cuando se trate de un proveedor que sea una entidad relacionada.

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

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

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

h) Los elementos mínimos a incorporar en el contrato de prestación de servicios, teniendo en cuenta los criterios contemplados en el numeral 1 anterior, que la entidad considere relevantes.

   En el caso de contratos de adhesión, que no cuenten con la totalidad de dichos elementos mínimos, la política deberá definir cuáles serán las excepciones, es decir, los aspectos que no estarán considerados en los contratos. Dichas excepciones deberán estar justificadas y limitarse únicamente a aquellos aspectos que escapen al control y gestión de la compañía. Al mismo tiempo, la política deberá considerar la adopción y documentación de los resguardos necesarios para la adecuada gestión de los riesgos derivados de la externalización mediante contratos de adhesión que no cuenten con los citados elementos mínimos.

i) 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. Proceso de debida diligencia

3.1 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 dicha 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 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 podrán variar según la compañía y la naturaleza del acuerdo de externalización que se esté contemplando.

3.2 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 relevantes. Al respecto, la variedad de servicios a los que es posible acceder a través de la nube, como de infraestructura, plataforma o incluso de *software*, importa 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 aprobar - al menos anualmente o cuando se produzca un cambio - 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 u otras normas o la legislación vigente, las compañías podrán externalizar en la nube pública o privada sus servicios no críticos conforme a las consideraciones mencionadas en los títulos precedentes.

En el evento que la compañía evalúe la contratación de un servicio en la nube para una actividad considerada significativa o principal, 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) Se considera una buena práctica que el proveedor del servicio realice informes de auditoría asociados a los servicios prestados y dichos informes se encuentren disponibles, para ser consultados en cualquier momento por la compañía contratante y esta Comisión, en las materias que resulten pertinentes.

d) Se considera una buena práctica que la compañía requiera que el proveedor cuente 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.

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

La entidad podrá justificar el cumplimiento de los requerimientos dispuestos en este numeral mediante mecanismos alternativos, siempre que se adopten los resguardos necesarios para la adecuada gestión de los riesgos derivados de la externalización. Lo anterior deberá quedar documentado en la política, con su debida justificación, especificando los elementos de debida diligencia que se sustituyen.

4. Plan de continuidad del negocio

La compañía debe requerir que sus proveedores de servicios críticos cuenten con planes que aseguren la continuidad de los servicios contratados. De igual forma se considera una buena práctica que los proveedores críticos de servicios subcontratados cuenten a su vez con apropiados planes de continuidad del negocio. Adicionalmente, la compañía también debe disponer de planes 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. Lo anterior, considerando criterios de razonabilidad y proporcionalidad.

Se considera una buena práctica que la compañía requiera 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 permitirle a la compañía 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 prestarlo.

5. 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 asegurados. Estas condiciones deben ser consistentes con las políticas y estándares adoptados por la compañía y, en lo posible, quedar incorporadas en el contrato de prestación de servicios. En caso de que, por tratarse de un contrato de adhesión no sea posible incorporar lo precedente, la compañía deberá mantener a disposición de la Comisión antecedentes que den cuenta de mecanismos para asegurar la confidencialidad, integridad, trazabilidad y disponibilidad de sus activos de información y la de sus clientes.

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.

6. Riesgo país

Sólo se podrá externalizar servicios en jurisdicciones que cuenten con calificación de riesgo país en grado de inversión, otorgada por una clasificadora de reconocido prestigio internacional. No obstante, el Directorio 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.

7. Responsabilidad por la gestión

La compañía será siempre responsable por la gestión de los riesgos y funciones de control. El hecho de que la ejecución técnica de determinadas actividades operativas, de soporte o monitoreo especializado sea encomendada a un proveedor externo, no exime a la compañía de su obligación de supervisión ni de su responsabilidad frente a esta Comisión por los resultados de dicha gestión. 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.

8. Acceso a la información por parte del supervisor

La compañía contratante debe asegurarse que esta Comisión tenga acceso permanente, a través suyo, 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.

9. 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 efectuar el monitoreo del servicio externalizado en el exterior. Dichas actividades de monitoreo 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

En el caso de aquellas entidades que hayan externalizado actividades significativas o principales o que las exponga a riesgos operacionales relevantes, esta Comisión podrá requerir mecanismos de gestión de contingencias y evaluación de riesgos para el adecuado desarrollo de la actividad aseguradora. En consideración a lo anterior, la compañía deberá mantener permanentemente actualizado un plan que posibilite cumplir con esos eventuales requerimientos.

VI. Vigencia y aplicación

La presente normativa entra en vigencia a contar de un año desde la fecha de emisión. Adicionalmente, para facilitar una implementación ordenada y resguardar la estabilidad de las relaciones contractuales, se establecen las siguientes reglas de transitoriedad:

1. **Nuevas contrataciones:** Todos los contratos de externalización suscritos a partir de la fecha de entrada en vigencia deberán cumplir íntegramente con los requisitos establecidos en esta norma.

2. **Adecuación de contratos vigentes:** Los contratos de externalización celebrados con anterioridad a la fecha de entrada en vigencia deberán adecuarse a lo dispuesto en la presente normativa en la primera oportunidad disponible, tal como su renovación, prórroga o ante enmiendas sustanciales a sus términos y condiciones. En cualquier

caso, deberán adecuarse a más tardar dentro del plazo de un año contado desde la entrada en vigencia.

CATHERINE TORNEL LEÓN
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, volumen de transacciones que se procesará, criticidad del servicio contratado y concentración de servicios con el mismo proveedor, 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, además del adecuado cumplimiento de las formalidades legales y normativas propias de esta clase de operaciones, éstas deberán ajustarse en precio, términos y condiciones a aquellas que prevalezcan en el mercado al tiempo de su aprobación, debiendo además, cumplir las condiciones económicas con principios de transparencia 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.

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 asegurados; restricciones sobre el uso de *software*; eliminación segura de los datos del cliente, cuando corresponda; además, indicar claramente donde operan los centros de datos.

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.

En caso de celebrarse contratos de adhesión, la compañía deberá verificar el cumplimiento de los elementos establecidos en su política de contratación y gestión de actividades relativas a la externalización de servicios, dejando constancia de la revisión efectuada y de los resguardos que se consideren relevantes al efecto.

Por último, las compañías, en el caso de contratos, subcontratos y sus respectivos anexos que se encuentren celebrados en un idioma extranjero, deberán proveer de una copia traducida al idioma español, cuando la CMF lo solicite para efectos de supervisión. La veracidad de la traducción será responsabilidad de la compañía.

4. Control permanente

Del proveedor: La compañía debe controlar el desempeño del proveedor durante la vigencia del contrato y sus eventuales modificaciones o prórrogas.

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.

Anexo N°2

Externalización de servicios no significativos

El Directorio deberá aprobar la Política donde se defina qué elementos de esta norma no serán aplicables a aquellos contratos de servicios que comúnmente se vinculan con actividades que no tienen un carácter significativo 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.

Lo anterior, sin perjuicio de que la comercialización de las pólizas deba 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 requerimiento legal o regulatorio que ponga en riesgo la adecuada provisión del servicio.

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.

COMISIÓN
PARA EL MERCADO
FINANCIERO

REGULADOR Y SUPERVISOR FINANCIERO DE CHILE

www.cmfchile.cl