Superintendencia de Bancos e Instituciones Financieras Chile

CIRCULAR

Bancos

Santiago,

RECOPILACIÓN ACTUALIZADA DE NORMAS. Capítulo 20-7.

Externalización de servicios. Servicios de procesamiento de datos realizados en el extranjero. Modifica instrucciones.

Con el propósito de que las entidades bancarias puedan hacer uso de aquellas innovaciones tecnológicas que permiten hacer más eficientes los mercados en que participan, pero siempre compatibilizándolo con una sólida gestión de los riesgos operacionales que ello involucra, mediante la presente Circular se modifican las condiciones que deben cumplir las instituciones fiscalizadas, en el caso que se externalicen servicios de procesamiento de datos fuera del país, según lo dispuesto en el Capítulo 20-7 de la Recopilación Actualizada de Normas.

Para dichos efectos, el Directorio podrá exceptuar al banco de la exigencia de disponer de un centro de procesamiento de datos de contingencia en el país, para las actividades consideradas significativas o estratégicas, siempre y cuando, además de contar con una adecuada calificación de gestión en la materia de riesgo operacional en las dos últimas evaluaciones realizadas por esta Superintendencia, de acuerdo con lo establecido en el Capítulo 1-13 de la referida Recopilación, asegure mediante un informe anual, que la entidad ha adoptado las medidas preventivas mínimas definidas por esta Superintendencia.

Cabe mencionar que estas modificaciones también deben ser compatibilizadas con los lineamientos mínimos para el uso de servicios externalizados en modalidad nube (*cloud computing)*, que fueron introducidos al Capítulo 20-7 mediante la Circular N° 3.629 de 27 de diciembre de 2017.

En concordancia con lo señalado, se introduce el siguiente párrafo segundo en el literal i) de la letra b) del numeral 1 del Título IV del mencionado Capítulo:

"Para el caso de bancos que mantengan una adecuada gestión del riesgo operacional en las dos últimas evaluaciones de esta Superintendencia, 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 a dicha instancia, por medio de un informe anual, que la entidad cumple al menos con la adopción de las siguientes medidas preventivas:

a) Que los servicios externalizados, en caso de indisponibilidad, no sobrepasen dos horas como tiempo de recuperación objetivo (RTO).
b) Que los *sites* de procesamiento de datos cumplen con un tiempo de disponibilidad de operación de al menos 99,995% o *downtime* anual de 0,8 horas.
c) Que los *sites* se encuentran en ubicaciones distintas que mitigan el riesgo geográfico y 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 el servicio que otorga".

En otro orden de cosas, se introduce un ajuste de concordancia en segundo párrafo del numeral 2 del Título III.

Como consecuencia de los cambios descritos se reemplazan las hojas N°s 7, 9 y siguientes del Capítulo 20-7, por las que se acompañan.

Saludo atentamente a Ud.,

MARIO FARREN RISOPATRÓN
Superintendente de Bancos e Instituciones Financieras

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 a esta Superintendencia, 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 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.

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*.

Para el caso de bancos que mantengan una adecuada gestión del riesgo operacional en las dos últimas evaluaciones de esta Superintendencia, 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 al menos con la adopción de las siguientes medidas preventivas:

a) Que los servicios externalizados, en caso de indisponibilidad, no sobrepasen dos horas como tiempo de recuperación objetivo (RTO).
b) Que los *sites* de procesamiento de datos cumplen con un tiempo de disponibilidad de operación de al menos 99,995% o *downtime* anual de 0,8 horas.
c) Que los *sites* se encuentran en ubicaciones distintas que mitigan el riesgo geográfico y 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 actualizado anualmente y realizado por una empresa independiente de reconocido prestigio y experiencia en el servicio que otorga.

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.