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 Superintendencia.

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.

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 entidades extranjeras podrán encargar la prestación de servicios a otras subsidiarias de la misma entidad que se encuentren situadas en países con una calificación distinta a grado de inversión, en actividades que no sean consideradas significativas o estratégicas.

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 este hecho produjo, o se estima que producirá, 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 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 en forma inmediata a esta Superintendencia, cuando corresponda, los incidentes operacionales relevantes 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 Superintendencia 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 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 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 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 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 Superintendencia.

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 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 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) La institución debe efectuar 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. 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 la Superintendencia, 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 la Superintendencia, 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 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 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 Superintendencia 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.