CAPÍTULO 20-7

EXTERNALIZACIÓN DE SERVICIOS

I. ÁMBITO DE APLICACIÓN.

1. Alcance de las presentes normas.

El presente Capítulo trata de las contrataciones por parte de las instituciones bancarias, de proveedores de servicios externos para que realicen una o más actividades operativas que podrían ser también efectuadas internamente por la entidad con sus propios recursos, tanto humanos como tecnológicos. En consecuencia, las disposiciones de este Capítulo no son aplicables a aquellos servicios que evidentemente una entidad 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.

En todo caso, dichos servicios siempre deberán ser considerados por las entidades dentro de sus procesos generales de evaluación y gestión de riesgo operacional, en el contexto de lo señalado en la letra C) del numeral 3.2 del Título II del Capítulo 1-13 de esta Recopilación.

Por otra parte, en concordancia con lo indicado en la letra D) del numeral 3.2 antes mencionado, los bancos deben procurar que las políticas y los procedimientos tratados en este Capítulo se apliquen también, cuando proceda una externalización de servicios según las regulaciones a las que deben atenerse, en todas sus filiales en el país y en sus sucursales y filiales en el exterior.

Las presentes normas no contemplan como actividades posibles de externalización, aquellas relacionadas con la captación de dinero de terceros fuera de las oficinas de la entidad, la apertura de cuentas corrientes y las vinculadas a funciones de control al interior de la empresa.

2. Definiciones.

Para los efectos de esta normativa se deberán considerar las siguientes 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 por la entidad contratante.

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

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

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

Entidad relacionada: aquélla vinculada a la propiedad o gestión del banco, en los términos definidos por este Organismo en el Capítulo 12-4 de esta Recopilación.

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 de importancia en las que cualquier debilidad o falla en la provisión o ejecución del servicio tiene un efecto significativo sobre el cumplimiento normativo, continuidad del negocio, seguridad de la información (propia o de sus clientes) y la calidad de los servicios, productos, información e imagen de la entidad contratante.

ii. cualquier actividad que involucre el procesamiento de datos que se encuentren sujetos a reserva o secreto bancario de acuerdo con lo establecido en la Ley General de Bancos.

iii. cualquier actividad que tenga impacto significativo en la gestión de riesgos.

iv. aquellas actividades de alta interacción sistémica en el mercado o que incorporan riesgos significativos en la entidad contratante.

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*.

II. PRINCIPALES RIESGOS QUE SE ASUMEN CON MOTIVO DE LA EXTERNALIZACIÓN DE SERVICIOS.

Aun cuando el riesgo operacional es el que se presenta en forma más frecuente, la externalización de servicios también se ve afectada por los riesgos estratégico, reputacional, de cumplimiento, de país, de concentración y legal, entre otros.

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 la letra C) del numeral 3.2 del Título II del Capítulo 1-13 de esta Recopilación.

Dentro de las evaluaciones de riesgo deben considerarse aquellos que se generan como consecuencia de la concentración de entidades financieras en un proveedor, ya que ante una eventual falla de éste, se podría generar una crisis a nivel de la industria; así como también cuando se entreguen varias actividades significativas a un mismo proveedor y al externalizar 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 instituciones deben definir de manera fundada los criterios de concentración y barreras de salida.

III. CONDICIONES QUE DEBEN CUMPLIRSE EN LA EXTERNALIZACIÓN DE SERVICIOS.

La entidad 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 deberá pronunciarse sobre la tolerancia 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 entidad.

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. 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 a los niveles de criticidad que les asigne.

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

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 institución 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 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 entidad 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 entidad.

l) La entidad 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 institución para administrar los riesgos de *outsourcing*, 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.

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 entidad o del órgano que haga sus veces, 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 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 entidad para determinar aquellos servicios que, a su juicio, se encuentran asociados con actividades significativas o estratégicas.

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 entidad.

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

i) Definición de los mecanismos para contar con autorización previa de cada cliente, en caso que el servicio a externalizar incluya la transmisión de datos fuera del país, que por su naturaleza están sujetos a lo dispuesto en el artículo 154 de la Ley General de Bancos, relativo a la reserva o secreto bancario. Sin perjuicio de lo anterior, cabe recordar que los servicios externalizados en Chile quedan sujetos a la misma obligación de reserva o secreto según corresponda, a la que se encuentra sujeto la entidad.

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 a lo dispuesto en el Anexo N° 4.

3. Continuidad del negocio.

La entidad debe verificar que sus proveedores de servicios críticos cuenten con planes apropiados que aseguren la continuidad de los servicios contratados. De igual forma la entidad debe verificar que sus proveedores críticos se aseguran 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 incluyendo, cuando corresponda, el escenario de desastre de sus distintos sitios de procesamiento, debiendo la entidad tomar conocimiento de dicha actividad y verificar los resultados obtenidos. Adicionalmente, la entidad también debe disponer de planes, igualmente probados, para asegurar la continuidad operacional ante la contingencia de no contar con dicho servicio externo.

La entidad 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 institución 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.

Los sitios de procesamiento e infraestructura tecnológica que soporten los servicios externalizados deben considerar los requerimientos señalados en el título II del Capítulo 20-9 de esta Recopilación.

4. Seguridad de la información propia y de sus clientes, en los casos que corresponda.

La entidad debe cerciorarse que el proveedor de 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 entidad y quedar incorporadas en el contrato de prestación de servicios.

La entidad 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 entidad 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 entidad 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 entidad 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 entidad. Asimismo, se deben definir los procedimientos de intercambio de claves entre el proveedor de servicios y la institución, además de establecerse los roles y responsabilidades de las personas involucradas en la administración de la seguridad.

En el caso de procesamiento de documentación física, la entidad deberá contar con procedimientos de control que velen 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 entidad por parte del proveedor, y que éste en ningún caso mantenga información en su poder después de finalizada la relación contractual.

5. 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 del análisis realizado al efecto. Lo anterior, sin perjuicio de lo señalado en el número 2 letra i) del Título III y el número 1 letra b) del Título IV de este Capítulo.

6. Responsabilidad por la gestión.

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

Por otra parte, en cumplimiento de lo dispuesto en el Capítulo 20-8 de esta Recopilación, la institución 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.

7. Acceso a la información por parte del supervisor.

La entidad 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. Asimismo, como parte de la gestión de riesgo, la entidad deberá incorporar dentro del análisis aquellos aspectos relacionados con los riesgos legales a la que se expone la información sujeta a secreto o reserva bancaria establecida en la Ley General de Bancos.

IV. FACTORES A CONSIDERAR AL EXTERNALIZAR SERVICIOS DE PROCESAMIENTO DE DATOS.

La contratación de servicios externos de procesamiento de datos deberá estar respaldada por los antecedentes que se detallan el Anexo N° 2 de este Capítulo, además de considerar los factores que se indican más adelante.

Adicionalmente, en la evaluación que al efecto realice esta Comisión, con ocasión de sus actividades de fiscalización, se distinguirá atendiendo al tipo de servicios de que se trate.

1. Ubicación geográfica del proveedor

a) Servicios realizados en el país

Cuando el servicio de procesamiento de datos, total o parcial, se realice por una empresa situada en el país, la institución deberá comprobar que la infraestructura tecnológica y los sistemas que se utilizarán para la comunicación, almacenamiento y procesamiento de datos, ofrecen suficiente seguridad para resguardar permanentemente la continuidad del negocio, confidencialidad, integridad, exactitud y calidad de la información. Asimismo, deberá verificar que las condiciones del servicio garantizan la obtención oportuna de cualquier registro, dato o información que necesite, sea para sus propios fines o para cumplir con los requerimientos de las autoridades competentes, como es el caso de la información que en cualquier momento puede solicitarle esta Comisión.

En cuanto al Centro de Procesamiento de Datos de contingencia, éste deberá cumplir con condiciones de ubicación y distancia del Centro de Procesamiento de Datos principal, que garanticen la continuidad operacional.

b) Servicios realizados en el extranjero

En el caso que la entidad externalice servicios de procesamiento de datos 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.

Adicionalmente, la entidad debe disponer de los antecedentes del proyecto, del contrato de servicios y, en el caso de existir subcontratos con terceros, estos también deben ser incorporados.

Para resguardar el adecuado funcionamiento del mercado financiero con todos sus participantes, incluidos los clientes, las instituciones que realicen en el exterior actividades consideradas significativas o estratégicas, deberán mantener a disposición de esta Comisión los antecedentes contenidos en el Anexo N° 2 de este Capítulo y cumplir las siguientes condiciones para la externalización de los servicios:

i) Se debe contar con un Centro de Procesamiento de Datos de contingencia ubicado en Chile y demostrar un tiempo de recuperación compatible con la criticidad del servicio externalizado. Asimismo, los tiempos de recuperación deberán ser evaluados por la entidad al menos una vez al año, tanto para los procesos transaccionales como *Batch*.

Para el caso de bancos que mantengan una adecuada gestión del riesgo operacional en la última evaluación realizada por esta Comisión, calificada de conformidad con lo establecido en el Capítulo 1-13 de esta Recopilación, el Directorio o la instancia que haga sus veces podrá excepcionar este requerimiento, cuando se asegure, por medio de un informe anual, que la entidad cumple entre otros aspectos con la adopción de las siguientes medidas preventivas:

a) El tiempo de recuperación objetivo (RTO) debe ser aprobado por el directorio en función de un análisis de impacto (BIA) y de riesgo (RIA) que sea consistente con la criticidad del(os) servicio(s) externalizado(s). Lo anterior, debe ser evaluado y probado al menos anualmente.
b) Que los *sites* de procesamiento de datos cumplan con un tiempo de disponibilidad de operación igual o superior a lo dispuesto en el Capítulo 20-9 de esta Recopilación.
c) Que los *sites* se encuentran en ubicaciones distintas que mitiguen tanto el riesgo geográfico como los riesgos políticos.
d) Que en términos de seguridad de la información los servicios externalizados se provean en un ambiente consistente con las políticas y estándares adoptados por la entidad.

El informe mencionado deberá ser realizado por una empresa independiente de reconocido prestigio y experiencia en la evaluación de este tipo de servicios.

Consideraciones especiales

En el caso de entidades bancarias que mantengan servicios externalizados en el exterior, bajo las condiciones señaladas en este literal, y que producto de una nueva evaluación sean calificados en la materia de riesgo operacional en una categoría de "Cumplimiento Insatisfactorio" o inferior, deberán informar a esta Comisión sobre las medidas específicas adicionales adoptadas para asegurar la adecuada operación de los servicios.

Para aquellas entidades bancarias que no cuentan con una calificación de gestión en el ámbito del riesgo operacional, y que externalicen servicios en el exterior, le serán aplicables todas las medidas preventivas anteriormente señaladas, con excepción de la calificación en esta materia.

ii) La institución 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. Dichas actividades deben estar debidamente fundamentadas de acuerdo a 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.

2. Proveedores externos de canales electrónicos.

Las instituciones que requieran contratar servicios externos necesarios para operar con corresponsalías, es decir, aquellos proporcionados por empresas que ponen a disposición canales electrónicos y mantienen acuerdos con establecimientos comerciales para la prestación de ciertos servicios financieros por mandato de la entidad, deberán contemplar, en lo que sea aplicable, los aspectos indicados en el Anexo N° 1 y mantener permanentemente a disposición de esta Comisión, aquellos antecedentes señalados en el Anexo N° 3. Adicionalmente, la institución deberá de asegurarse del cumplimiento de lo establecido en el Capítulo 1-7 de esta Recopilación.

V. 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 de la banca.

Para efectos de contratar cualquier tipo de servicio a través de la modalidad denominada nube, el Directorio de la entidad deberá pronunciarse anualmente sobre la tolerancia 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 este Capítulo 20-7, las instituciones financieras 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 entidad 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 entidad 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 institución contratante y los proveedores, con la finalidad de minimizar los riesgos que podría aportar el rol de intermediario en este tipo de servicios.

d) La entidad 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 entidad 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 entidad 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 entidad 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 entidad.

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

VI. REVISIONES DE ESTA COMISIÓN

En sus visitas de inspección, esta Comisión examinará la gestión de riesgos que realiza la entidad sobre la externalización de servicios, como parte de las evaluaciones de que trata el Capítulo 1-13 de esta Recopilación.

En el caso de incumplimientos a esta normativa, en especial por aquellas entidades que hayan externalizado en el exterior actividades significativas o estratégicas o que las exponga a riesgos operacionales relevantes, este Organismo podrá requerir que los servicios se realicen en el país, o sean ejecutados internamente por la entidad, según corresponda. En consideración a lo anterior, la entidad deberá mantener permanentemente actualizado un plan que posibilite cumplir con esos eventuales requerimientos.

ANEXO N° 1

ASPECTOS MÍNIMOS QUE DEBEN CONSIDERARSE PARA LA EXTERNALIZACION DE SERVICIOS.

1. Evaluación del riesgo.

Antes de decidir la externalización de una actividad, se debe efectuar una evaluación, que considere a todos los agentes involucrados respecto de los riesgos que esta decisión incorpora a la institución, 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 entidad fiscalizada, la que deberá encontrarse debidamente sustentada.

2. Selección del proveedor de servicios.

La institución debe evaluar las propuestas recibidas de acuerdo a sus requerimientos y llevar a cabo un *due diligence* 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 entidad 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 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 de establecer una autorización permanente que permita tanto a esta Comisión como a la entidad fiscalizada examinar *in situ*, o en forma remota, según se disponga, en cualquier momento, todos los aspectos relacionados con el servicio contratado.

Adicionalmente, la institución 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 institución debe controlar el desempeño del proveedor y los posibles cambios en los requerimientos de la institución 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 institución 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

ANTECEDENTES ADICIONALES PARA LA EXTERNALIZACIÓN DE SERVICIOS DE PROCESAMIENTO DE DATOS

I. Información general

1. Estructura de gobierno definida entre la entidad y el proveedor, identificando claramente su nivel estratégico, táctico y operacional, tanto en la etapa de desarrollo del proyecto como de relacionamiento en régimen.
2. Estructura detallada de costos del procesamiento de datos actual y posterior al procesamiento externo (para los mismos ítems considerados).

II. Información del proyecto

1. Alcance detallado del servicio de procesamiento externo.
2. Identificación detallada de las plataformas y aplicaciones de negocios que se procesarán externamente y aquellas que se quedarán en la institución.
3. Documentos de respaldo del proyecto de procesamiento externo, que deben ser concordantes con la metodología de gestión de proyectos adoptada por la entidad.
4. Detalle de los ítems que se considerarán en el respectivo acuerdo tarifario.
5. Informe de análisis y evaluación de riesgo efectuado por una entidad independiente. Este informe debe incluir la matriz de riesgos del proyecto, la que debe contemplar al menos, la identificación de los procesos externalizados, la identificación de las fuentes y factores de riesgo que los afectan, el riesgo inherente, el impacto y probabilidad de ocurrencia, y una evaluación del diseño y operación de los controles para la determinación del riesgo residual resultante.
6. Evaluación técnica y financiera del proyecto.
7. Evaluaciones efectuadas para la selección de proveedores.
8. Detalle de la metodología de traslado utilizada en caso que corresponda (*hardware*, *software* y telecomunicaciones).
9. Metodología de certificación de pruebas y simulacros.
10. Criterios de aceptación establecidos para cada sub-etapa y actividades que conforman el proyecto.
11. Contrato de servicios (incluyendo todos los anexos) y en el caso de existir subcontratos con terceros estos también deben ser incorporados.
12. Políticas de seguridad de la información y continuidad de negocio del proveedor del servicio.
13. Descripción, antecedentes y características técnicas detalladas del sitio de producción y contingencia del proveedor de servicios y las certificaciones con que cuenta.
14. Carta GANTT detallada del proyecto de externalización.
15. Proceso y herramientas que le permitan a la entidad controlar la aplicación de sus políticas y buenas prácticas, en la empresa prestadora del servicio.
16. Proceso y herramientas que le permitirán controlar el cumplimiento de los niveles de servicios comprometidos en el contrato suscrito.
17. Estructura organizacional que estará encargada de las mantenciones de *hardware*, *software* y comunicaciones, especialmente al inicio del proceso externo.

18. Políticas y procedimientos que se utilizarán para la mantención de *software* operativo y comercial, tanto para aquellos que son de índole evolutivo y correctivo.

19. Plan de continuidad del negocio que adoptará la institución ante el evento de una contingencia que impida el procesamiento por parte del proveedor o los subcontratados por éste.

20. Planes de contingencia previstos para mantener la continuidad operacional de la entidad contratante en caso que se produzcan fallas en la comunicación o almacenamiento de la información.

ANEXO N° 3

ANTECEDENTES SOBRE SERVICIOS RELACIONADOS CON CANALES ELECTRÓNICOS PARA OPERAR CON CORRESPONSALÍAS

Se deberá mantener permanentemente a disposición de esta Comisión, según corresponda, los siguientes antecedentes debidamente actualizados:

1. Detalle de los productos ofrecidos a través de canales externos.
2. Modelo de negocios, incluyendo políticas comerciales y tarifarias.
3. Límites de operación (por monto, por día, por transacción, por RUT, etc.).
4. Criterios de selección de los comercios, calendario de apertura, características y localización geográfica.
5. Tipo de validaciones, dónde y quiénes las realizan durante el trayecto de la transacción, para efectos de autorizarla. Ejemplo: comercio registrado y vigente; vigencia del producto, del RUT, etc.
6. Políticas de seguridad física a los comercios, tales como seguros contra robos, asaltos o fraudes a los comercios.
7. Procedimientos de administración de la controversia ante probabilidad de fraudes tanto al comercio como al cliente.
8. Políticas de difusión en los puntos de atención.
9. Pruebas efectuadas al proyecto. Pruebas de funcionamiento del canal con todas las funcionalidades del *software*, pruebas de borde, pruebas de conectividad, pruebas de carga.
10. Descripción del modelo contable de la cuenta del comerciante. Detalle del flujo de efectivo para cada una de las operaciones.
11. Esquemas de monitoreos de canales para fraudes, lavado de activos, soporte, etc.
12. Modelo de atención de mesa de ayuda.
13. Contrato con los comercios, incluyendo anexos, en caso que corresponda.
14. Esquema tarifario con los Comercios.
15. Informes de auditoría interna relativos al proyecto, donde se pronuncie al menos sobre aspectos de control interno, seguridad de la información y continuidad operacional, antes del inicio del proyecto respectivo.
16. Políticas de selección y desvinculación de comercios, y de eventuales vetos a comercios que no cumplen con las políticas de la entidad.

ANEXO N° 4

EXTERNALIZACIÓN DE SERVICIOS NO ESTRATÉGICOS

El Directorio o el órgano que haga sus veces, debe definir qué elementos de este Capítulo no serán aplicables a aquellos servicios contratados en el país, debido a que comúnmente se vinculan con actividades que no tienen un carácter estratégico 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 bancarios, antecedentes de clientes y publicidad, entre otros.

iv) Otros: Servicios de arrendamiento.

Sin perjuicio de lo señalado, para estas actividades la entidad 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 entidad 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 este Capítulo, de acuerdo a las características particulares de cada institución.

———