INFORME NORMATIVO

COMISIÓN PARA EL MERCADO FINANCIERO

NORMAS DE GESTIÓN DE RIESGOS OPERACIONALES APLICABLES A LAS COOPERATIVAS DE AHORRO Y CRÉDITO FISCALIZADAS POR LA COMISIÓN

Enero 2022

www.cmfchile.cl

COMISIÓN PARA EL MERCADO FINANCIERO

Normas de resguardo y gestión de riesgos operacionales aplicables a las cooperativas de ahorro y crédito fiscalizadas por la Comisión

Comisión para el Mercado Financiero.
Enero 2022.

CONTENIDO

I. INTRODUCCIÓN.

Durante los últimos años, con la irrupción y masificación de las tecnologías de la información y el uso de medios remotos para la prestación de servicios financieros, la normativa de la Comisión aplicable a los bancos y sus sociedades de apoyo al giro, así como a los emisores y operadores de tarjetas de pago se ha ido actualizando, con la finalidad de que dichas entidades desarrollen y perfeccionen su marco de gestión de riesgos operacionales.

En este contexto, si bien dichas normas son un marco de referencia para toda la industria financiera nacional, en el caso de las cooperativas de ahorro y crédito (en adelante "CAC") fiscalizadas por la Comisión, resulta necesario dar un paso adicional y comenzar a hacerles exigible el cumplimiento de las referidas disposiciones, considerando las particularidades de cada entidad, habida cuenta de los servicios que pueden prestar y la cantidad de usuarios que potencialmente podrían verse afectados, en caso de no contar con una adecuada gestión en el ámbito de los riesgos operacionales.

II. OBJETIVO DE LA PROPUESTA NORMATIVA.

El objetivo principal de la modificación a las normas generales aplicables a las CAC fiscalizadas por la Comisión, es homologar las disposiciones que deben observar en el ámbito de los riesgos operacionales, con respecto del marco que actualmente rige a los bancos y sus sociedades de apoyo al giro, así como a los emisores y operadores de tarjetas de pago no bancarios, todos los cuales se rigen por una serie de normas que abarcan diversos ámbitos de la gestión de dichos riesgos.

En tal sentido, cabe señalar que las CAC están habilitadas por la Ley General de Cooperativas para efectuar un amplio rango de operaciones y servicios financieros (apertura de cuentas vista, cuentas de ahorro, otorgamiento de depósitos a plazo, emisión de tarjetas de crédito, tarjetas de débito y tarjetas de pago con provisión de fondos, entre otros), por lo que a la fecha resulta imprescindible que cuenten con un marco normativo claro que les permita ir desarrollando sus servicios, con niveles adecuados de seguridad, acordes con la escala y complejidad de las operaciones de cada entidad. Asimismo, dicha ley también establece que las CAC "deberán contar con las instalaciones, recursos humanos, tecnológicos, procedimientos y controles necesarios para desarrollar adecuadamente sus funciones y operaciones", y es en tal sentido que se plantea la adopción de las normas actualmente vigentes a operaciones de naturaleza similar.

III. EVOLUCIÓN DE LA NORMATIVA DE RIESGO OPERACIONAL.

La CMF cuenta con una serie de normas que contienen requisitos generales, así como principios y buenas prácticas de gestión en el ámbito de los riesgos operacionales, contenidos en diversos capítulos de su Recopilación Actualizada de Normas para bancos (en adelante RAN), que se han venido desarrollando desde fines de la década de 1980[2] y que actualmente se pueden agrupar en las siguientes temáticas:

- **Capítulo 1-7 de la RAN sobre "Transferencia electrónica de información y fondos"**: establece los requisitos generales que deben cumplir los sistemas utilizados para efectuar operaciones mediante sistemas electrónicos, tales como el registro, trazabilidad y respaldo de la información; las medidas para asegurar la identidad de los usuarios; la disponibilidad de canales de comunicación para requerir bloqueos (en línea y tiempo real); requerimientos específicos de seguridad para efectuar transferencias electrónicas de fondos (encriptación, dos factores de autentificación y firma digital avanzada para altos montos), incluidos sistemas de monitoreo y prevención de fraudes, que controlen operaciones de usuarios, puntos de acceso (IP) y correlacionen parámetros, incluidos aquellos vinculados a operaciones de lavado de activos, entre otros. Asimismo, establece los estándares de disponibilidad de efectivo que deben cumplir los cajeros automáticos.

- **Capítulo 20-7 de la RAN "Externalización de servicios"**: contiene pautas de carácter general relativas a servicios externalizados y, en forma particular, a la tercerización de servicios de procesamiento de datos y resguardos adicionales en el caso de servicios en la nube. La norma señala las condiciones que debe cumplir una entidad ante la decisión de externalizar un servicio, contempla requisitos esenciales respecto a los sitios de procesamiento; los aspectos de continuidad del negocio, seguridad de la información propia y de sus clientes; entre otros. En cuanto a este último aspecto, la entidad bancaria debe exigir al proveedor asegurar la confidencialidad, integridad, trazabilidad y disponibilidad de sus activos de información y la de sus clientes.

- **Capítulo 20-8 de la RAN "Información de incidentes operacionales"**: establece lineamientos para la información que las entidades supervisadas a las que la misma aplica, deben remitir ante la ocurrencia de incidentes operacionales relevantes que afecten la continuidad del negocio, la seguridad de la información o la imagen de la institución, y además, señala las condiciones mínimas que se deben

[2] Ver anexo.

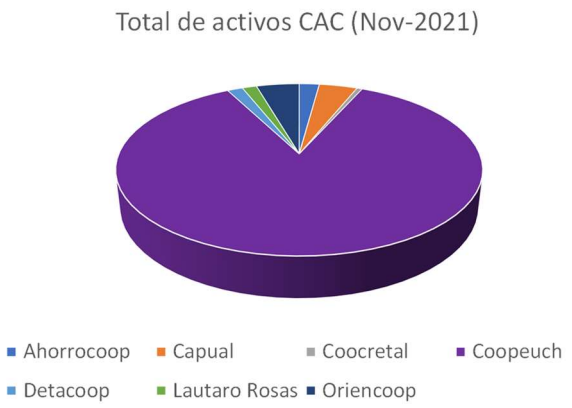
considerar para el desarrollo y mantención de bases de información respecto de incidentes de ciberseguridad. El 31 de agosto de 2018 se introdujeron cambios que perfeccionan el sistema de reporte de incidentes, creando una plataforma digital especialmente establecida por la CMF para reportar los incidentes al regulador en un plazo máximo de 30 minutos. Adicionalmente, se definió la obligación de designar un encargado de nivel ejecutivo para comunicarse con la CMF en todo momento.

- **Capítulo 20-9 de la RAN "Gestión de continuidad del negocio"**: contempla una serie de lineamientos para la adecuada gestión de los riesgos de continuidad del negocio, teniendo en cuenta el volumen y la complejidad de las operaciones de las entidades supervisadas a las que la misma aplica. De esta manera, indica la debida existencia de una estrategia aprobada por la máxima instancia de la entidad, de una función de riesgos que se encargue de este ámbito en conjunto con instancias colegiadas de alto nivel, de una estructura para el manejo de situaciones de crisis, de la evaluación de escenarios mínimos de contingencia, entre otros. Dentro de los escenarios de contingencia para los cuales se deben definir y probar planes se encuentran los "ataques maliciosos que afecten la ciberseguridad". Incluye la operatoria de los sitios de procesamiento de datos como parte de los aspectos relevantes que contribuyen a fortalecer la resiliencia operacional de las entidades.

- **Capítulo 20-10 de la RAN sobre "Seguridad de la información y ciberseguridad"**: contiene una serie de disposiciones, basadas en las mejores prácticas internacionales, que deben ser consideradas para la gestión de la seguridad de la información y ciberseguridad. Entre otros, se definen lineamientos específicos respecto del rol que debe tener el Directorio para la adecuada gestión, tanto de seguridad de la información como de ciberseguridad, otorgándole como responsabilidad la aprobación de la estrategia institucional en esta materia, junto a la responsabilidad de asegurar que las entidades mantengan un sistema de gestión de la seguridad de la información y ciberseguridad. Asimismo, se establece la necesidad de que las entidades definan sus activos críticos, así como las funciones de protección de éstos, la detección de las amenazas y vulnerabilidades, la respuesta ante incidentes y la recuperación de la operación normal de la entidad; además de disponer de políticas y procedimientos para la identificación de aquellos activos que componen la infraestructura crítica de la industria financiera y del sistema de pagos, y para el adecuado intercambio de información técnica de incidentes que afecten o pudieran afectar la ciberseguridad de la entidad.

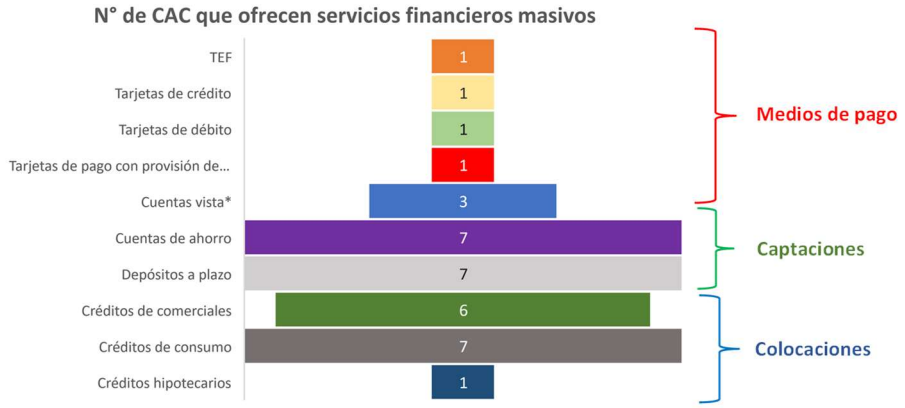
Situación actual de las CAC

Actualmente son 7 las CAC que están sujetas a la fiscalización de la CMF, siendo una de estas la que tiene una participación preponderante en dicha industria.



Fuente: CMF

A la fecha, las únicas disposiciones que se han hecho extensivas a las CAC corresponden a las normas sobre información de incidentes operacionales[3]; e indirectamente las del Capítulo 1-7, en el marco de la emisión de tarjetas de pago, por la remisión al Capítulo 8-41 de la RAN[4]. Lo anterior, obedece principalmente a que gran parte de las cooperativas fiscalizadas por la CMF prestan un rango limitado de servicios, focalizados principalmente productos de captación sin funcionalidades de pago, además de tradicionales colocaciones de créditos comerciales y de consumo.



*** Solo una CAC mantiene cuentas de depósito a la vista con atributos transaccionales**
Fuente: CMF

[3] Circular N°170 de 31-08-2018: http://www.sbif.cl/sbifweb3/internet/archivos/norma_12210_1.pdf
[4] El número 8 de la Circular N°108, remite a Capítulo 8-41 de la RAN, el cual a su vez establece que se deben adoptar los resguardos contemplados en el N°2 del Capítulo 1-7, para efectos de la autorización y registro de las transacciones realizadas mediante tarjetas de pago.

No obstante lo anterior, por muy acotados que sean los servicios prestados, la necesidad de utilizar las tecnologías que permitan la atención remota (por ejemplo, para pagar créditos, efectuar giros o habilitar funcionalidades de pago) ha resultado evidente en los últimos meses producto de la pandemia; y en dicho contexto, los servicios que se contraten deben cumplir con resguardos mínimos de seguridad.

IV. PROPUESTA NORMATIVA PUBLICADA EN CONSULTA.

Como se indicó previamente, la modificación normativa contempla incorporar en la Circular N°108[5] de Cooperativas (que contiene sus normas generales) una remisión a las normas de gestión de riesgos operacionales de la RAN, con las precisiones del caso y recalcando que la aplicación de dichas normas debe efectuarse considerando la naturaleza, volumen y complejidad de las operaciones de cada CAC.

De esta forma, durante el mes de mayo de 2021 se publicó[6] la propuesta normativa que introduciría un nuevo numeral 16 a la citada Circular, el cual se presenta a continuación:

> "**16. Normas de resguardo y gestión de riesgos operacionales**
>
> Las cooperativas fiscalizadas por esta Comisión deberán adoptar resguardos operacionales y de seguridad de la información propios de los servicios financieros que presten y de los sistemas tecnológicos que utilicen, considerando aquellas materias y elementos específicos que complementan la gestión de diversos ámbitos del riesgo operacional aplicables a las instituciones financieras fiscalizadas por la Comisión.
>
> En atención a lo indicado, se dispone que las cooperativas cumplan con las instrucciones contenidas en los Capítulos de la Recopilación Actualizada de Normas para bancos que se indican a continuación, las que en todo caso deben ser observadas considerando la naturaleza, volumen y complejidad de las operaciones de cada entidad.
>
> **16.1 Transferencia electrónica de información y fondos**
>
> Para la prestación de servicios financieros que se efectúen mediante transmisiones de mensajes o instrucciones a través de redes de comunicación propias o de terceros, efectuadas mediante el uso de dispositivos electrónicos (computadores, cajeros automáticos, teléfonos,

[5] http://www.cmfchile.cl/portal/principal/605/articles-30162_doc_pdf.pdf
[6] https://www.cmfchile.cl/portal/prensa/615/w3-article-47635.html

terminales de venta, etc.), las cooperativas deben considerar aquellas disposiciones contenidas en el Capítulo 1-7 de la citada Recopilación, que resulten aplicables a los servicios que provean, referidos a los requisitos que deben cumplir los sistemas utilizados, las condiciones que se deben considerar para las transferencias electrónicas de fondos de sus clientes y la prevención de fraudes, entre otros.

16.2 Gestión de la seguridad de la información y ciberseguridad

El Capítulo 20-10 de la Recopilación Actualizada de Normas, contiene el conjunto de lineamientos y buenas prácticas para una adecuada gestión de la seguridad de información y ciberseguridad que también deberá ser observado por las cooperativas, en todo aquello que le resulte aplicable a cada entidad. Asimismo, este Capítulo se complementa con las disposiciones del numeral 13.2 de esta circular, referido a la información de los incidentes operacionales.

Como es natural, las responsabilidades que dicho Capítulo asigna al Directorio de las entidades, en el caso de las cooperativas deberán ser observadas por el Consejo de Administración.

16.3 Normas aplicables a la externalización de servicios

Para la contratación de proveedores de servicios externos que realicen una o más actividades operativas que podrían ser también efectuadas internamente por la entidad con sus propios recursos, tanto humanos como tecnológicos, las cooperativas deberán atenerse a 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 relativas a los riesgos que se asumen, 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) Los factores que se deben considerar para externalizar servicios de procesamiento de datos del Título IV. El requisito contemplado en el literal i) de la letra b) del numeral 1 de este Título, podrá ser

excepcionado por el Consejo de Administración, 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 este Organismo, calificada de conformidad con lo establecido en el Capítulo 1-13 de esta Recopilación, aplicable únicamente a los bancos.

e) Los requisitos considerados en el Título V, en el ámbito de la externalización de servicios en la nube, cuando se encuentren asociados a una actividad estratégica o crítica para la cooperativa.

16.4 Normas sobre continuidad de negocio

Las cooperativas deberán desarrollar planes y medidas de continuidad operacional que consideren lineamientos y buenas prácticas para la gestión de los riesgos de continuidad de negocios contenidas en los título I y II del Capítulo 20-9 de la Recopilación antes referida, acordes a las condiciones propias de cada entidad.

Para efectos de la implementación de estas normas, se contempla que el Consejo de Administración apruebe un plan de implementación a más tardar en julio de 2021, para que estas normas rijan a partir del 1° de enero de 2022. El cumplimiento de las nuevas disposiciones será parte de la evaluación habitual que realiza este Organismo en el ámbito de los riesgos operacionales."

V. RESULTADO DE LA CONSULTA PÚBLICA Y VERSIÓN DEFINITIVA DE LA NORMA.

Durante el periodo de consulta pública los comentarios recibidos se focalizaron en los plazos de implementación de las nuevas disposiciones. En este sentido, las cooperativas manifestaron comprender la importancia de la iniciativa e incluso algunas han comenzado de forma voluntaria su implementación, pero solicitan ampliar los plazos para su aplicación. Respecto de esto último, requerían que la aplicación de las normas fuera gradual y dependiendo de la materia, partiendo en julio de 2022 y terminando en diciembre de 2023.

En este sentido, acogiendo en lo sustantivo dichos comentarios, la versión definitiva de la normativa establece que el plazo de implementación para las disposiciones relativas a la externalización de servicios (Capítulo 20-7), continuidad de negocios (Capítulo 20-9) y seguridad de la información y ciberseguridad (Capítulo 20-10) se extenderá hasta julio del año 2023. Para dichos efectos, se contempla que el Consejo de Administración apruebe un plan

de implementación a más tardar en mayo de 2022, para que estas normas rijan a partir del 1° de julio de 2023.

Asimismo, cabe recordar que las disposiciones contenidas en el Capítulo 1-7, aplicables a sistemas de autorización y registros de transacciones con tarjetas de pago, incluidas las transferencias de fondos, actualmente son aplicables a las cooperativas que emiten tarjetas de pago, según lo establecido en el numeral 15 de la Circular N°108, el cual se remite al Capítulo 8-41 de la Recopilación Actualizada de Normas. En tal sentido, y considerando que solo una cooperativa ofrece este tipo de servicios financieros, no resulta necesario definir normas transitorias sobre dicha materia.

VI. IMPACTO REGULATORIO.

Se estima que los efectos de la normativa debieran ser acotados, porque las exigencias son proporcionales al volumen y naturaleza de las operaciones que cada CAC desarrolla, y aquellas que prestan una mayor cantidad de servicios financieros, ya cuentan con una estructura y procesos de gestión de riesgos operacionales. De todas formas, se estima que una de las tareas más relevantes de su implementación inicial será la revisión de los contratos con sus proveedores de servicios, así como la adecuación de procedimientos de control de las actividades calificadas como estratégicas para la institución, para lo cual se estableció un plazo holgado de aplicación.

Para las demás entidades, la implementación del marco de gestión debería estar focalizado en sus sistema de información y los procesos asociados a sus productos de captación y crédito, con un mayor énfasis en el ámbito de la seguridad de la información, pudiendo requerir en algunos casos la contratación de asesorías o personal especializado.

Anexo: Principales hitos de la normativa sobre riesgos operacionales de la CMF aplicable a bancos, sociedades de apoyo al giro y emisores de tarjetas de pago

Año	Regulación
1988	A esa fecha, la recientemente creada Recopilación Actualizada de Normas (RAN) para bancos incorporó el Capítulo 1-7, que regula el uso de dispositivos electrónicos autosuficientes, tales como los terminales de auto consulta y cajeros automáticos, los cuales en un inicio requerían contar con un informe técnico que respaldara su implementación y la autorización de la Superintendencia de Bancos e Instituciones Financieras (SBIF).
1993	Se regulan los requerimientos mínimos que deben cumplir los sistemas que apoyen los servicios de depósito y giro automático de fondos prestados mediante dispositivos electrónicos, incorporando los requisitos que se debían cumplir en el caso de las transferencias electrónicas de fondos, muchos de los cuales aún resultan aplicables en la actualidad[7].
1996	Se reformulan las disposiciones del Capítulo 1-7[8], en atención a la constante evolución del uso de los medios computacionales para el desarrollo de las operaciones bancarias. Se reorientan las instrucciones, reforzando las aspectos relativos a la gestión del riesgo inherente al uso de los medios electrónicos, no requiriendo autorización previa para los nuevos desarrollos, lo que en todo caso se establece como parte de las evaluaciones periódicas a las que están sometidos los bancos.
2000	En concordancia con las disposiciones del Título V de la Ley General de Bancos, que establece que la SBIF debe mantener clasificadas a las instituciones financieras de acuerdo con su gestión y solvencia, se introduce a la RAN el Capítulo 1-13, que entre otros, contiene un enfoque de la evaluación de la gestión de los riesgos de los bancos (de cuyo resultado dependerá la calificación), entre los cuales se encuentra el riesgo operacional y tecnológico[9].
2000	Se incorpora a la RAN el Capítulo 20-7, denominado "Procesamiento de datos. Servicios prestados y recibidos"[10], mediante el cual se establecen las condiciones para que los bancos aprovechen la capacidad instalada y experiencia de las instituciones financieras para prestar servicios de procesamiento de datos a otras entidades o, en sentido contrario, encargar a empresas diferentes a una sociedad de apoyo al giro el

[7] https://www.bcn.cl/leychile/navegar?idNorma=1064033
[8] El Capítulo 1-7 se reformula y pasa a denominarse "Transferencias electrónicas de información y de fondos": https://www.bcn.cl/leychile/navegar?idNorma=1065345
[9] El Capítulo 1-13 se aplica exclusivamente a los bancos, pero su enfoque centrado en supervisión de la gestión de los riesgos también es considerado para la supervisión de otras entidades fiscalizadas por la ex SBIF: https://www.bcn.cl/leychile/navegar?idNorma=1068284
[10] https://www.bcn.cl/leychile/navegar?idNorma=1068307

procesamiento de todo o parte de los datos que se generan en las operaciones de las instituciones financieras, previa autorización de la SBIF. Estas normas exigen que los bancos establezcan condiciones contractuales que resguarden la confidencialidad de la información en conformidad con la legislación chilena y aseguren su control sobre el riesgo operativo y tecnológico, cuando el procesamiento sea realizado por una empresa externa.

2007 Se establecen las instrucciones para que las transferencias electrónicas de fondos se realicen en forma simultánea con el correspondiente cargo a la cuenta del ordenante, siendo de responsabilidad de los propios bancos establecer los procedimientos para disponer la cobertura oportuna de esas transferencias.

2008 Se actualizan las disposiciones del Capítulo 20-7[11], relativas a la contratación de servicios externos, incluidos el procesamiento de datos, con el propósito de precaver los riesgos que envuelve el procesamiento de actividades del banco por proveedores externos y sus efectos sistémicos, así como también, los antecedentes que deben entregar aquellos bancos que decidan contratar tales servicios externos.

2014 Se elimina el requisito de autorización previa de la SBIF para externalizar servicios[12] (Capítulo 20-7), centrándose la atención en el cumplimiento de las nuevas normas (rol del gobierno corporativo, requisitos particulares para externalizar actividades críticas o estratégicas, sitios de procesamiento de datos alternativo en Chile, etc.), junto con el examen de la gestión de riesgos que se realiza sobre la externalización de servicios, como parte de las evaluaciones de que trata el Capítulo 1-13 de la RAN.

2015 Se establecen las instrucciones[13] (Capítulo 20-8) para alertar a la SBIF de los incidentes operacionales que afecten la continuidad del negocio, la seguridad de la información o la imagen de la institución, que puedan afectar a las entidades fiscalizadas, incluyendo en este caso a los bancos, cooperativas, sociedades de apoyo al giro, filiales bancarias, emisores y operadores de tarjetas.

2015 Se incorporan al Capítulo 1-7 disposiciones relativas a los estándares de disponibilidad de efectivo de los cajeros automáticos, considerando parámetros comunes para su medición; así como la necesidad de que los bancos los incorporen en sus políticas, para asegurar el cumplimiento de los niveles mínimos de servicio exigidos[14].

2016 Se incorpora el Capítulo 20-9 sobre continuidad negocios[15], mediante el cual se establecen un conjunto de lineamientos y buenas prácticas

[11] https://www.bcn.cl/leychile/navegar?idNorma=1071783
[12] https://www.bcn.cl/leychile/navegar?idNorma=1072952
[13] https://www.bcn.cl/leychile/navegar?idNorma=1095475&idParte=9739050&idVersion=2015-03-23
[14] https://www.bcn.cl/leychile/navegar?idNorma=1095474&idParte=9739033&idVersion=2015-03-17
[15] https://www.bcn.cl/leychile/navegar?idNorma=1106790&idParte=9833131&idVersion=2016-11-02

específicas a considerar para la gestión de los riesgos de continuidad, las que complementan el enfoque de evaluación de los riesgos operacionales de los bancos, establecido en el Capítulo 1-13. Entre otros aspectos, se establece que cada entidad debe contar con una estrategia de administración, asignándole al Directorio la responsabilidad en la aprobación de las directrices y en la mantención de una función de riesgos e instancias de alto nivel para la administración. Asimismo, en el contexto de una adecuada gestión, se identifican elementos relevantes de diseño y construcción de los sitios de procesamientos de datos y configuraciones de la infraestructura tecnológica que contribuyen a fortalecer la resiliencia operacional de las entidades.

2017 En concordancia con las nuevas disposiciones del Banco Central de Chile, aplicables a los emisores de tarjetas de pago, se establecen las normas[16] que se deben observar para el resguardo de los aspectos operacionales y de seguridad propios de sistemas de pago a través de tarjetas y otros medios electrónicos, así como de aquellas materias y elementos específicos que complementan la gestión del riesgo operacional. Para dichos efectos, se establece que deberán cumplir aquellas disposiciones aplicables a la industria bancaria, en el ámbito de las medidas de seguridad de las transacciones electrónicas, de continuidad de negocio y de externalización de servicios, que les resultan atingentes.

2017 Se actualizan las disposiciones en el ámbito de la externalización de servicios, a fin de establecer lineamientos mínimos para el uso de servicios externalizados en modalidad nube (*Cloudcomputing*)[17].

2018 Ante el incremento de los incidentes operacionales en materia de ciberseguridad se instruye que dicha dimensión debe ser tratada especialmente en el ámbito de la gestión de los riesgos operacionales, incluyendo un rol más activo de los directorios. A su vez, se establece una plataforma para informar al regulador la evolución de estos incidentes, además de instruir la obligación de mantener un sistema de alerta de incidentes de Ciberseguridad entre los miembros de la industria, para que compartan la información de los incidentes[18].

2019 Se revisan las disposiciones aplicables a la externalización de servicios en la nube, conciliando la forma en que se estructuran dichos servicios con la necesidad de mantener una sólida gestión de los riesgos operacionales que ello involucra; pudiendo a partir de ese momento, exceptuar a las entidades fiscalizadas de la condición de disponer un centro de procesamiento de datos de contingencia en el país, en la medida que el directorio lo autorice y se asegure mediante un informe anual, que la entidad ha tomado las medidas preventivas mínimas definidas por la CMF[19].

[16] http://www.cmfchile.cl/portal/principal/605/articles-30170_doc_pdf.pdf
[17] https://www.bcn.cl/leychile/navegar?idNorma=1113077&idParte=9873614&idVersion=2017-12-27
[18] https://www.bcn.cl/leychile/navegar?idNorma=1122834&idParte=9947486&idVersion=2018-08-31
[19] https://www.bcn.cl/leychile/navegar?idNorma=1141849&idParte=10098436&idVersion=2019-12-23

2020	Se incorpora el nuevo Capítulo 20-10[20] sobre gestión de seguridad de la información y ciberseguridad, que contiene lineamientos mínimos que deben observar tanto los bancos, como sus sociedades de apoyo al giro y filiales, además de los emisores y operadores de tarjetas de pago, con el objetivo de establecer sanas prácticas para una adecuada gestión de los riesgos en seguridad de información y ciberseguridad.

[20] https://www.bcn.cl/leychile/navegar?idNorma=1150515&idParte=10166535&idVersion=2020-07-06

www.cmfchile.cl