CAPÍTULO DÉCIMO SEGUNDO: REQUERIMIENTOS MÍNIMOS DE SEGURIDAD Y CALIDAD PARA LA REALIZACIÓN DE OPERACIONES

Superfinanciera. 26/03/2012

CONTENIDO

CAPÍTULO DÉCIMO SEGUNDO: REQUERIMIENTOS MÍNIMOS DE SEGURIDAD Y CALIDAD PARA LA REALIZACIÓN DE OPERACIONES

1. Ámbito de aplicación

Las instrucciones de que trata el presente capitulo deberán ser adoptadas por todas las entidades sometidas a la inspección y vigilancia de la Superintendencia Financiera de Colombia (SFC), con excepción de las siguientes: el Fondo de Garantías de Instituciones Financieras

"Fogafín", el Fondo de Garantías de Entidades Cooperativas "Fogacoop", el Fondo Nacional de Garantías S.A. "F.N.G. S.A.", el Fondo Financiero de Proyectos de Desarrollo "Fonade", los Almacenes Generales de Depósito, los Fondos de Garantía que se constituyan en el mercado público de valores, los Fondos Mutuos de Inversión, los Fondos Ganaderos, las Sociedades Calificadoras de Valores y/o Riesgo, las Oficinas de Representación de Instituciones Financieras y de Reaseguros del Exterior, los Corredores de Seguros y de Reaseguros, los Comisionistas Independientes de Valores, las Sociedades Comisionistas de Bolsas Agropecuarias y los Organismos de Autorregulación.

Sin embargo, las entidades exceptuadas de la aplicación del presente capítulo citadas en el párrafo anterior, deberán dar cumplimiento a los criterios de seguridad y calidad de la información, establecidos en los numerales 2.1. y 2.2 del presente capítulo.

El numeral 3.1.13 "Elaborar el perfil de las costumbres transacciones de cada uno de sus clientes…" deberá ser aplicado únicamente por los establecimientos de crédito, sin perjuicio de que las demás entidades, cuando lo consideren conveniente, pongan en práctica las instrucciones allí contenidas.

El numeral 7 "Análisis de vulnerabilidades" deberá ser aplicado únicamente por los establecimientos de crédito y los administradores de sistemas de pago de bajo valor, sin perjuicio de que las demás entidades, cuando lo consideren conveniente, pongan en práctica las instrucciones allí contenidas.

Los establecimientos de crédito que presten servicios financieros a través de corresponsales bancarios deberán sujetarse, para el uso de este canal de distribución, a las instrucciones contenidas en el capítulo noveno, Título III de la presente circular.

En todo caso las entidades vigiladas destinatarias de las instrucciones del presente numeral, deberán implementar los requerimientos exigidos atendiendo la naturaleza, objeto social y demás características particulares de su actividad.

2. Definiciones y criterios de seguridad y calidad de la información

Para el cumplimiento de los requerimientos mínimos de seguridad y calidad de la información que se maneja a través de canales e instrumentos para la realización de operaciones, las entidades deberán tener en cuenta las siguientes definiciones y criterios:

2.1 Criterios de seguridad de la información

a) Confidencialidad: Hace referencia a la protección de información cuya divulgación no está autorizada.

b) Integridad: La información debe ser precisa, coherente y completa desde su creación hasta su destrucción.

c) Disponibilidad: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

2.2 Criterios de calidad de la información

a) Efectividad: La información relevante debe ser pertinente y su entrega oportuna, correcta y consistente.

b) Eficiencia: El procesamiento y suministro de información debe hacerse utilizando de la mejor manera posible los recursos.

c) Confiabilidad: La información debe ser la apropiada para la administración de la entidad y el cumplimiento de sus obligaciones.

2.3 Canales de distribución de servicios financieros

Para los efectos del presente capítulo son canales de distribución de servicios financieros, entre otros, los siguientes:

a) Oficinas.
b) Cajeros Automáticos (ATM).
c) Receptores de cheques.
d) Receptores de dinero en efectivo.
e) POS (incluye PIN Pad).
f) Sistemas de Audio Respuesta (IVR).
g) Centro de atención telefónica (Call Center, Contact Center).
h) Sistemas de acceso remoto para clientes (RAS).
i) Internet.
j) Dispositivos móviles.

2.4 Instrumentos para la realización de operaciones

Son los elementos con los que se imparten las órdenes para la realización de operaciones a través de los canales de distribución, los cuales son, entre otros, los siguientes:

a) Tarjetas débito.
b) Tarjetas crédito.
c) Dispositivos móviles (teléfonos móviles).
d) Órdenes electrónicas para la transferencia de fondos.

2.5 Vulnerabilidad informática

Ausencia o deficiencia de los controles informáticos que permiten el acceso no autorizado a los canales de distribución o a los sistemas informáticos de la entidad.

2.6 Cifrado fuerte

Técnicas de codificación para protección de la información que utilizan algoritmos reconocidos internacionalmente, brindando al menos los niveles de seguridad ofrecidos por 3DES o AES.

2.7 Sistema de acceso remoto (RAS)

Acceso brindado por las entidades vigiladas a sus clientes para la realización de operaciones mediante el uso de aplicaciones personalizadas, utilizando generalmente enlaces dedicados.

2.8 Operaciones

2.8.1. Operaciones no monetarias
Son las acciones a través de las cuales se desarrollan, ejecutan o materializan los productos o servicios que prestan las entidades a sus clientes o usuarios y que no conllevan movimiento, manejo o transferencia de dinero.

2.8.2. Operaciones monetarias
Son las acciones que implican o conllevan movimiento, manejo o transferencia de dinero.

2.9. Cliente

Es toda persona natural o jurídica con la cual la entidad establece y mantiene una relación contractual o legal para el suministro de cualquier producto o servicio propio de su actividad.

2.10. Usuario

Aquella persona natural o jurídica a la que, sin ser cliente, la entidad le presta un servicio.

2.11. Producto

Son las operaciones legalmente autorizadas que pueden adelantar las entidades vigiladas mediante la celebración de un contrato o que tienen origen en la ley.

2.12. Servicio

Es toda aquella interacción de las entidades sometidas a inspección y vigilancia de la SFC con sus clientes y usuarios para el desarrollo de su objeto social.

2.13. Dispositivo
Mecanismo, máquina o aparato dispuesto para producir una función determinada.

2.14. Información confidencial

Atendiendo lo dispuesto en el artículo 15 de la Constitución Política de Colombia y sin perjuicio de lo establecido en el numeral 4 Capítulo Noveno de la presente Circular y demás normas aplicables sobre la materia, se considerará confidencial para efectos de la aplicación del presente Capitulo, toda aquella información amparada por la reserva bancaria.

Las entidades podrán clasificar como confidencial otro tipo de información. Esta clasificación deberá estar debidamente documentada y a disposición de la Superintendencia Financiera de Colombia.

2.15. Autenticación

Conjunto de técnicas y procedimientos utilizados para verificar la identidad de un cliente, entidad o usuario.

2.16. Mecanismos fuertes de autenticación

Se entenderán como mecanismos fuertes de autenticación los siguientes:

2.16.1. Biometría.
2.16.2. OTP (One Time Password).
2.16.3. Tarjetas que cumplan el estándar EMV, en combinación con un segundo factor de autenticación.
2.16.4. Registro y validación de algunas características físicas de los computadores desde los cuales se realizarán las operaciones, en combinación con un segundo factor de autenticación.

2.17. Banca Móvil

Servicio de banca electrónica en el cual el teléfono móvil es el dispositivo utilizado para realizar operaciones, cuyo número de línea es asociado al servicio.

Los servicios que se presten a través de dispositivos móviles y utilicen navegadores web, son considerados banca por internet.

2.18. Proveedor de telecomunicaciones

Empresa que presta el servicio de conexión entre la entidad destinataria de comunicación y el operador de telefonía.

2.19. Operador de Telefonía Móvil

Compañía que provee los servicios de comunicación a los usuarios de telefonía móvil.

3. Obligaciones generales

En desarrollo de lo dispuesto en el presente Capitulo, las entidades deberán incluir en sus políticas y procedimientos relativos a la administración de la información, los criterios de que tratan los numerales 2.1 y 2.2.

Adicionalmente, para dar aplicación a dichos criterios las entidades deberán adoptar, al menos, las medidas que se relacionan a continuación:

3.1 Seguridad y calidad

En desarrollo de los criterios de seguridad y calidad las entidades deberán cumplir, como mínimo, con los siguientes requerimientos:

3.1.1 Disponer de hardware, software y equipos de telecomunicaciones, así como de los procedimientos y controles necesarios, que permitan prestar los servicios y manejar la información en condiciones de seguridad y calidad.
3.1.2 Gestionar la seguridad de la información, para lo cual podrán tener como referencia el estándar ISO 27000, o el que lo sustituya.
3.1.3 Disponer que el envío de información confidencial y de los instrumentos para la realización de operaciones a sus clientes, se haga en condiciones de seguridad. Cuando dicha información se envíe como parte de, o adjunta a un correo electrónico, ésta deberá estar cifrada.
3.1.4 Dotar de seguridad la información confidencial de los clientes que se maneja en los equipos y redes de la entidad.

3.1.5 Velar porque la información enviada a los clientes esté libre de software malicioso.

3.1.6 Proteger las claves de acceso a los sistemas de información. En desarrollo de esta obligación, las entidades deberán evitar el uso de claves compartidas, genéricas o para grupos. La identificación y autenticación en los dispositivos y sistemas de cómputo de las entidades deberá ser única y personalizada.

3.1.7 Dotar a sus terminales, equipos de cómputo y redes de los elementos necesarios que eviten la instalación de programas o dispositivos que capturen la información de sus clientes y de sus operaciones.

3.1.8 Velar porque los niveles de seguridad de los elementos usados en los canales no se vean disminuidos durante toda su vida útil.

3.1.9 Ofrecer los mecanismos necesarios para que los clientes tengan la posibilidad de personalizar las condiciones bajo las cuales realicen operaciones monetarias por los diferentes canales, siempre y cuando éstos lo permitan. En estos eventos se puede permitir que el cliente inscriba las cuentas a las cuales realizará transferencias, registre las direcciones IP fijas y el o los números de telefonía móvil desde los cuales operará.

3.1.10 Ofrecer la posibilidad de manejar contraseñas diferentes para los instrumentos o canales, en caso de que éstos lo requieran y/o lo permitan.

3.1.11 Establecer los mecanismos necesarios para que el mantenimiento y la instalación o desinstalación de programas o dispositivos en las terminales o equipos de cómputo sólo pueda ser realizado por personal debidamente autorizado.

3.1.12 Establecer procedimientos para el bloqueo de canales o de instrumentos para la realización de operaciones, cuando existan situaciones o hechos que lo ameriten o después de un número de intentos de accesos fallidos por parte de un cliente, así como las medidas operativas y de seguridad para la reactivación de los mismos.

3.1.13 Elaborar el perfil de las costumbres transaccionales de cada uno de sus clientes y definir procedimientos para la confirmación oportuna de las operaciones monetarias que no correspondan a sus hábitos.

3.1.14 Realizar una adecuada segregación de funciones del personal que administre, opere, mantenga y, en general, tenga la posibilidad de acceder a los dispositivos y sistemas usados en los distintos canales e instrumentos para la realización de operaciones. En desarrollo de lo anterior, las entidades deberán establecer los procedimientos y controles para el alistamiento, transporte, instalación y mantenimiento de los dispositivos usados en los canales de distribución de servicios.

3.1.15 Definir los procedimientos y medidas que se deberán ejecutar cuando se encuentre evidencia de la alteración de los dispositivos usados en los canales de distribución de servicios financieros.

3.1.16 Sincronizar todos los relojes de los sistemas de información de la entidad involucrados en los canales de distribución. Se deberá tener como referencia la hora oficial suministrada por la Superintendencia de Industria y Comercio.

3.1.17 Tener en operación sólo los protocolos, servicios, aplicaciones, usuarios, equipos, entre otros, necesarios para el desarrollo de su actividad.

3.1.18 Contar con controles y alarmas que informen sobre el estado de los canales, y además permitan identificar y corregir las fallas oportunamente.

3.1.19 Incluir en el informe de gestión a que se refiere el artículo 47 de la ley 222 de 1995 y sus modificaciones, un análisis sobre el cumplimiento de las obligaciones enumeradas en la presente Circular.

3.1.20 Considerar en sus políticas y procedimientos relativos a los canales de distribución, la atención a personas con discapacidades físicas, con el fin de que no se vea menoscabada la seguridad de su información.

3.2 Tercerización – Outsourcing

Las entidades que contraten bajo la modalidad de *outsourcing* o tercerización, a personas naturales o jurídicas, para la atención parcial o total de los distintos canales o de los dispositivos usados en ellos, o que en desarrollo de su actividad tengan acceso a información confidencial de la entidad o de sus clientes, deberán cumplir, como mínimo, con los siguientes requerimientos:

3.2.1 Definir los criterios y procedimientos a partir de los cuales se seleccionarán los terceros y los servicios que serán atendidos por ellos.

3.2.2 Incluir en los contratos que se celebren con terceros o en aquellos que se prorroguen a partir de la entrada en vigencia del presente Capitulo, por lo menos, los siguientes aspectos:

a) Niveles de servicio y operación.
b) Acuerdos de confidencialidad sobre la información manejada y sobre las actividades desarrolladas.
c) Propiedad de la información.
d) Restricciones sobre el software empleado.
e) Normas de seguridad informática y física a ser aplicadas.
f) Procedimientos a seguir cuando se encuentre evidencia de alteración o manipulación de dispositivos o información.
g) Procedimientos y controles para la entrega de la información manejada y la destrucción de la misma por parte del tercero una vez finalizado el servicio.

Las entidades contarán con los procedimientos necesarios para verificar el cumplimiento de las obligaciones señaladas en el presente numeral, los cuales deberán ser informados previamente a la auditoría interna o quien ejerza sus funciones.

3.2.3 Exigir que los terceros contratados dispongan de planes de contingencia y continuidad debidamente documentados. Las entidades deberán verificar que los planes, en lo que corresponde a los servicios convenidos, funcionen en las condiciones pactadas.

3.2.4 Establecer procedimientos que permitan identificar físicamente, de manera inequívoca, a los funcionarios de los terceros contratados.

3.2.5 Implementar mecanismos de cifrado fuerte para el envío y recepción de información confidencial con los terceros contratados.

3.3 Documentación

En materia de documentación las entidades deben cumplir, como mínimo, con los siguientes requerimientos:

Dejar constancia de todas las operaciones que se realicen a través de los distintos canales, la cual deberá contener cuando menos lo siguiente: fecha, hora, código del dispositivo (para operaciones realizadas a través de IVR: el número del teléfono desde el cual se hizo la llamada; para operaciones por Internet: la dirección IP desde la cual se hizo la misma; para operaciones con dispositivos móviles, el número desde el cual se hizo la conexión), cuenta(s), número de la operación y costo de la misma para el cliente o usuario.

En los casos de operaciones que obedecen a convenios, se dejará constancia del costo al que se refiere el presente numeral, cuando ello sea posible.

3.3.1 Velar porque los órganos de control, incluyan en sus informes la evaluación acerca del cumplimiento de los procedimientos, controles y seguridades, establecidos por la entidad y las normas vigentes, para la prestación de los servicios a los clientes y usuarios, a través de los diferentes canales de distribución.

3.3.2 Generar informes trimestrales sobre la disponibilidad y número de operaciones realizadas en cada uno de los canales de distribución. Esta información deberá ser conservada por un término de dos (2) años.

3.3.3 Cuando a través de los distintos canales se pidan y se realicen donaciones, se deberá generar y entregar un soporte incluyendo el valor de la donación y el nombre del beneficiario.

3.3.4 Conservar todos los soportes y documentos donde se hayan establecido los compromisos, tanto de las entidades como de sus clientes y las condiciones bajo las cuales éstas prestarán sus servicios. Se debe dejar evidencia documentada de que los clientes las han conocido y aceptado. Esta información deberá ser conservada por lo menos por dos (2) años, contados a partir de la fecha de terminación de la relación contractual o en caso de que la información sea objeto o soporte de una reclamación o queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

3.3.5 Llevar un registro de las consultas realizadas por los funcionarios de la entidad sobre la información confidencial de los clientes, que contenga al menos lo siguiente: identificación del funcionario que realizó la consulta, canal utilizado, identificación del equipo, fecha y hora. En desarrollo de lo anterior, se deberán establecer mecanismos que restrinjan el acceso a dicha información, para que solo pueda ser usada por el personal que lo requiera en función de su trabajo.

3.3.6 Llevar el registro de las actividades adelantadas sobre los dispositivos finales a cargo de la entidad, usados en los canales de distribución de servicios, cuando se realice su alistamiento, transporte, mantenimiento, instalación y activación.

3.3.7 Dejar constancia del cumplimiento de la obligación establecida en el numeral 3.4.4.

3.3.8 Grabar las llamadas realizadas por los clientes a los centros de atención telefónica cuando consulten o actualicen su información.

3.3.9 La información a que se refieren los numeral 3.3.1, 3.3.6 y 3.3.9 deberá ser conservada por lo menos por dos (2) años. En el caso en que la información respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

3.4 Divulgación de información

En materia de divulgación de información las entidades deberán cumplir, como mínimo, con los siguientes requerimientos:

3.4.1 En concordancia con lo dispuesto en el artículo 97 del E.O.S.F., suministrar a los clientes información clara, completa y oportuna de los productos, servicios y operaciones.

3.4.2 Dar a conocer a sus clientes y usuarios, por el respectivo canal y en forma previa a la realización de la operación, el costo de la misma, si lo hay, brindándoles la posibilidad de efectuarla o no. Tratándose de cajeros automáticos la obligación sólo aplica para operaciones realizadas en el territorio nacional y cuyo autorizador tenga domicilio en Colombia.

3.4.3 Establecer las condiciones bajo las cuales los clientes podrán ser informados en línea acerca de las operaciones realizadas con sus productos.

3.4.4 Informar adecuadamente a los clientes respecto de las medidas de seguridad que deberán tener en cuenta para la realización de operaciones por cada canal, así como los procedimientos para el bloqueo, inactivación, reactivación y cancelación de los productos y servicios ofrecidos.

3.4.5 Establecer y publicar por los canales de distribución, en los que sea posible, las medidas de seguridad que deberá adoptar el cliente para el uso de los mismos.

3.4.6 Diseñar procedimientos para dar a conocer a los clientes, usuarios y funcionarios, los riesgos derivados del uso de los diferentes canales e instrumentos para la realización de operaciones.

3.4.7 Generar un soporte al momento de la realización de cada operación monetaria. Dicho soporte deberá contener al menos la siguiente información: fecha, hora (hora y minuto), código del dispositivo (para Internet: la dirección IP desde la cual se hizo la misma; para dispositivos móviles: el número desde el cual se hizo la conexión), número de la operación, costo para el cliente o usuario, tipo de operación, entidades involucradas (si a ello hay lugar) y número de las cuentas que afectan. Se deberán ocultar los números de las cuentas con excepción de los últimos cuatro (4) caracteres, salvo cuando se trate de la cuenta que recibe una transferencia. Cuando no se pueda generar el soporte, se deberá advertir previamente al cliente o usuario de esta situación. Para el caso de IVR y dispositivos móviles se entenderá cumplido el requisito establecido en este numeral cuando se informe el número de la operación. En relación con el costo de la operación y tratándose de cajeros automáticos, la obligación sólo aplica para operaciones realizadas en el territorio nacional y cuyo autorizador tenga domicilio en Colombia. Tratándose de pagos inferiores a dos (2) salarios mínimos legales diarios vigentes SMLDV, no será obligatorio la generación del soporte al que se refiere el presente numeral.

3.4.8 Dentro de los procedimiento de cancelación o terminación de un producto, siempre que el cliente lo solicite, las entidades deberán entregar constancia en la que se advierta encontrarse a paz y salvo por todo concepto, asegurándose que los futuros reportes a los operadores de bancos de datos de que trata la Ley 1266 de 2008 sean consistentes con su estado de cuenta. Tratándose de tarjetas de crédito dicha constancia deberá entregarse al cliente en un tiempo máximo de cuarenta y cinco (45) días, contados a partir de la fecha de solicitud de la cancelación.

4 Obligaciones adicionales por tipo de canal

4.1 Oficinas

Para las oficinas donde se realicen operaciones monetarias las entidades deberán cumplir, como mínimo, con los siguientes requerimientos:

4.1.1 Los sistemas informáticos empleados para la prestación de servicios en las oficinas deben contar con soporte por parte del fabricante o proveedor.

4.1.2 Los sistemas operacionales de los equipos empleados en las oficinas deben cumplir con niveles de seguridad adecuados que garanticen protección de acceso controlado.

4.1.3 Contar con cámaras de video, las cuales deben cubrir al menos el acceso principal y las áreas de atención al público. Las imágenes deberán ser conservadas por lo menos ocho (8) meses o en el caso en que la imagen respectiva sea objeto o soporte de una

reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

4.1.4 Disponer de los mecanismos necesarios para evitar que personas no autorizadas atiendan a los clientes o usuarios en nombre de la entidad.

4.1.5 La información que viaja entre las oficinas y los sitios centrales de las entidades deberá estar cifrada usando hardware de propósito específico, o software, o una combinación de los anteriores. Para los Establecimientos de Crédito el hardware o software empleados deberán ser totalmente separados e independientes de cualquier otro dispositivo o elemento de procesamiento de información, de seguridad informática, de transmisión y/o recepción de datos, de comunicaciones, de conmutación, de enrutamiento, de gateways, servidores de acceso remoto (RAS) y/o de concentradores. En cualquiera de los casos anteriores se deberá emplear cifrado fuerte. Las entidades deberán evaluar con regularidad la efectividad y vigencia de los mecanismos de cifrado adoptados.

4.1.6 Establecer procedimientos necesarios para atender de manera segura y eficiente a sus clientes en todo momento, en particular cuando se presenten situaciones especiales tales como: fallas en los sistemas, restricciones en los servicios, fechas y horas de mayor congestión, posible alteración del orden público, entre otras, así como para el retorno a la normalidad. Las medidas adoptadas deberán ser informadas oportunamente a los clientes y usuarios.

4.1.7 Contar con los elementos necesarios para la debida atención del público, tales como: lectores de código de barras, contadores de billetes y monedas, PIN Pad, entre otros, que cumplan con las condiciones de seguridad y calidad, de acuerdo con los productos y servicios ofrecidos en cada oficina.

4.1.8 Los PIN Pad deberán estar en capacidad de operar con las tarjetas a que alude los numerales 6.11 y 6.12 del presente capítulo.

4.2 Cajeros automáticos (ATM)

Los cajeros automáticos deberán cumplir, como mínimo, con los siguientes requerimientos:

4.2.1 Contar con sistemas de video grabación que asocien los datos y las imágenes de cada operación monetaria. Las imágenes deberán ser conservadas por lo menos ocho (8) meses o en el caso en que la imagen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

4.2.2 Cuando el cajero automático no se encuentre físicamente conectado a una oficina, la información que viaja entre este y su respectivo sitio central de procesamiento se deberá proteger utilizando cifrado fuerte, empleando para ello hardware de propósito específico independiente. Las entidades deberán evaluar con regularidad la efectividad y vigencia del mecanismo de cifrado adoptado.

4.2.3 Los dispositivos utilizados para la autenticación del cliente o usuario en el cajero deben emplear cifrado.

4.2.4 Implementar el intercambio dinámico de llaves entre los sistemas de cifrado, con la frecuencia necesaria para dotar de seguridad a las operaciones realizadas.

4.2.5 Los sitios donde se instalen los cajeros automáticos deberán contar con las medidas de seguridad físicas para su operación y estar acordes con las especificaciones del fabricante. Adicionalmente, deben tener mecanismos que garanticen la privacidad en la realización de operaciones para que la información usada en ellas no quede a la vista de terceros.

4.2.6 Implementar mecanismos de autenticación que permitan confirmar que el cajero es un dispositivo autorizado dentro de la red de la entidad.

4.2.7 Estar en capacidad de operar con las tarjetas a que alude los numerales 6.11 y 6.12 del presente capítulo.

4.3 Receptores de cheques

Los dispositivos electrónicos que permitan la recepción o consignación de cheques deberán cumplir, como mínimo, con los siguientes requerimientos:

4.3.1 Contar con mecanismos que identifiquen y acepten los cheques, leyendo automáticamente, al menos, los siguientes datos: la entidad emisora, el número de cuenta y el número de cheque.

4.3.2 Los cheques o documentos no aceptados por el módulo para recepción de cheques no podrán ser retenidos y deberán ser retornados inmediatamente al cliente o usuario, informando la causa del reintegro.

4.3.3 Una vez el cliente o usuario deposite el cheque, el sistema deberá mostrar una imagen del mismo y la información asociada a la operación monetaria, para confirmar los datos de la misma y proceder o no a su realización. En caso negativo deberá devolver el cheque o documento, dejando un registro de la operación

4.3.4 Como parte del procedimiento de consignación del cheque se le debe poner una marca que indique que este fue depositado en el módulo.

4.4 Receptores de dinero en efectivo

Los dispositivos que permitan la recepción de dinero en efectivo deberán cumplir, como mínimo, con los siguientes requerimientos:

4.4.1 Contar con mecanismos que verifiquen la autenticidad y denominación de los billetes.

4.4.2 Totalizar el monto de la operación con los billetes aceptados y permitir que el cliente o usuario confirme o no su realización. En este último caso se debe devolver la totalidad de los billetes entregados, generando el respectivo registro.

4.4.3 Las operaciones en efectivo deben realizarse en línea, afectando el saldo de la respectiva cuenta. La operación no quedará sujeta a verificación.

4.4.4 Los billetes no aceptados no podrán ser retenidos y deben ser retornados inmediatamente al cliente o usuario.

4.5 POS (incluye PIN Pad)

Los POS deberán cumplir, como mínimo, con los siguientes requerimientos:

4.5.1 La lectura de tarjetas solo se deberá hacer a través de la lectora de los datáfonos y los PIN Pad.

4.5.2 Cumplir el estándar EMV (Europay MasterCard VISA).

4.5.3 Los administradores de las redes de este canal deberán validar automáticamente la autenticidad del datáfono que se intenta conectar a ellos, así como el medio de comunicación a través del cual operará.

4.5.4 Establecer procedimientos que le permitan a los responsables de los datáfonos en los establecimientos comerciales, confirmar la identidad de los funcionarios autorizados para retirar o hacerle mantenimiento a los dispositivos.

4.5.5 Velar porque la información confidencial de los clientes y usuarios no sea almacenada o retenida en el lugar en donde los POS estén siendo utilizados.

4.5.6 Contar con mecanismos que reduzcan la posibilidad de que terceros puedan ver la clave digitada por el cliente o usuario.

4.6 Sistemas de audio respuesta (IVR)

Los sistemas de audio respuesta deberán cumplir, como mínimo, con los siguientes requerimientos:

4.6.1 Permitir al cliente confirmar la información suministrada en la realización de la operación monetaria.

4.6.2 Permitir transferir la llamada a un operador, al menos en los horarios hábiles de atención al público.

4.6.3 Las entidades que permitan realizar operaciones monetarias por este canal, deben ofrecer a sus clientes mecanismos fuertes de autenticación.

4.7 Centro de atención telefónica (Call Center, Contact Center)

Los centros de atención telefónica deberán cumplir, como mínimo, con los siguientes requerimientos:

4.7.1 Destinar un área dedicada exclusivamente para la operación de los recursos necesarios en la prestación del servicio, la cual deberá contar con los controles físicos y lógicos que impidan el ingreso de personas no autorizadas, así como la extracción de la información manejada.

4.7.2 Impedir el ingreso de dispositivos que permitan almacenar o copiar cualquier tipo de información, o medios de comunicación, que no sean suministrados por la entidad.

4.7.3 Dotar a los equipos de cómputo que operan en el centro de atención telefónica de los elementos necesarios que impidan el uso de dispositivos de almacenamiento no autorizados por la entidad. Igualmente, se deberá bloquear cualquier tipo de conexión a red distinta a la usada para la prestación del servicio.

4.7.4 Garantizar que los equipos de cómputo destinados a los centros de atención telefónica solo serán utilizados en la prestación de servicios por ese canal.

4.7.5 En los equipos de cómputo usados en los centros de atención telefónica no se permitirá la navegación por Internet, el envío o recepción de correo electrónico, la mensajería instantánea, ni ningún otro servicio que permita el intercambio de información, a menos que se cuente con un sistema de registro de la información enviada y recibida. Estos registros deberán ser conservados por lo menos ocho (8) meses o en el caso en que la información respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

4.8 Sistemas de acceso remoto para clientes

Las entidades que ofrezcan servicio de acceso remoto para la realización de operaciones monetarias deberán contar con un módulo de seguridad de hardware para el sistema, que cumpla al menos con el estándar de seguridad **FIPS-140-2** (Federal Information Processing Standard), el cual deberá ser de propósito específico (appliance) totalmente separado e independiente de cualquier otro dispositivo o elemento de procesamiento de información, de

seguridad informática, de transmisión y/o recepción de datos, de comunicaciones, de conmutación, de enrutamiento, de gateways, de servidores de acceso remoto (RAS) y/o de concentradores.

4.9 Internet

Las entidades que ofrezcan la realización de operaciones por Internet deberán cumplir con los siguientes requerimientos:

4.9.1 Implementar los algoritmos y protocolos necesarios para brindar una comunicación segura.

4.9.2 Realizar como mínimo dos veces al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación usados en la realización de operaciones monetarias por este canal. Sin embargo, cuando se realicen cambios en la plataforma que afecten la seguridad del canal, deberá realizarse una prueba adicional.

4.9.3 Promover y poner a disposición de sus clientes mecanismos que reduzcan la posibilidad de que la información de sus operaciones monetarias pueda ser capturada por terceros no autorizados durante cada sesión.

4.9.4 Establecer el tiempo máximo de inactividad, después del cual se deberá dar por cancelada la sesión, exigiendo un nuevo proceso de autenticación para realizar otras operaciones.

4.9.5 Informar al cliente, al inicio de cada sesión, la fecha y hora del último ingreso a este canal.

4.9.6 Implementar mecanismos que permitan a la entidad financiera verificar constantemente que no sean modificados los enlaces (links) de su sitio Web, ni suplantados sus certificados digitales, ni modificada indebidamente la resolución de sus DNS.

4.9.7 Contar con mecanismos de protección para incrementar la seguridad de los portales, protegiéndolos de ataques de negación de servicio, inyección de código malicioso u objetos maliciosos, que afecten la seguridad de la operación o su conclusión exitosa.

4.9.8 Las entidades que permitan realizar operaciones monetarias por este canal, deben ofrecer a sus clientes mecanismos fuertes de autenticación.

4.10 Prestación de servicios a través de nuevos canales

Cuando la entidad decida iniciar la prestación de servicios a través de nuevos canales, diferentes a los que tiene en uso, además del cumplimiento de las instrucciones generales de seguridad y calidad, deberá adelantar el respectivo análisis de riesgos del nuevo canal. Dicho análisis deberá ser puesto en conocimiento de la junta directiva y los órganos de control.

La entidad deberá remitir a la SFC, con al menos quince (15) días calendario de antelación a la fecha prevista para el inicio de la distribución de servicios a través del nuevo canal, la siguiente información:

a) Descripción del procedimiento que se adoptará para la prestación del servicio.
b) Tecnología que utilizará el nuevo canal.
c) Análisis de riesgos y medidas de seguridad y control del nuevo canal.
d) Planes de contingencia y continuidad para la operación del canal.

e) Plan de capacitación dirigido a los clientes y usuarios, para el uso del nuevo canal, así como para mitigar los riesgos a los que se verían expuestos.

4.11 Banca Móvil

Los servicios de banca móvil que presten las entidades deberán cumplir con los siguientes requerimientos:

4.11.1 Contar con mecanismos de autenticación de dos (2) factores para la realización de operaciones monetarias y no monetarias.

4.11.2. Para operaciones monetarias individuales o que acumuladas mensualmente por cliente superen dos (2) SMLMV, implementar mecanismos de cifrado fuerte de extremo a extremo para el envío y recepción de información confidencial de las operaciones realizadas, tales como clave, número de cuenta, número de tarjeta, etc. Esta información, en ningún caso, podrá ser conocida por los operadores de telefonía móvil o los proveedores de telecomunicaciones, ni almacenada en el teléfono móvil.

Los mensajes de texto que se envíen al teléfono móvil como parte del servicio de alertas o notificación de operaciones no requieren ser cifrados, salvo que incluyan información confidencial.

4.11.3 Cuando el servicio que se preste no cifre la información de extremo a extremo, la entidad deberá adoptar las medidas necesarias para mitigar el riesgo asociado a esta forma de operar, el cual debe incluir la revisión de los mecanismos de seguridad en donde la información no se encuentre cifrada. La Superintendencia Financiera de Colombia (SFC) podrá suspender el uso del canal cuando se advierta que existen fallas que afecten la seguridad de la información.

4.11.4 El servicio de banca móvil deberá contar con medidas que garanticen la atomicidad de las operaciones y eviten su duplicidad debido a fallas en la comunicación ocasionadas por la calidad de la señal, el traslado entre celdas, etc.

4.11.5 Los servicios que se presten para la realización de operaciones a través de Internet, en sesiones originadas desde el teléfono móvil, deben cumplir con los requerimientos establecidos en el numeral 4.9 Internet.

5 Reglas sobre actualización de software

5.1.1 Con el propósito de mantener un adecuado control sobre el software, las entidades deberán cumplir, como mínimo, con las siguientes medidas:

5.2 Mantener tres ambientes independientes: uno para el desarrollo de software, otro para la realización de pruebas, y un tercer ambiente para los sistemas en producción. En todo caso, el desempeño y la seguridad de un ambiente no podrá influir en los demás.

5.3 Implementar procedimientos que permitan verificar que las versiones de los programas del ambiente de producción corresponden a las versiones de programas fuentes catalogadas.

5.4 Cuando las entidades necesiten tomar copias de la información de sus clientes para la realización de pruebas, se deberán establecer los controles necesarios para garantizar su destrucción, una vez concluidas las mismas.

5.5 Contar con procedimientos y controles para el paso de programas a producción. El software en operación deberá estar catalogado.

5.6 Contar con interfases para los clientes o usuarios que cumplan con los criterios de seguridad y calidad, de tal manera que puedan hacer uso de ellas de una forma simple e intuitiva.

5.7 Mantener documentada y actualizada, al menos, la siguiente información: parámetros de los sistemas donde operan las aplicaciones en producción, incluido el ambiente de comunicaciones; versión de los programas y aplicativos en uso; soportes de las pruebas realizadas a los sistemas de información; y procedimientos de instalación del software.

6 Obligaciones específicas para tarjetas débito y crédito

6.1 Establecer y documentar los procedimientos, controles y medidas de seguridad necesarias para la emisión, transporte, recepción, custodia, entrega, devolución y destrucción de las tarjetas. Se debe estipular el tiempo máximo de permanencia de las tarjetas en cada una de estas etapas.

6.2 Cifrar la información de los clientes que sea remitida a los proveedores y fabricantes de tarjetas, para mantener la confidencialidad de la misma.

6.3 Velar porque los centros de operación en donde se realizan procesos tales como: realce, estampado, grabado y magnetización de las tarjetas, entre otros, así como de la impresión del sobreflex, mantengan procedimientos, controles y medidas de seguridad orientadas a evitar que la información relacionada pueda ser copiada, modificada o utilizada con fines diferentes a los de la fabricación de la misma.

6.4 Velar porque en los centros donde se realicen los procesos citados en el numeral anterior, apliquen procedimientos y controles que garanticen la destrucción de aquellas tarjetas que no superen las pruebas de calidad establecidas para su elaboración, así como la información de los clientes utilizada durante el proceso. Iguales medidas se deberán aplicar a los sobreflex.

6.5 Establecer los procedimientos, controles y medidas de seguridad necesarias para la creación, asignación y entrega de las claves a los clientes.

6.6 Cuando la clave (PIN) asociada a una tarjeta débito haya sido asignada por la entidad vigilada, esta deberá ser cambiada por el cliente antes de realizar su primera operación.

6.7 Ofrecer a sus clientes mecanismos que brinden la posibilidad inmediata de cambiar la clave de la tarjeta débito en el momento que éstos lo consideren necesario.

6.8 Establecer en los convenios que se suscriben con los establecimientos de comercio la obligación de verificar la firma y exigir la presentación del documento de identidad del cliente para las operaciones monetarias que se realicen con tarjeta de crédito.

6.9 Emitir tarjetas personalizadas que contengan al menos la siguiente información: nombre del cliente, indicación de si es crédito o débito, nombre de la entidad emisora, fecha de expiración, espacio para la firma del cliente y número telefónico de atención al cliente.

6.10 Al momento de la entrega de la tarjeta a los clientes, ésta deberá estar inactiva. Las entidades deberán definir un procedimiento para su respectiva activación, el cual contemple al menos dos de tres factores de autenticación: algo que se sabe, algo que se tiene, algo que se es. En cualquier caso, se deberán entregar las tarjetas exclusivamente al cliente o a quien este autorice.

6.11 Entregar a sus clientes tarjetas de crédito que manejen internamente mecanismos fuertes de autenticación, tales como OTP (One Time Password), biometría, etc, siempre que los cupos aprobados superen dos (2) SMLMV. Dichas tarjetas deberán servir indistintamente para realizar operaciones en cajeros automáticos (ATM) y en puntos de pago (POS).

6.12 Entregar a sus clientes tarjetas débito que manejen internamente mecanismos fuertes de autenticación, tales como OTP (One Time Password), biometría, entre otros. Dichas tarjetas deberán servir indistintamente para realizar operaciones en cajeros automáticos (ATM) y en puntos de pago (POS).

Sin perjuicio de otras medidas de seguridad, los mecanismos fuertes de autenticación no serán obligatorios en tarjetas débito ligadas a productos utilizados para canalizar recursos provenientes de programas de ayuda y/o subsidios otorgados por el Estado Colombiano siempre que estos no superen dos (2) SMLMV.

7 Análisis de vulnerabilidades

7.1.1 Las entidades deberán implementar un sistema de análisis de vulnerabilidades informáticas que cumpla al menos con los siguientes requisitos

7.2 Estar basado en un hardware de propósito específico (appliance) totalmente separado e independiente de cualquier dispositivo de procesamiento de información, de comunicaciones y/o de seguridad informática.

7.3 Generar de manera automática por lo menos dos (2) veces al año un informe consolidado de las vulnerabilidades encontradas. Los informes de los últimos dos años deberán estar a disposición de la SFC.

7.4 Las entidades deberán tomar las medidas necesarias para remediar las vulnerabilidades detectadas en sus análisis.

7.5 Realizar un análisis diferencial de vulnerabilidades, comparando el informe actual con respecto al inmediatamente anterior.

7.6 Las herramientas usadas en el análisis de vulnerabilidades deberán estar homologadas por el CVE (Common Vulnerabilities and Exposures) y actualizadas a la fecha de su utilización.

7.6.1 Para la generación de los informes solicitados se deberá tomar como referencia la lista de nombres de vulnerabilidades CVE publicada por la corporación Mitre (www.mitre.org).