COMISIÓN
PARA EL MERCADO
FINANCIERO

Informe Normativo

Modificación Capítulo 20-7
Externalización de Servicios

Diciembre 2019

Informe Normativo

Modificación Capítulo 20-7

Externalización de Servicios

diciembre 2019

Contenido

I. Introducción

El Capítulo 20-7 de la Recopilación Actualizada de Normas (RAN), entrega los lineamientos que deben observar las entidades al externalizar servicios en el país o en el extranjero en la gestión del riesgo operacional. Uno de los requerimientos que establece en el caso de que una entidad externalice servicios de procesamiento de datos fuera del país que afecten actividades consideradas significativas o estratégicas[1], es que se debe contar con un centro de procesamiento de contingencia ubicado en Chile. Esta exigencia es aplicable a bancos y se hace extensiva a filiales, sociedades de apoyo al giro bancario, y operadores de tarjetas de pago no bancarios.

El nuevo entorno creciente de innovación y desarrollo del mercado financiero ha hecho necesario que las entidades incursionen en nuevos modelos tecnológicos, requiriéndose en ocasiones de proveedores especializados de servicios que son considerados críticos ubicados en el extranjero, lo que ha impulsado la necesidad de flexibilizar la condición de mantener un *site* en Chile a fin de permitir la innovación y el desarrollo de los mercados.

A raíz de esto se hace necesario flexibilizar la disposición mencionada en la normativa, considerando que el impacto de este requerimiento podría desalentar a las instituciones financieras a adoptar las nuevas tendencias de transformación digital, imposibilitados de asumir el costo de instalar un sitio de procesamiento en Chile, lo cual constituye una importante barrera de entrada y por ende, afectar al desarrollo de la industria y la generación de competencia.

II. Objetivo del Cambio en la Normativa

La modificación busca avanzar hacia un esquema en el cual los directorios podrán excepcionar la exigencia, tanto de contar con un centro de procesamiento de datos de contingencia en el país para las actividades externalizadas consideradas significativas o estrategias, siempre y cuando el directorio se asegure que las respectivas entidades cumplan con ciertos requerimientos regulatorios, así como la de externalizar servicios sólo en jurisdicciones que cuenten con calificación de riesgo país en grado de inversión.

III. Regulación actual

El Capítulo 20-7, establece los lineamientos que deben observar las entidades al externalizar servicios en el país o en el extranjero en la gestión del riesgo operacional. Desde su promulgación en el año 2000, ha sido modificada en varias oportunidades con el objeto de ir alineando la normativa local a los mejores estándares internacionales en regulación bancaria.

[1] El mismo Cap. 20-7 define como actividades significativas o estratégicas (críticas) las siguientes:

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.

El detalle de las principales modificaciones ocurridas desde su promulgación se presenta a continuación:

- En julio del año 2000 se emite la normativa, que establecía requerimientos para el procesamiento de datos, tanto a nivel de servicios prestados como servicios contratados con terceros. En este contexto, la norma entregaba la posibilidad de que una institución financiera establecida en Chile procesara datos a otras entidades bancarias o financieras relacionadas por propiedad, previa autorización por parte de este Organismo. Asimismo, establecía la posibilidad de entregar el procesamiento de sus datos a una empresa externa, en la medida que se cumplieran ciertas condiciones contractuales que resguardaran la confidencialidad de la información y aseguraran su control sobre el riesgo operativo y tecnológico.
- En marzo del año 2008 se estableció la necesidad de solicitar autorización a este Organismo cuando se encargara a otra empresa situada en Chile o en el exterior, el procesamiento parcial o total de sus datos. Esta medida se aplicó debido a que se observó, tanto en el ámbito global como en el sistema financiero, un incremento en la contratación de servicios de terceros para el desarrollo de ciertas actividades significativas. Además, se instauró la exigencia de que los bancos que sean calificados como sistémicamente relevantes que decidieran externalizar el procesamiento de datos en el exterior, debían contar con un centro de procesamiento de datos alternativo o de contingencia ubicado en Chile.
- En octubre del año 2014 se eliminó el requisito de autorización previa de este Organismo para externalizar servicios en el exterior por parte de las instituciones financieras, y se establecieron nuevas disposiciones para una autorregulación, lo cual conllevó a una mayor responsabilidad para las entidades fiscalizadas debido a que en el caso de incumplimientos a esta normativa, esta Comisión puede requerir que los servicios se realicen en el país, o sean ejecutados internamente por la entidad. Por otra parte, se amplió el requisito de contar con un sitio de contingencia en Chile a cualquier entidad que externalice actividades significativas o estratégicas en el exterior.
- En diciembre del año 2017, como consecuencia de la evolución de los servicios informáticos que apoyan la actividad bancaria, se incorporan los lineamientos mínimos para el uso de servicios externalizados en modalidad *cloud computing*. Adicionalmente, se incluyeron instrucciones en el ámbito de la seguridad de la información y continuidad del negocio, que aplican a la externalización de servicios en general.

IV. Jurisdicciones Extranjeras

Del análisis de la normativa de supervisores de distintas jurisdicciones sobre la externalización de servicios, se observa que, si bien existen requerimientos específicos cuando éstos son otorgados fuera del país, no se contempla el requerimiento de contar con un sitio de procesamiento alternativo en territorio nacional. Por otra parte, de la normativa analizada, sólo la emitida por el Organismo supervisor de Uruguay exige que los países donde se externalicen servicios de procesamiento de datos, considerados significativos a juicio de la Superintendencia de ese país, cuenten con una categoría de inversión igual o superior a BBB- o equivalente. Un resumen de dichas normativas se presenta a continuación.

Argentina[2]

El Banco Central de la República Argentina (B.C.R.A), organismo rector del sistema financiero de ese país, establece que las entidades financieras pueden tercerizar actividades previa comunicación a la Superintendencia de Entidades Financieras y Cambiarias (SEFyC) antes de 60 días de la fecha de inicio de esas actividades. Esto, siempre que las funciones a externalizar no consistan en la atención de clientes y/o el público general.

Con los proveedores externalizados se deberán suscribir contratos sobre el alcance y las condiciones de las actividades que se tercericen. Los contratos deberán fijar como mínimo: el alcance de las actividades; los niveles mínimos de prestación; la participación de subcontratistas; los derechos a realizar auditorías por parte de la entidad; compromisos de confidencialidad; los mecanismos de resolución de disputas; la duración del contrato; cláusulas de terminación del contrato; los mecanismos de notificación en cambios del gerenciamiento; el procedimiento por el cual la entidad pueda obtener los datos, los programas fuentes, los manuales y la documentación técnica de los sistemas, ante cualquier situación que pudiera sufrir el proveedor externo por la cual dejara de prestar sus servicios o de operar en el mercado, a fin de poder asegurar la continuidad de procesamiento. Además, los contratos deben establecer claramente la "no existencia" de limitaciones para la Superintendencia en cuanto a: el acceso a los datos y a toda documentación técnica relacionada y a la realización de auditorías periódicas en las instalaciones del proveedor, a fin de verificar el cumplimiento de todos los aspectos contemplados en estas normas.

En cuanto al tipo de servicio tecnológico que se puede externalizar, las entidades financieras pueden contratar, en forma total o parcial, los servicios provistos por terceros referidos a: Infraestructura de Tecnología y Sistemas; Procesamiento de Datos; Soporte, Prevención y Mantenimiento; Comunicaciones; Almacenamiento y Custodia; Desarrollo de Aplicaciones; Contingencia y Recuperación.

Uruguay[3]

De acuerdo con la regulación uruguaya, las instituciones deben solicitar autorización previa de la Superintendencia de Servicios Financieros para la contratación de terceros para la prestación de servicios inherentes a su giro. Las empresas que presten tales servicios deben someterse a las mismas normas que las que rigen cuando son cumplidas por las entidades controladas, con excepción de aquellas de carácter sancionatorio. Se hace mención de que no se puede tercerizar la aceptación de clientes ni la ejecución de operaciones con valores por cuenta de clientes y que la tercerización del procesamiento de datos está sujeta a mayores restricciones.

Dentro de lo definido para la tercerización del procesamiento de datos se encuentra que la institución debe acreditar que los procedimientos de resguardo de datos y *software* satisfacen

[2] Sección 2 del Texto Ordenado de las normas sobre "Expansión De Entidades Financieras"; Sección 7 del Texto Ordenado de las normas sobre "Requisitos Mínimos de Gestión, Implementación, y Control de los Riesgos relacionados con Tecnología Informática, Sistemas de Información y Recursos Asociados para las Entidades Financieras"; Sección 5 del Texto Ordenado de las normas sobre Requisitos Operativos Mínimos del Área de Sistemas de Información (Si) - Tecnología Informática, todos emitidos por el B.C.R.A.

[3] Capítulo VI – BIS – Tercerización de Servicios de la Recopilación de Normas de Regulación y Control del Sistema Financiero.

ciertas condiciones y que la infraestructura tecnológica y los sistemas que se emplean para la comunicación, almacenamiento y procesamiento de datos ofrecen seguridad suficiente, así como para resguardar permanentemente la continuidad operacional.

Cuando el procesamiento externo de la información se realice en el extranjero, las instituciones deberán, además, prestar particular atención a los requerimientos legales y regulatorios existentes en la jurisdicción anfitriona así como a las potenciales condiciones políticas, económicas y sociales u otros eventos que puedan conspirar contra la habilidad del proveedor de cumplir satisfactoriamente con las obligaciones acordadas. Estos elementos deben cumplirse tanto al momento de la selección inicial del proveedor como al momento de eventuales renovaciones de contrato.

Con relación al resguardo de la información en el exterior, una de las copias debe radicarse físicamente en el Uruguay y permanecer accesible al Organismo supervisor en un plazo no mayor al que fije la Superintendencia en función del lugar del procesamiento.

Cuando el procesamiento de datos en el exterior sea considerado significativo a juicio de la Superintendencia se debe cumplir con las siguientes condiciones:

a) El país donde se realice el procesamiento y el país donde se brinde la contingencia para la continuidad operacional, en caso de que fuera diferente, deberán estar calificados en una categoría igual o superior a BBB- o equivalente.
b) La institución que solicite procesar la información en otro país o el grupo financiero que integre, debe tener habilitación como institución financiera en aquel país, así como en el país seleccionado para brindar la contingencia para la continuidad operacional si este último fuera diferente del primero.
c) Las empresas que realicen el procesamiento y brinden la contingencia deben integrar el grupo financiero al cual pertenece la institución que solicite procesar la información en el exterior.
d) El procesamiento o el suministro de la contingencia para la continuidad operacional sea realizada por un banco del exterior calificado en una categoría no inferior a BBB+ o equivalente.

Panamá[4]

La Superintendencia de Bancos de Panamá establece que se podrán externalizar ciertos servicios sin necesidad de solicitar autorización a esa Superintendencia (actividades administrativas, servicios generales, mercadeo, distribución y logística, transporte de valores, centros de llamada, entre otros). Sin embargo, el resto de los contratos de tercerización de servicios requieren de una autorización de la Superintendencia de Bancos. El análisis de la solicitud de autorización se realiza en un término no mayor de 30 días hábiles, y hasta tanto la entidad bancaria no sea notificada de la decisión adoptada, no puede llevar a cabo la tercerización solicitada.

Por otra parte, pueden tercerizarse sin dicha autorización previa, los servicios tecnológicos que no involucren procesos en los que se pueda afectar la confidencialidad, la integridad, la

[4] Acuerdo N°009-2005 de Tercerización u Outsourcing y Circular N° 064-2006, emitidos por la Superintendencia de Bancos de Panamá.

disponibilidad o la custodia de los bienes de clientes, y que no representan un riesgo para la subsistencia e imagen del banco. Esto aplica únicamente para los servicios tecnológicos que pueden ser directamente provistos por un banco.

Asimismo, se establece que las entidades bancarias que tengan sus centros de procesamientos tecnológicos en el extranjero (casas matrices, etc.) deben contar con acuerdos de servicio internos que garanticen el cumplimiento de las distintas disposiciones definidas en la normativa.

Por último, la normativa establece que todo banco que tercerice las funciones o procesos de TI deberá asegurarse que en el contrato de tercerización se incluyan las siguientes condiciones:

1. La obligación de la empresa contratada de permitir a la Superintendencia de Bancos, cuando ésta así lo requiera, el acceso a la infraestructura de TI, a los sistemas de información y bases de datos (en la medida de lo permitido en la Ley Bancaria), en lo que se refiere al servicio tercerizado por el banco.
2. La obligación de la empresa contratada de remitir al banco toda la información que requiera la Superintendencia respecto al servicio tercerizado por el banco, en la medida de lo permitido en la Ley Bancaria.

Colombia[5]

En el caso de la Superintendencia Financiera de Colombia, se emitió normativa respecto de los servicios contratados en la nube, frente a los cuales se les exige a las instituciones fiscalizadas cumplan una serie de requisitos, como son: contemplar dentro de su Sistema de Administración de Riesgo Operativo (SARO) la gestión de los riesgos derivados de la utilización de servicios en la nube; establecer criterios de selección; verificar que el proveedor cuente con certificaciones; que el proveedor ofrezca una disponibilidad de al menos el 99.95%; verificar que las jurisdicciones en donde se procesa la información cuenten con normas equivalentes o superiores a las aplicables en Colombia; mecanismos de respaldo; cifrado de la información; control de la administración de usuarios y de privilegios; monitoreo de los servicios; entre otros elementos.

Asimismo, esta norma define los elementos mínimos que deben contemplar los contratos o acuerdos que se suscriban con los proveedores, así como en la administración de la continuidad del negocio.

Adicionalmente, establece que, dentro de los 15 días anteriores al inicio del procesamiento de información en la nube, relacionada con procesos misionales[6] o de gestión contable y financiera, las entidades deben remitir cierta información básica respecto del servicio contratado, como es el nombre del proveedor, procesos que son manejados en la nube, ubicación física o región donde se procesan los datos, certificaciones del proveedor, auditorías, niveles de servicios y el diagrama de la plataforma.

[5] Instrucciones Generales Aplicables a las Entidades Vigiladas, Título I, Capítulo VI: Reglas Relativas al Uso de Servicios de Computación en la Nube, emitida por la Superintendencia Financiera de Colombia.

[6] Procesos Misionales: son aquellos procesos que contribuyen directamente al resultado previsto por la entidad en cumplimiento de su objeto social. Estos procesos están relacionados con la naturaleza, misión, objetivos y función de la entidad y no están asociados a actividades de apoyo o complementarias.

México[7]

En México, la normativa emitida por la Comisión Nacional Bancaria y de Valores, establece ciertos elementos mínimos a considerar cuando se externalizan servicios de cualquier índole, como son contar con un informe que especifique los procesos operativos o de administración de bases de datos y sistemas informáticos; indicar en los contratos que se pueden hacer visitas por parte de auditoría (interna o externa); que se deben poder entregar libros, sistemas, registros, manuales y documentos en general en caso de que la institución o la comisión lo solicite; que se debe contar con políticas y procedimientos; se debe resguardar la confidencialidad de la información y la continuidad operacional; entre otros elementos.

Además, define que para el caso en que se requiera la contratación de terceros para la realización de un proceso operativo o para la administración de bases de datos y sistemas informáticos, se deberá dar aviso a la Comisión, previamente a la contratación con terceros, con una anticipación de por lo menos veinte días hábiles a la fecha en que pretendan contratar dichos servicios y precisando el proceso operativo o de administración de bases de datos y sistemas informáticos objeto de los servicios. La Comisión tiene la facultad de requerir que la prestación de dicho servicio no se realice a través del tercero.

Por otro lado, cuando la realización de un proceso se proporcione o ejecute parcial o totalmente fuera de territorio nacional, las Instituciones tienen que requerir autorización de la Comisión para la contratación del tercero. Esta solicitud debe hacerse con al menos 20 días hábiles de anticipación y acompañar con cierta documentación: Que los terceros con los que se contrate residan en países cuyo derecho interno proporcione protección a los datos de las personas, resguardando su debida confidencialidad, o bien, los países de residencia mantengan suscritos con México acuerdos internacionales en dicha materia. Así como que las instituciones manifiesten a la Comisión que mantendrán en sus oficinas principales ubicadas en México al menos la documentación e información relativa a las evaluaciones, resultados de auditorías y reportes de desempeño.

Nicaragua[8]

En Nicaragua, la normativa emitida por la Superintendencia de Bancos y de Otras Instituciones Financieras (SIBOIF), establece los requisitos mínimos que las entidades supervisadas deben cumplir para la contratación de terceros proveedores de servicios para la realización de actividades u operaciones de manera continua o temporal.

Dicha norma define las responsabilidades de la junta directiva, de la gerencia o la instancia de administración integral de riesgos, los elementos que debe incluir la política de contratación y las obligaciones con la Superintendencia y con los clientes. Adicionalmente, define el concepto de materialidad e insta a las instituciones a determinarla, junto con una evaluación de riesgos previo a la contratación. Asimismo, detalla los elementos mínimos que deben contener los contratos de servicios y el monitoreo que se debe realizar a dichos proveedores.

[7] Disposiciones de Carácter General Aplicables a las Instituciones de Crédito, Titulo Quinto, Capítulo XI, Sección Tercera: De la contratación con terceros de servicios o comisiones que tengan por objeto la realización de procesos operativos o administración de bases de datos y sistemas informáticos, emitidas por la Comisión Nacional Bancaria y de Valores.

[8] Norma sobre la Contratación de Proveedores de Servicios para la realización de operaciones o servicios a favor de las Instituciones Financieras, emitida por el Consejo Directivo de la Superintendencia de Bancos y de Otras Instituciones Financieras.

Menciona también que, cuando el proveedor de servicios se encuentre en otro país o jurisdicción, la institución financiera debe identificar las implicaciones que podrían resultar de la discrepancia entre las exigencias legales de ambos países. Las razones también deberán considerar el impacto global de todas las contrataciones de operaciones en la estabilidad y seguridad de la institución financiera. Adicionalmente, el programa de administración de riesgos deberá contemplar el ambiente político y económico, sofisticación tecnológica y el perfil de riesgo legal de la jurisdicción extranjera.

En general las instituciones financieras deben notificar a la Superintendencia de cualquier impacto significativo negativo que afecte el desarrollo del servicio y el Superintendente puede suspender, limitar o prohibir la contratación de cierto tipo de operaciones o servicios a terceros, tomando en consideración la materialidad del acuerdo de contratación y la protección del interés público en la intermediación financiera, de manera particular o general.

V. Propuesta Normativa Inicial

La Comisión trabajó en el desarrollo de una modificación que contiene un modelo en el cual los directorios pueden excepcionar disponer de un centro de procesamiento de datos de contingencia en el país, para las actividades consideradas significativas o estrategias. Lo anterior a fin de facilitar el ingreso de nuevos actores al mercado, y contribuir al desarrollo de la industria y a la generación de competencia.

Para esto el directorio podría excepcionar esta condición bajo el cumplimiento de determinados requisitos, sustentados en un informe anual de una empresa de reconocido prestigio.

Los requisitos establecidos para efectuar la excepción fueron:

- En el caso particular de los bancos, contar con una adecuada calificación de gestión de riesgo operacional en las dos últimas revisiones de la Comisión.
- En caso de indisponibilidad de los servicios críticos externalizados el Tiempo de Recuperación Objetivo (RTO) no debe sobrepasar las dos horas.
- Los *sites* de procesamiento de datos cumplan con un tiempo de disponibilidad de operación de al menos 99,995% o *downtime* de 0,8 horas anuales.
- Los *sites* se encuentran en ubicaciones distintas mitigando riesgos geopolíticos.
- Ambiente de seguridad de la información consistente con sus políticas.

VI. Proceso de Consulta Pública

Con fecha 27 de mayo de 2019, la CMF dio inicio al proceso de consulta pública de la propuesta normativa relativa a la “Modificación al Capítulo 20-7, de la Recopilación Actualizada de Normas (RAN) sobre externalización de servicios, y a la Circular N° 2 para empresas emisoras de tarjetas de pago no bancarias y empresas operadores de tarjetas de pago, en relación a la misma materia”, poniendo a disposición del público, tanto el contenido de la propuesta como una infografía con los principales elementos del cambio.

Posteriormente, con fecha 28 de junio del 2019, se amplió el plazo de la consulta pública, recibiéndose comentarios a la propuesta normativa hasta el 19 de julio de 2019. En total se recibieron 18 documentos con comentarios, los cuales de desglosan de la siguiente forma:

- Empresas fiscalizadas: 9
- Otras empresas: 7
- Asociaciones gremiales: 2

Los comentarios recogidos durante la consulta pública mediante el sitio web de la CMF fueron cuidadosamente analizados y considerados, de manera de conseguir que la propuesta normativa aborde los temas e inquietudes que parecen adecuados.

Descripción de Comentarios:

1. Se solicita incorporar una excepción en el ítem de Riesgo País para aquellas jurisdicciones que, si bien no cumplen con la calificación de grado de inversión si sean considerados como "adecuadas" según estándares internacionales de protección de datos.

Respuesta de la CMF:
Si bien el punto de Riesgo País no se encontraba sujeto a consulta, se introducen modificaciones que flexibilizan el requerimiento de calificación de grado de inversión para las jurisdicciones donde las instituciones financieras externalicen servicios en el exterior. En efecto, el directorio puede excepcionar dicho requisito en la medida en que el país en el que se externalizan los servicios cuente con leyes de protección y seguridad de datos personales adecuadas.

2. Seis de los comentarios solicitaron eliminar la condición de contar con una adecuada calificación de gestión en la materia de riesgo operacional en las dos últimas evaluaciones de la CMF.

Respuesta de la CMF:
Se acoge parcialmente la solicitud, dejando como requisito sólo la última evaluación de esta Comisión, debido a que para este Organismo es de vital importancia que las entidades que opten a esta alternativa que flexibiliza la norma, cumplan con adecuados estándares en cuanto a la gestión de sus riesgos operacionales, siendo la evaluación de la materia una de las maneras de validar este punto.

3. Cuatro de los comentarios solicitaron aclaración respecto a cuáles son las entidades que deben cumplir con la totalidad de las exigencias y formalidades establecidas en este cambio normativo.

Respuesta de la CMF:
Se acoge la solicitud, explicitando que las condiciones son aplicables a todas las entidades, con excepción de la calificación de gestión que es sólo para bancos. Para ello se establece de manera explícita que este requisito solo aplica para las entidades bancarias.

4. Nueve de los comentarios solicitan que el tiempo de recuperación objetivo (RTO) exigido sea aquel definido por la entidad para cada uno de sus procesos y no dos horas como se propone en la norma en consulta.

Respuesta de la CMF:
Se acoge la solicitud, dejando como requisito que el tiempo de recuperación objetivo (RTO) sea aprobado por el directorio en función del análisis de impacto (BIA) y de riesgo (RIA), siendo consistente con la criticidad de los servicios externalizados. Esto considerando que para este Organismo es de vital importancia que las entidades que opten por la alternativa de prescindir de un *site* de contingencia en Chile cuando externalicen servicios críticos en el exterior, deban cumplir con adecuados estándares en cuanto a la gestión de sus riesgos operacionales, y particularmente en este caso en el ámbito de la continuidad del negocio.

5. Ocho de los comentarios indican que la exigencia del 99,995% de disponibilidad de servicio (*uptime*) para los *sites* de procesamiento externos es equivalente a un estándar Tier 4, lo que resulta restrictivo para externalizar estos servicios, motivo por el cual solicitan flexibilizar este requisito a un estándar Tier 3.

Respuesta de la CMF:
Se acoge la solicitud de modificar el tiempo de disponibilidad de operación, estableciéndolo como un valor igual o superior a lo dispuesto en el Capítulo 20-9 de la RAN (99,98%).

6. Dos de los comentarios recomiendan la aceptación de certificaciones internacionales de seguridad de la información para evaluar que se han adoptado las mejores prácticas internacionales en esta materia, considerando que es la forma más práctica y correcta para abordar la materia.

Respuesta de la CMF:
Este Organismo estima que la adopción de estándares internacionales por parte de los proveedores de servicios si bien se consideran una buena práctica, estas son condiciones generales que no aseguran los riesgos específicos de cada institución. Además, la experiencia empírica ha demostrado que empresas con certificaciones internacionales han sido afectadas por eventos relevantes, producto que los controles que mantienen a propósito de las certificaciones no son específicos a su tipo de negocio.

7. Dos de los comentarios sugieren autorizar a las entidades para realizar internamente el informe anual de evaluación del cumplimiento de los requisitos establecidos.

Respuesta de la CMF:
Este Organismo considera que para que sea de mayor utilidad debe ser un informe independiente, emitido por una empresa de reconocido prestigio y experiencia en la evaluación de este tipo de servicios, debido a que las autoevaluaciones han demostrado no ser del todo efectivas.

8. Siete de los comentarios solicitan reemplazar la generación de un informe independiente por certificaciones internacionales, dado que si el proveedor está certificado se entiende que cumple el estándar y no es necesario emitir un informe al respecto.

Respuesta de la CMF:
Como se mencionó anteriormente, si bien la adopción de estándares internacionales se consideran una buena práctica, estas evalúan condiciones generales que no aseguran los riesgos específicos de cada institución.

Adicionalmente, se recibieron una serie de comentarios, no directamente asociados a esta modificación normativa, los cuales fueron analizados uno a uno, sin embargo, no se consideran para este cambio en particular.

VII. Normativa Emitida

La normativa a ser emitida se elaboró sobre la base del objetivo contenido en el presente informe, las atribuciones conferidas por ley a esta Comisión, el análisis efectuado de las jurisdicciones extranjeras, el impacto de la propuesta normativa y los antecedentes y comentarios recibidos en el proceso de consulta ciudadana realizados con motivo de este proyecto.

El siguiente cambio normativo está dirigido a los bancos, y se hace extensivo a filiales y sociedades de apoyo al giro bancario, y emisores y operadores de tarjetas de pago no bancarios, quienes deberán dar cumplimiento a ésta atendiendo al volumen y complejidad de sus operaciones, a contar de su entrada en vigencia que será a la fecha de su publicación.

Texto definitivo de la Normativa en sus aspectos principales

CAPÍTULO 20-7 "Externalización de servicios"

Se reemplazan los párrafos del numeral 5 "Riesgo País" del Título III del mencionado Capítulo por el siguiente:

"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."

Además, se incorpora 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 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."

En otro orden de cosas, se incorporan ajustes de concordancia en diferentes párrafos del Capítulo 20-7, modificando la alusión a "Superintendencia" por "Comisión".

CIRCULAR N° 2 - Empresas emisoras de tarjetas de pago no bancarias / Empresas operadoras de tarjetas de pago

Se incorporan los siguientes ajustes al numeral 3 de la Circular N° 2:

1. *Se reemplaza el segundo párrafo del numeral 3 de la Circular N° 2 por el siguiente:*

"Para efectos de la presente Circular los Emisores y Operadores, deberán observar las instrucciones contenidas en el Capítulo 20-7 de la Recopilación Actualizada de Normas para bancos que se detallan a continuación:

a) Las definiciones que deben ser consideradas para efectos de determinar el alcance de los servicios afectos a dichas normas, contenidas en el Título I.

b) Las consideraciones contenidas en el Título II, con excepción del inciso segundo en lo referido a la mención del Capítulo 1-13 de la mencionada Recopilación.

c) Las condiciones que deben cumplirse en la externalización de servicios, a que se refiere el Título III.

d) Las consideraciones contenidas en el Título IV a excepción del numeral 2. El requisito contemplado en el numeral 1 letra b) literal i) de este Título, podrá ser excepcionado por el directorio o la instancia que haga sus veces, cuando se asegure, por medio de un informe anual, que la entidad cumple con las medidas preventivas allí contempladas, con excepción de la exigencia que menciona la necesidad de mantener 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.

e) Los requisitos considerados en el Título V."

2. *Se elimina el tercer párrafo del numeral 3 de la Circular N° 2, cuyas instrucciones ya están contenidas en el Capítulo 20-7 de la Recopilación Actualizada de bancos, al cual se remite la Circular N° 2.*

VIII. Análisis de Impacto Regulatorio

a. Principales Costos de la Aplicación del cambio normativo

i. Principales Costos para las Entidades Fiscalizadas

Lo anterior, podría implicar a las instituciones financieras una disminución de los costos asociados a los proyectos de externalización de servicios críticos en el extranjero.

Cabe señalar, que actualmente hay instituciones que cuentan con un centro de procesamiento en Chile para servicios externalizados en el extranjero, diseño que debe ser evaluados por los directorios respectivos para su mantención o la adopción de los cambios normativos.

ii. Principales Costos para la CMF

Si bien en la actualidad durante la fiscalización en terreno se validan aspectos de servicios externalizados, el cambio normativo, podrían derivar en aquellas instituciones que opten por la alternativa de externalizar servicios en el extranjero sin un centro de procesamiento en Chile, en acciones específicas de supervisión de la CMF a los informes emitidos por las instituciones independientes, que dan cuenta del cumplimiento de las exigencias establecidas en la norma.

b. Principales Beneficios

i. Principales Beneficios para las Entidades Fiscalizadas

Con la modificación normativa, las entidades financieras tendrán un marco de referencia que les permite una mayor flexibilidad para adaptarlo a sus actuales modelos de negocios, aprovechando de esta manera las nuevas tendencias de transformación digital. Adicionalmente, les otorga claridad de los elementos que

resultan esenciales para esta Comisión para efectos de externalizar servicios catalogados como críticos o significativos.

c. Principales Riesgos

i. Principales Riesgos de No Emitir la Normativa

En caso de que la normativa no se emita se mantendrían las restricciones vigentes, dificultando las opciones de las instituciones financieras para optar a las nuevas tendencias de transformación digital, lo cual podría constituirse en una barrera de entrada al mercado, con posibles impactos negativos en el desarrollo de la industria y la generación de mayor competencia.

ii. Principales Riesgos de Emitir la Normativa

La emisión de los cambios normativos en materia de servicios externalizados, en general, no presenta riesgos relevantes para los objetivos de supervisión de la CMF, considerando que se trata de modificaciones que permitirán flexibilizar algunas exigencias normativas particulares, pero complementándolas, con medidas que mitigan el posible impacto en la gestión de los riesgos operacionales en caso de ser adoptadas.

Sin embargo, el hecho de considerar como válido un informe de una empresa externa podría generar ciertos riesgos en cuanto a la fiabilidad de la información, así como encarecer el trabajo de supervisor en el caso de tener que eventualmente corroborar en terreno en el extranjero el cumplimiento de lo señalado en los informes de las empresas externas.

COMISIÓN
PARA EL MERCADO
FINANCIERO

www.cmfchile.cl