CAPÍTULO 20-7

EXTERNALIZACIÓN DE SERVICIOS.

I. ÁMBITO DE APLICACIÓN.

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, funciones o procesos operativos, que podrían ser también efectuados internamente por la entidad, con sus propios recursos, tanto humanos como tecnológicos.

Las instrucciones contempladas en este Capítulo resultan también aplicables a las sociedades filiales y sociedades de apoyo al giro de que tratan los artículos 70 y 74 de la Ley General de Bancos, respectivamente.

Para los efectos de esta normativa se deberán considerar las siguientes definiciones:

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

Proveedor de servicios: entidad relacionada o no al banco 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 este (subcontrato de otros proveedores).

Actividades significativas o estratégicas:

i. actividades de importancia o críticas 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 del banco contratante.

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

iii. aquellas actividades de alta interacción sistémica en el mercado o que incorporan riesgos significativos a la entidad bancaria.

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 puede también acarrear riesgos estratégicos, reputacionales, de cumplimiento, de país, de concentración y contractuales, 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 dispuesto en la letra C) del numeral 3.2 del Título II del Capítulo 1-13 de la Recopilación Actualizada de Normas.

Medidas adicionales de mitigación deben ser consideradas al contratar un proveedor de servicios que concentre un número importante de entidades financieras, ya que ante una eventual falla de dicho proveedor se podría generar una crisis a nivel de la industria. Dichas medidas también deberán ser contempladas cuando se entreguen actividades significativas a un mismo proveedor.

III. CONDICIONES QUE DEBEN CUMPLIRSE EN LA EXTERNALIZACIÓN DE SERVICIOS

El banco que decida externalizar alguna actividad, debe dar cumplimiento a las siguientes condiciones:

1. Condiciones generales.

a) 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.

b) Establecer procedimientos formales para la selección, contratación y monitoreo de proveedores. Para estos efectos, se deberán considerar al menos los elementos detallados en el Anexo N° 1 de este Capítulo.

c) 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.

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

e) Velar por que existan auditorías independientes al proceso de selección, contratación y seguimiento de los proveedores, así como también que se cumpla con la normativa tanto interna como externa. Asimismo, deberá 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 Superintendencia.

f) 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 el banco y el proveedor de servicios inicial.

g) El banco debe incorporar en los 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 y la exposición a aquellos servicios considerados críticos.

h) Los datos, plataformas tecnológicas y aplicaciones a utilizar en la externalización de los servicios deben encontrarse en sitios de procesamiento específicos y en una jurisdicción definida y conocida.

2. Política de contratación y gestión de actividades asociadas al procesamiento externo

La política que corresponde ser sancionada por el Directorio del banco 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 de evaluación de riesgos y 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 sociedad relacionada;

e) Elementos que serán considerados por el banco 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, así como también las que en ningún caso deben externalizarse (ej. captación de dineros de terceros fuera de las oficinas del banco y la apertura de cuentas corrientes);

g) La revisión periódica de la política, especialmente, cuando existan cambios relevantes en el perfil de riesgo del banco;

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 el caso que el servicio a externalizar incluya la transmisión de antecedentes sujetos a reserva o secreto fuera del país. Sin perjuicio de lo anterior, cabe recordar que los servicios externalizados en Chile quedan sujetos a la misma obligación de reserva a la que se encuentra sujeto el banco.

3. Continuidad del negocio.

La institución bancaria debe verificar que sus proveedores de servicios críticos cuenten con planes apropiados que aseguren la continuidad de los servicios contratados. 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 el banco tomar conocimiento de dicha actividad y verificar los resultados obtenidos. Adicionalmente, la entidad bancaria también debe disponer de planes, igualmente probados, para asegurar la continuidad operacional ante la contingencia de no contar con dicho servicio externo.

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

El banco 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 los activos de información de la institución financiera y de sus clientes. Estas condiciones deben ser consistentes con las políticas y estándares adoptados por la entidad financiera y quedar incorporadas en el contrato de prestación de servicios.

La información una vez procesada, debe ser almacenada y transportada en forma encriptada, manteniéndose las llaves de desencriptación en poder del banco. Asimismo, se deben definir los procedimientos de intercambio de claves entre el proveedor de servicios y el banco, 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, el banco 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 al banco por parte del proveedor, y que éste en ningún caso mantenga información en su poder después de finalizada la relación contractual.

5. Riesgo país.

No se podrán externalizar servicios en jurisdicciones que no cuenten con calificación de riesgo país en grado de inversión. No obstante, sin perjuicio de la necesaria evaluación de los riesgos involucrados, las sucursales o filiales de bancos extranjeros podrán encargar la prestación de servicios a otras subsidiarias del mismo banco que se encuentren situadas en países con una calificación distinta a grado de inversión.

En el caso de entidades que mantengan servicios externalizados en países que pierdan su grado de inversión, deberán informar a esta Superintendencia sobre el efecto que puede producir, o bien producirá este hecho, en la calidad e idoneidad de los servicios contratados.

6. Responsabilidad por la gestión.

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

Por otra parte, el banco deberá comunicar a esta Superintendencia de forma inmediata cualquier evento derivado de la externalización de un servicio determinado, que pueda implicar el incumplimiento por parte del banco de instrucciones legalmente impartidas por esta Superintendencia, de obligaciones para con los clientes de la entidad o bien que signifiquen fallas graves en los servicios externalizados.

7. Acceso a la información por parte del supervisor.

La institución bancaria contratante debe asegurarse que esta Superintendencia tenga acceso permanente, sea mediante visitas a los lugares de procesamiento 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.

En el caso de tratarse de un proveedor de servicios establecido en el exterior, el banco debe prestar especial atención a las restricciones legales del país anfitrión que pudieren impedir la visita de esta Superintendencia 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

La contratación de servicios externos de procesamiento de datos deberá estar respaldada por los antecedentes que se detallan en 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 este Organismo, 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 bancaria 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 y los datos. 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 Superintendencia.

Para aquellos servicios que requieran de un Centro de Procesamiento de Datos de contingencia, este deberá cumplir con condiciones de ubicación y distancia del Centro de Procesamiento de Datos principal, que garanticen su operación.

b) Servicios realizados en el extranjero

En el caso que el banco pretenda externalizar servicios fuera del país deberá disponer en todo momento de los antecedentes necesarios de la empresa con la cual contratará el servicio. En especial, deberá mantener aquellos antecedentes que respalden la solidez financiera del proveedor del servicio, que la organización y el personal a cargo de este posean adecuados conocimientos y experiencia en el servicio contratado, y que mantiene certificaciones de calidad, seguridad y apropiados sistemas de control. Adicionalmente, el banco debe disponer de los antecedentes del proyecto, del contrato de servicios y, en el caso de existir subcontratos con terceros, también deben ser incorporados.

Para resguardar el adecuado funcionamiento del mercado financiero con todos sus participantes, incluidos los clientes, los bancos que realicen en el exterior actividades consideradas significativas o estratégicas, deberán mantener a disposición de esta Superintendencia, 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 alternativo o 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*.

ii) El banco debe efectuar desde Chile el control y monitoreo del servicio externalizado en el Centro de Procesamiento de Datos 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. Lo anterior, independiente de las actividades propias de control y monitoreo que realice el proveedor del servicio.

En cuanto a los centros de Procesamiento de Datos principal y alternativo, estos deberán tener una infraestructura que les permita contar al menos con capacidad de mantenimiento simultáneo, además de una ubicación y distancia, que garanticen su operación bajo escenarios de indisponibilidad que puedan afectarlos.

2. Proveedores externos de canales electrónicos.

Los bancos que requieran contratar servicios externos necesarios para operar con corresponsalías y con medios de pago electrónicos, 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 del banco, deberán contemplar, en lo que sea aplicable, los aspectos indicados en el Anexo N° 1 y mantener permanentemente a disposición de la Superintendencia, aquellos antecedentes señalados en el Anexo N° 3. Adicionalmente el banco, deberá de asegurarse del cumplimiento de lo establecido en el Capítulo 1-7 de esta Recopilación.

V. REVISIONES DE ESTA SUPERINTENDENCIA

En sus visitas de inspección, esta Superintendencia examinará la gestión de riesgos que realiza la entidad sobre la externalización de servicios, como parte de la evaluación de la administración del riesgo operacional contemplada en el Capítulo 1- 13 de esta Recopilación.

En el caso de incumplimientos a esta normativa, en especial por aquellos bancos que hayan externalizado en el exterior actividades significativas o estratégicas o que les 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, el banco deberá mantener permanentemente actualizado un plan que posibilite cumplir con esos eventuales requerimientos.

———

ANEXO N° 1

ASPECTOS MÍNIMOS A CONSIDERAR PARA LA CONTRATACION DE PROCESAMIENTOS EXTERNOS

1. Evaluación del riesgo.

Antes de decidir el procesamiento externo 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 del banco, 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 que los servicios contratados se realicen con un proveedor relacionado al banco, las condiciones económicas de aquellos deben cumplir con principios de transparencia y equidad, aspectos que deben estar definidos en la política que regula las actividades asociadas al procesamiento externo.

3. Contrato.

La entidad financiera 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, 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 software, además de establecer una autorización permanente que permita a esta Superintendencia como al banco examinar *in situ*, en cualquier momento, todos los aspectos relacionados con el servicio contratado**.** Los costos en que incurra esta Superintendencia por la supervisión del procesamiento de datos en el lugar dispuesto por el proveedor de servicios, serán de cargo de la respectiva institución bancaria.

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 documentos deberán estar en idioma español o bien con las traducciones que correspondan debidamente legalizadas, y con las correspondiente rúbrica 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

I. Información general

1. Estructura de gobierno definida entre el banco 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 el banco.
3. Documentos de respaldo del proyecto de procesamiento externo.
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 proceso 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. Borrador del 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 institución financiera 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 el banco 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 institución contratante en caso que se produzcan fallas en la comunicación o almacenamiento de la información.

ANEXO N° 3

ANTECEDENTES RELATIVOS A SERVICIOS RELACIONADOS CON CANALES ELECTRÓNICOS PARA OPERAR CON CORRESPONSALÍAS Y MEDIOS DE PAGO ELECTRÓNICOS

1. Detalle de los productos que se van a ofrecer 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. Borrador de 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.

——————