TEXTO ACTUALIZADO

Disposición:	**CIRCULAR Nº 2** (de 28.11.2017)
Para:	**EMPRESAS EMISORAS DE TARJETAS DE PAGO NO BANCARIAS** **EMPRESAS OPERADORAS DE TARJETAS DE PAGO**
Materia:	Normas comunes sobre resguardos operacionales y de seguridad para la emisión y operación de tarjetas de pago.

ACTUALIZACIONES:

Modificaciones introducidas mediante Circulares emitidas por la Superintendencia de Bancos e Instituciones Financieras:

1. **Empresas emisoras de tarjetas de pago no bancarias**

Circular Nº 5 de 31 de agosto de 2018

2. **Empresas operadoras de tarjetas de pago**

Circular Nº 4 de 31 de agosto de 2018

Modificaciones introducidas mediante acuerdos adoptados por el Consejo de la Comisión para el Mercado Financiero*:

Circular Nº 2.245 de 23 de diciembre de 2019
Circular Nº 2.263 de 06 de julio de 2020

* De acuerdo a lo dispuesto en el artículo noveno transitorio de la Ley N° 21.130, y lo establecido en el Decreto con Fuerza de Ley Nº 2, expedido a través del Ministerio de Hacienda y publicado en el Diario Oficial el 2 de mayo de 2019, la Comisión para el Mercado Financiero asumió las competencias de la Superintendencia de Bancos e Instituciones Financieras a partir del 1º de junio de 2019, determinándose igualmente esa fecha para la supresión de esta última.

Normas comunes sobre resguardos operacionales y de seguridad para la emisión y operación de tarjetas de pago.

1. Aspectos generales

Las presentes instrucciones se refieren al conjunto de resguardos 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, que deben ser observados por todas las entidades que emiten u operan tarjetas de pago, conforme a las nuevas disposiciones impartidas por el Banco Central de Chile (en adelante "BCCH") en los Capítulos III.J.1 y III.J.2 de su Compendio de Normas Financieras (en adelante "CNFBCCH"), así como en los sub Capítulos III.J.1.1, III.1.2 y III.J.1.3 del referido Compendio, que contienen instrucciones particulares sobre la emisión de tarjetas de crédito, tarjetas de débito y tarjetas de pago con provisión de fondos (en adelante "tarjetas de pago"), respectivamente.

En todo caso, las disposiciones contenidas en esta Circular deben ser aplicadas en concordancia con el marco integral de control y gestión de riesgos, según lo indicado en el numeral 2.3 del Título II de la Circular Nº 1, dirigida a Emisores de Tarjetas de Pago No Bancarios; y en el Nº 3 del Título III de la Circular Nº 1, dirigida a Operadores de Tarjetas de Pago.

2. Normas aplicables a los sistemas de autorización y registro de transacciones

El Nº 3 del Título I del Capítulo III.J.1 del CNFBCCH establece expresamente que los emisores de tarjetas deben disponer de resguardos operacionales y de seguridad adecuados en función de los medios que emitan, conforme a los estándares y mejores prácticas internacionales sobre la materia. Asimismo, como requisitos mínimos, prescribe que deben contar con una tecnología de seguridad que permita proteger apropiadamente la información contenida en las tarjetas de pago, implementar mecanismos robustos de autentificación y prevención de fraudes, así como facilitar la verificación oportuna de la disponibilidad de cupos y saldos de éstas, y su bloqueo, según corresponda.

Resguardos equivalentes deben ser adoptados en los contratos que suscriban los Emisores y Operadores con los Titulares de las Marcas a que adhieran, para efectos de la modalidad de operación contemplada en el numeral ii del N° 3 del Título I del Capítulo III.J.2 del CNFBCCH.

Lo anterior se enmarca dentro de las responsabilidades que recaen sobre los emisores y operadores de tarjetas de pago, dado que las disposiciones del BCCH también indican claramente que en la medida que se cumplan los procedimientos de autentificación del medio de pago y la verificación de la identidad del tarjetahabiente, definidos en el contrato con las entidades afiliadas, estos no podrán eximirse de la obligación de pago por las ventas que aquéllas realicen, una vez que la transacción ha sido autorizada.

2.1 Requisitos generales que deben cumplir los sistemas transaccionales

Los sistemas deben proveer un perfil de seguridad que garantice que las operaciones sólo puedan ser realizadas por personas debidamente autorizadas para ello, debiendo resguardar, además, la privacidad o confidencialidad de la información transmitida o procesada por ese medio.

Los procedimientos deberán impedir que tanto el originador como el destinatario, en su caso, desconozcan la autoría de las transacciones o mensajes y la conformidad de su recepción, debiendo utilizarse métodos de autentificación para el acceso al sistema, que permitan asegurar su legitimidad e integridad.

2.2 Requisitos para efectuar transferencias electrónicas de fondos desde Cuentas de Provisión de Fondos

Para efectos de esta Circular, por transferencias electrónicas de fondos desde una Cuenta de Provisión de Fondos (CPF) se entienden los cargos realizados por medios electrónicos en dichas cuentas, con el propósito que los fondos sean abonados a otras CPF, a Cuentas Corrientes Bancarias, Cuentas de Ahorro a la Vista o Cuentas a la Vista, y siempre que se trate de Tarjetas Nominativas, en los términos prescritos en el segundo párrafo del N° 3 del Título IV del sub Capítulo III.J.1.3 del CNFBCCH.

Los procedimientos utilizados para realizar transferencias electrónicas de fondos desde una CPF a través de canales remotos, deberán impedir que tanto el originador como el destinatario, en su caso, desconozcan la autoría de las transacciones o mensajes y la conformidad de su recepción, debiendo utilizarse métodos de autentificación robustos que consideren a lo menos un factor para el acceso al sistema y otro factor distinto para la autorización de cada cargo que se efectúe sobre la CPF originadora, que permitan asegurar su autenticidad e integridad. En el caso de transferencias entre cuentas de distintos Emisores, al menos uno de los factores de autorización utilizados por parte del usuario debe ser de generación o asignación dinámica.

2.3 Prevención de fraudes

Las entidades deben contar con sistemas o procedimientos que permitan identificar, evaluar, monitorear y detectar en el menor tiempo posible aquellas operaciones con patrones de fraude, de modo de marcar o abortar actividades u operaciones sospechosas, para lo cual deberán establecer y mantener, de acuerdo a la dinámica de los fraudes, patrones conocidos de estos y comportamientos que no estén asociados al cliente.

Estos sistemas o mecanismos deberán permitir tener una vista integral y oportuna de las operaciones del tarjetahabiente (por ejemplo en los intentos de acceso), de los puntos de acceso (por ejemplo direcciones IP, Cajero Automático, POS u otros), además de hacer el seguimiento y correlacionar eventos a objeto de detectar otros fraudes, puntos en que estos se cometen, *modus operandi* y puntos de compromisos, entre otros.

3. Normas aplicables a la externalización de servicios

Las disposiciones del BCCH establecen que tanto los Emisores como Operadores que contraten con terceros la provisión de los servicios propios del funcionamiento de los sistemas de tarjetas de pago deben asumir, frente a las entidades afiliadas y a los tarjetahabientes, la responsabilidad por la prestación efectiva de sus servicios y el resguardo de la seguridad operacional de las actividades encomendadas a dichos terceros, independientemente de la responsabilidad que puedan perseguir a su vez respecto de dichos proveedores.

Para efectos de la presente Circular los Emisores y Operadores, según se distinga, 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 literal i) de la letra b) del numeral 1 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 este Organismo, calificada de conformidad con lo establecido en el Capítulo 1-13 de esta Recopilación.

e) Los requisitos considerados en el Título V.

Por su parte, si bien las disposiciones del mencionado Capítulo no definen taxativamente aquellas actividades que deban ser clasificadas como significativas, estratégicas o críticas, el Nº 4 del Título I del Capítulo III.J.2 del CNFBCCH establece expresamente que al menos los servicios de autorización y registro de transacciones que efectúen los Titulares o Usuarios de la o las Tarjetas, deben ser clasificados de esa forma.

4. Normas sobre continuidad operacional

Como parte de los elementos que deben ser considerados para el desarrollo e implementación de las políticas de gestión y control de riesgos de los emisores y operadores de tarjetas de pago, el BCCH establece que en estas se incluyan las medidas necesarias para resguardar la continuidad operacional, indicando las infraestructuras y sistemas tecnológicos que se contempla utilizar al efecto, como también, las medidas de Ciberseguridad y de otra índole adoptadas para prevenir y mitigar los riesgos de fraude, así como los demás aspectos que pueda instruir esta Comisión. Asimismo, dispone que los emisores deben establecer planes y procedimientos para asegurar la continuidad del servicio, en términos que permitan solucionar oportuna y eficazmente las contingencias operativas que puedan afectarlos, contemplando, entre otras medidas, aquellas que propendan a una alta disponibilidad de sus sistemas (*up time*).

En atención a lo indicado, se dispone que las entidades de que trata la presente Circular cumplan con las instrucciones del Capítulo 20-9 de la Recopilación Actualizada de Normas para bancos, que contiene el conjunto de lineamientos y buenas prácticas para la gestión de los riesgos de continuidad de negocios y que deben ser considerados para desarrollar los planes y medidas de continuidad operacional antes indicadas, las que en todo caso deben ser observadas considerando la naturaleza, volumen y complejidad de las operaciones de cada institución.

5. Comunicación de incidentes operacionales

Las entidades deberán comunicar a esta Comisión los incidentes operacionales a los que se refiere el N° 1 del Capítulo 20-8 de la Recopilación Actualizada de Normas para bancos, mediante la casilla habilitada por esta Comisión a través de su Extranet, en la oportunidad y forma que indica el numeral 1.1 del referido Capítulo.

Asimismo, la institución será responsable de informar oportunamente a los clientes o usuarios sobre la ocurrencia de incidentes que afecten la calidad o continuidad de los servicios, o cuando se trate de un hecho de público conocimiento, según se indica en el numeral 1.2 del citado Capítulo.

6. Gestión de seguridad de la información y ciberseguridad

Las disposiciones del BCCH establecen que como parte de los elementos que deben ser considerados para el desarrollo e implementación de las políticas de gestión y control de riesgos de los emisores y operadores de tarjetas de pago, se incluyan las medidas necesarias para resguardar la ciberseguridad y de otra índole adoptadas para prevenir y mitigar los riesgos de fraude, así como los demás aspectos que pueda instruir esta Comisión.

En atención a lo indicado, se dispone que las entidades de que trata la presente Circular cumplan con las instrucciones contenidas en el Capítulo 20-10 de la Recopilación Actualizada de Normas para bancos, que contiene el conjunto de lineamientos y buenas prácticas para una adecuada gestión de la seguridad de información y ciberseguridad, las que en todo caso deben ser observadas considerando la naturaleza, volumen y complejidad de las operaciones de cada institución.
