CAPÍTULO 1-7

TRANSFERENCIA ELECTRÓNICA DE INFORMACIÓN Y FONDOS

1. Aplicación de las presentes normas.

Las presentes normas se refieren a la prestación de servicios bancarios y la realización de operaciones interbancarias que se efectúan mediante transmisiones de mensajes o instrucciones a un computador conectado por redes de comunicación propias o de terceros, efectuadas desde otro computador o mediante el uso de otros dispositivos electrónicos (cajeros automáticos, teléfonos, PINPAD, etc.).

Dichos servicios comprenden tanto las transferencias electrónicas de fondos como cualquier otra operación que se realice utilizando documentos o mensajes electrónicos, o dispositivos que permiten a los clientes del banco la ejecución automática de operaciones. Además, estas normas alcanzan también a las comunicaciones por vía electrónica que no den origen a una operación propiamente tal, cuando la información transmitida esté sujeta a secreto o reserva de acuerdo con lo establecido por la Ley General de Bancos.

Por transferencias electrónicas de fondos se entienden todas aquellas operaciones realizadas por medios electrónicos que originen cargos o abonos de dinero en cuentas, tales como: traspasos automatizados de fondos efectuados por un cliente de una cuenta a otra; órdenes de pago para abonar cuentas de terceros (proveedores, empleados, accionistas, etc.); recaudaciones mediante cargos a cuentas corrientes (impuestos, imposiciones previsionales, servicios, etc.); giros de dinero mediante cajeros automáticos, etc. En general, comprenden las descritas y cualquier otra operación que se efectúe por aquellos medios, en que un usuario habilitado para ello instruye o ejecuta movimientos de dinero en una o más cuentas.

2. Requisitos que deben cumplir los sistemas utilizados.

Para habilitar un sistema de transferencia electrónica de información o de fondos, los bancos deberán considerar el cumplimiento de los siguientes requisitos básicos:

A) Para la prestación de los servicios deberá celebrarse un contrato entre el banco y el cliente, en el cual queden claramente establecidos los derechos y responsabilidades de cada una de las partes que intervienen en las operaciones.

B) Los sistemas utilizados, junto con permitir el registro y seguimiento íntegro de las operaciones realizadas, deberán generar archivos que permitan respaldar los antecedentes de cada operación, necesarios para efectuar cualquier examen o certificación posterior, tales como, fechas y horas en que se realizaron, contenido de los mensajes, identificación de los operadores, emisores y receptores, cuentas y montos involucrados, terminales desde los cuales se operó, etc.

La conservación de estos archivos se regirá por lo establecido por esta Superintendencia en el Capítulo 1-10 de esta Recopilación Actualizada de Normas.

C) El sistema debe 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 y al tipo de operación, que permitan asegurar su autenticidad e integridad.

La institución financiera debe mantener permanentemente abierto y disponible un canal de comunicación que permita al usuario ejecutar o solicitar el bloqueo de cualquier operación que intente efectuarse utilizando sus medios de acceso o claves de autenticación. Cada sistema que opere en línea y en tiempo real, debe permitir dicho bloqueo también en tiempo real.

D) Las instalaciones y configuraciones de los equipos y de las redes deben garantizar la continuidad de las operaciones frente a eventos fortuitos o deliberados, debiendo considerarse el uso de equipos y respaldos, como asimismo de procedimientos alternativos, que permitan superar las contingencias que pudieren afectar o interrumpir el normal funcionamiento de los sistemas.

Los sistemas deberán contener los mecanismos físicos y lógicos de seguridad para controlar que se ejecuten todas las operaciones que se inician, debiendo estar en condiciones de detectar cualquier alteración o intervención a la información transferida, entre el punto en que ésta se origina y aquel en que es recibida por el destinatario.

E) Los sistemas que permitan ejecutar transferencias de fondos, junto con reconocer la validez de la operación que el usuario realice, deben controlar que los importes girados no superen el saldo disponible o el límite que se haya fijado para el efecto.

Para todos los sistemas de transferencia automática de fondos deberá establecerse un límite en los montos de transferencia con respecto a cada cliente con acceso al sistema. Cuando se trate de un servicio de uso masivo que no contempla la posibilidad de efectuar transacciones importantes, dicho límite podrá fijarse en forma general para todos los usuarios.

En todo caso, los sistemas deberán contemplar el cumplimiento de cualquier restricción normativa que pueda afectar una transacción, como es el caso de límites de crédito, sobregiros y retenciones, extracción desde cuentas de ahorro con giro diferido, etc.

F) Los sistemas de transferencia electrónica de fondos deberán generar la información necesaria para que el cliente pueda conciliar los movimientos de dinero efectuados, tanto por terminales como por usuario habilitado, incluyendo, cuando corresponda, totales de las operaciones realizadas en un determinado período.

En todo caso, los terminales de acceso común a cualquier cliente en que se originen transacciones, tales como cajeros automáticos o dispositivos asociados al uso de tarjetas de débito, deben generar los comprobantes en que conste el detalle de la transacción u operación ejecutada.

G) Las instituciones que contraten los servicios de una empresa de intermediación electrónica, deberán quedar en posición de verificar el cumplimiento de los requisitos básicos mencionados en los literales anteriores y de los demás aspectos que aseguren la autenticidad, integridad y confidencialidad de los documentos electrónicos y de las claves de acceso.

Dichas empresas deberán estar en condiciones de certificar, a petición de cualquiera de las partes involucradas, la validez y oportunidad de emisión y recepción de los mensajes transmitidos.

En todo caso, debe tenerse presente que la generación de algunos documentos electrónicos que constituyen documentación de carácter oficial para el cumplimiento de disposiciones legales, puede requerir la realización de las correspondientes operaciones de transferencia electrónica de información y fondos a través de una empresa de servicio de intermediación electrónica, de acuerdo con las regulaciones o autorizaciones de los respectivos organismos fiscalizadores. Así ocurre, por ejemplo, con las facturas en relación con las normas del Servicio de Impuestos Internos, con las planillas de imposiciones previsionales según las instrucciones de la Superintendencia de Pensiones, etc.

H) Los bancos deberán ponderar la exposición al riesgo financiero y operativo de los sistemas de transferencia de que se trata y considerar, en consecuencia, las instancias internas de revisiones y autorizaciones previas que sean necesarias.

Para el adecuado control de los riesgos inherentes a la utilización de estos sistemas, es necesario que los bancos cuenten con profesionales capacitados para evaluarlos antes de su liberación y para mantener bajo vigilancia, mediante procedimientos de auditoría acordes con la tecnología utilizada, su funcionamiento, mantención y necesidades de adecuación de los diversos controles computacionales y administrativos que aseguran su confiabilidad.

3. Transferencias interbancarias.

Los bancos pueden participar, a través de empresas de servicio o con servidores administrados por ellas mismas y con las modalidades de operación convenidas entre las partes, en sistemas de transferencia electrónica de fondos interbancaria.

Los pagos que diariamente deban efectuarse como consecuencia del uso de tales sistemas, sea que se compensen o no previamente las obligaciones recíprocas, deberán resolverse en definitiva en la cámara de compensación de operaciones interfinancieras de que trata el Capítulo III.H.2 del Compendio de Normas Financieras del Banco Central de Chile.

En ningún caso el sistema de transferencia electrónica de fondos al cual esté adherida una institución, podrá incorporar el canje de documentos, puesto que éste sólo puede realizarse a través de la Cámara de Compensación.

4. Transferencias electrónicas de fondos entre clientes de distintos bancos, mediante redes públicas de comunicaciones.

4.1. Generalidades.

Con el objeto de proveer mayor seguridad y un mejor servicio a sus clientes, los bancos deberán disponer que las transferencias que se realicen a través de canales electrónicos se cumplan de forma inmediata, en la medida que exista la correspondiente provisión de fondos. Así, los respectivos cargos y abonos o puesta a disposición de los respectivos beneficiarios del importe de estas transferencias deben efectuarse simultáneamente y de inmediato, en el mismo día en que se ordena y curse la transferencia. Esta simultaneidad debe cumplirse tanto en aquellas transferencias que se realicen entre cuentas dentro del mismo banco, como en aquellas en que el abono en cuenta o pago al respectivo beneficiario deba efectuarse en otro banco.

Los canales electrónicos que ofrezcan las instituciones bancarias para realizar estas transferencias deberán contar con apropiados privilegios de autorización y medidas de autentificación, controles de acceso lógico y físicos, adecuada infraestructura de seguridad para observar el cumplimiento de las restricciones y límites que se establezcan para las actividades internas y externas, así como para cuidar la integridad de los datos de cada transacción y la adecuada privacidad de los registros e información de los clientes. Para esos efectos deberán:

a) contar con una plataforma tecnológica que comprenda una encriptación sólida;

b) disponer de a lo menos dos factores de autentificación distintos para cada transacción, debiendo ser uno de ellos de generación o asignación dinámica;

c) establecer la exigencia de firma digital avanzada para las transferencias superiores a un monto que el banco determine.

Lo anterior, sin perjuicio de incorporar en sus procesos las mejores prácticas para la administración del riesgo operacional, de banca electrónica y los estándares internacionales que existen sobre la materia.

4.2. Prevención de fraudes.

Los bancos deberán 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 potencialmente fraudulentas, 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 cliente, del no cliente (por ejemplo en los intentos de acceso), de los puntos de acceso (por ejemplo direcciones IP, Cajero Automático u otros), hacer el seguimiento y correlacionar eventos y/o fraudes a objeto de detectar otros fraudes, puntos en que estos se cometen, modus operandi, y puntos de compromisos, entre otros.

4.3. Detección de Lavado de activos.

Las transferencias electrónicas de fondos dentro del mercado financiero pueden ser utilizadas como una herramienta más para realizar el lavado de activos. Para mitigar el riesgo de dicha práctica por esta vía, es necesario que las instituciones bancarias, complementando los esquemas de autentificación robusta, cuenten con mecanismos o herramientas de identificación, evaluación de riesgos, monitoreo y detección de lavado de activos, para facilitar dos aspectos principales: la detección de patrones predefinidos en la operación de lavado de activo y el rastreo transaccional para la detección de formas o prácticas emergentes mediante el análisis de las desviaciones de comportamiento respecto a los estándares de cada uno de los clientes.

5. Cajeros automáticos.

5.1 Generalidades.

Los bancos son responsables, ya sea que el servicio se preste directamente o a través de terceros, del debido funcionamiento de su red de cajeros automáticos y del cumplimiento de los requisitos que se establecen a continuación. Dichos requerimientos se refieren a actividades relacionadas con la reposición de efectivo, mantención periódica de los dispositivos, monitoreo continuo del funcionamiento de las redes y sistemas sobre los que se sustenta el servicio, así como la oportuna resolución de los incidentes que pongan en riesgo la continuidad operacional.

Asimismo, dichas entidades deben velar por el cumplimiento de las exigencias legales en materia de seguridad pública aplicables a los cajeros automáticos y transporte de valores, precaviendo que tal responsabilidad se encuentre resguardada en los contratos que se celebren con terceros, especialmente cuando los dispositivos se encuentren ubicados fuera de las dependencias de un banco.

5.2 Definiciones.

Período de funcionamiento predefinido: Corresponde al lapso dentro del cual cada uno de sus cajeros automáticos tendrá la capacidad de dispensar dinero de manera continua.

Para efectos de determinar el período de funcionamiento predefinido de cada cajero automático, se deben considerar los horarios de funcionamiento de los establecimientos donde estos se encuentran emplazados.

Indicador de disponibilidad de servicio o *Uptime*: Se refiere al tiempo, respecto de un período de funcionamiento predefinido, en que los cajeros automáticos estuvieron habilitados para efectuar giros de dinero.

Indicador de indisponibilidad de servicio o *Downtime*: Período de tiempo dentro del lapso de funcionamiento predefinido, en que los cajeros automáticos no se encontraron habilitados para efectuar giros de dinero.

El *Downtime* de un cajero automático se computará como el cociente entre el tiempo en que el dispositivo no permitió realizar transacciones de retiro de efectivo y el período de funcionamiento predefinido

5.3 Estándares mínimos de disponibilidad de servicio.

La disponibilidad de servicio de los cajeros automáticos no podrá ser inferior a 95%. Por lo tanto, el *Downtime* de la red de cajeros automáticos de cada entidad deberá mantenerse dentro de un rango no superior al 5%. Esto, sin perjuicio de las políticas que defina el directorio de cada entidad, relativas a establecer un límite de *Downtime* inferior.

Además de aquellas situaciones que puedan ser catalogadas como caso fortuito o fuerza mayor, las instituciones bancarias podrán descontar en dicha medición aquellos tiempos de indisponibilidad producidos por la necesidad de realizar ajustes a su dotación de cajeros automáticos, que se encuentren en proceso de adaptación a cambios en las regulaciones en materia de seguridad pública, debiendo para el efecto remitir a esta Superintendencia el plan asociado a su implementación. Asimismo, se podrán descontar del cómputo las indisponibilidades que resulten de actos vandálicos que inhabiliten la operatividad de los dispositivos. También se podrán restar aquellos casos relacionados con remodelaciones, traslados o cierres de los locales, cuando se trate de cajeros emplazados en establecimientos no dependientes de la administración de la propia institución, sin perjuicio de que esta situación deba ser adecuadamente informada a los usuarios.

El cómputo del referido índice de disponibilidad corresponderá a lo siguiente:

$$DS = \sum \left(PF_n^{\,i} - d_n^{\,i} \right) \times \frac{1}{\sum PF_n^{\,i}} ,$$

donde:

DS = Disponibilidad promedio de servicio mensual de todos los cajeros de la institución bancaria.

PF_n^i = Período de funcionamiento predefinido, en minutos, del dispositivo n durante el día i del mes de medición. Se trata de un indicador fijo para cada dispositivo en particular, definido según los días, horarios y condiciones de funcionamiento del lugar en que está emplazado.

d_n^i = Cantidad de minutos en que el dispositivo n no se encontraba habilitado para efectuar giros de dinero durante el día i del mes de medición (*Downtime* del dispositivo), dentro del período de funcionamiento predefinido.

5.4 Requisitos de gestión.

Sin perjuicio de las disposiciones contenidas en los números 1 y 2 del presente Capítulo y de lo indicado en materia de administración de riesgo operacional en el Capítulo 1-13 de esta Recopilación, el banco deberá contemplar dentro de sus políticas de gestión las siguientes medidas:

5.4.1. Sistemas de monitoreo.

Las entidades deben disponer de sistemas de monitoreo que permitan detectar, de manera continua, las fallas y causas que impidan el normal funcionamiento de los cajeros automáticos. Los sistemas de monitoreo dispuestos por las entidades deberán mantenerse activos durante la totalidad del período de funcionamiento predefinido de los dispositivos y contar con medidas de contingencia en caso de falla del sistema principal.

5.4.2 Información de gestión.

Los bancos deben mantener un sistema de información de gestión, que permita una oportuna identificación de las situaciones que afectan los índices de disponibilidad, tales como las fluctuaciones de demanda de efectivo, fallas en el funcionamiento del dispositivo o de su red de cajeros, así como la naturaleza, frecuencia y origen de las mismas. Dicho sistema debe generar los antecedentes necesarios para una adecuada y oportuna evaluación, tanto del cumplimiento de los estándares de disponibilidad de servicio definidos por la entidad, como de los establecidos en este Capítulo.

La información generada deberá ser dada a conocer periódicamente al Directorio o a quién haga sus veces, para una adecuada toma de decisiones.

5.4.3 Políticas y procedimientos de funcionamiento de los cajeros automáticos.

Los bancos deben mantener políticas y procedimientos formales, aprobados por el Directorio, para administrar los riesgos operacionales relacionados con el funcionamiento de su red de cajeros automáticos, el cumplimiento de los niveles mínimos de disponibilidad de servicio y los planes de regularización de los dispositivos afectados por siniestros graves, que puedan requerir la reposición de los mismos.

Las políticas y procedimientos también deben referirse a las condiciones generales que deberán cumplir los lugares donde se encuentren emplazados los dispositivos, acordes con la cobertura geográfica que se contempla mantener y la naturaleza o el tipo de establecimientos en que sean instalados (ej. sucursales del propio banco, estaciones de servicios, centros comerciales, etc.). Asimismo, deben considerar directrices para el establecimiento de las condiciones contractuales mínimas para la instalación de cajeros fuera de las dependencias de la institución.

El área o función que será responsable de la observancia de dichas políticas deberá quedar claramente definida.

5.4.4 Manejo de incidentes.

Para responder a los eventos que impidan el normal funcionamiento de los dispositivos, la institución deberá contar con la estructura necesaria para el manejo de incidentes, que le permitan evaluar cada situación y tomar oportunamente las medidas para su regularización.

La información que se presente al público, acerca de los problemas de funcionamiento de los cajeros automáticos deberá dar cuenta, en términos generales, del plazo estimado para las restitución del servicio.

5.5 Información a la Superintendencia.

Las instituciones bancarias deberán mantener sistemas de información que les permitan generar estadísticas del funcionamiento de su red de cajeros automáticos (identificación de los terminales, ubicación, disponibilidad de servicio, horarios de funcionamiento predefinidos, cantidad de interrupciones, causales de indisponibilidad, etc.), las cuales deben estar disponibles a solicitud de la Superintendencia.

———