obstante lo anterior, es posible la contratación sin ninguna información sobre el estado del riesgo, caso en el cual debe entenderse que la entidad aseguradora asume el riesgo sin consideración respecto del estado del mismo.

Los mecanismos de comprobación de la asegurabilidad deben identificar como mínimo aquella información necesaria para acreditar que el consumidor financiero cumple con las condiciones para ser asegurado (p. ej.: edad, profesión, características del empleo). Estos mecanismos deben permitir a la entidad aseguradora determinar si el tomador o asegurado, dadas sus condiciones particulares al momento de contratación del seguro, se encuentra fuera del amparo del producto, es decir, que este no se encuentra afectado, previamente a la adquisición del seguro, por circunstancias que conducirían a una objeción en la reclamación del seguro.

Las entidades aseguradoras deben abstenerse de celebrar contratos de seguro en aquellos casos en que el mecanismo de comprobación de asegurabilidad refleje que la cobertura no le es aplicable al tomador o asegurado.

## 1.3. Otros canales e instrumentos de prestación de servicios financieros

En adición a la forma de prestación de servicios indicados en los numerales anteriores, se reconocen como canales en la distribución de los servicios ofrecidos por las entidades vigiladas, especialmente las que realizan intermediación financiera, los siguientes:

1.3.1. Cajeros Automáticos (ATM).

1.3.2. Receptores de cheques.

1.3.3. Receptores de dinero en efectivo.

1.3.4. POS (incluye PIN Pad).

1.3.5. Sistemas de Audio Respuesta (IVR).

1.3.6. Centro de atención telefónica (Call Center, Contact Center).

1.3.7. Sistemas de acceso remoto para clientes (RAS).

1.3.8. Internet.

1.3.9. Banca móvil.

Como complemento de los canales señalados se reconocen dentro de los instrumentos adecuados en la prestación de estos servicios las tarjetas débito, tarjetas crédito, los móviles y demás dispositivos electrónicos que sirvan para realizar operaciones y las órdenes electrónicas como los elementos a través de los cuales se imparten las órdenes que materializan las operaciones a través de los canales de distribución.

Para los efectos de estas instrucciones se entiende por dispositivo el mecanismo, máquina o aparato dispuesto para producir una función determinada.

**Las entidades vigiladas pueden adoptar tecnologías como realidad aumentada, internet de las cosas, blockchain, inteligencia artificial, machine learning, big data, robots, entre otras, cuando lo consideren pertinente para mejorar la prestación de servicios a los consumidores financieros y optimizar sus procesos. Para el efecto, la entidad debe realizar una adecuada gestión de los riesgos asociados a la tecnología adoptada, verificar de manera regular la efectividad de los controles implementados y dar cumplimiento a las normas vigentes en materia de protección de datos y habeas data.**

## 1.4. Uso de red

Se imparten las instrucciones que deben atender las entidades vigiladas, en desarrollo de las modalidades de uso de red, establecidas en el art. 93 del EOSF y el art. 5 de la Ley 389 de 1997, así como en el Capítulo 2, Título 2, Libro 31 y el Título 1, Libro 34, de la Parte II del Decreto 2555 de 2010.

## 1.4.1. Modalidades de uso de red

## 1.4.1.1. Modalidad prevista en el art. 5 de la Ley 389 de 1997.

Según lo establecido en el parágrafo del art. 2.34.1.1.1 del Decreto 2555 de 2010, se entiende como Red el conjunto de medios o elementos a través de los cuales sus prestadores suministran los servicios del usuario de la red al público. Forman parte de la Red los canales presenciales y no presenciales, los empleados y los sistemas de información que tenga habilitados el respectivo prestador.

Son sistemas de información, el conjunto de elementos tecnológicos orientados al tratamiento y administración de datos destinados a la realización de las operaciones autorizadas por el art. 2.34.1.1.2 del Decreto 2555 de 2010.

Son canales presenciales aquellos en los que el consumidor financiero asiste personalmente al mismo, tales como las oficinas, los cajeros automáticos, los receptores de cheques, los receptores de dinero en efectivo y los datáfonos (POS, incluye PIN Pad).

Son canales no presenciales aquellos en los que el consumidor financiero es atendido de manera remota, tales como la banca móvil, el internet, los sistemas de audio respuesta (IVR), los centros de atención telefónica (Call Center, Contact Center) y los sistemas de acceso remoto para clientes.

1.4.1.1.1. Contrato de uso de red

Las entidades usuarias de la red deben remitir a la SFC los contratos en que se acuerde el uso de red, previamente a su celebración y con la antelación prevista en los arts. 2.31.2.2.4 y 2.34.1.1.4 del Decreto 2555 de 2010, según cada caso. En adición a lo establecido en el art. 2.34.1.1.3 del Decreto 2555 de 2010, los contratos deben contener al menos lo siguiente:

1.4.1.1.1.1. Identificación de las partes y objeto del contrato.

1.4.1.1.1.2. Los productos y operaciones que se van a promocionar y gestionar en virtud del contrato de uso de red, especificando en cada caso el detalle de los canales presenciales y no presenciales por medio de los cuales se prestará el servicio. Se debe indicar si los servicios incluirán la prestación del deber de asesoría, de acuerdo con lo dispuesto en el parágrafo 4° del art. 2.34.1.1.2 y el art. 3.1.4.1.3 del Decreto 2555 de 2010.

1.4.1.1.1.3. Las obligaciones de las partes asociadas al intercambio de información que permita garantizar un adecuado suministro de información a los consumidores financieros para cada producto específico; así como las que correspondan a la administración del riesgo operativo y del riesgo de lavado de activos y financiación del terrorismo, asociados al desarrollo del contrato.

2.2.2. 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.

2.2.3. 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.

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

2.2.5. Autenticación: Conjunto de técnicas y procedimientos utilizados para verificar la identidad de un cliente, entidad o usuario. Los factores de autenticación son: algo que se sabe, algo que se tiene, algo que se es.

2.2.6. Mecanismos fuertes de autenticación: Se entienden como mecanismos fuertes de autenticación los siguientes:

**2.2.6.1. Biometría en combinación con un segundo factor de autenticación para operaciones no presenciales. En aquellos eventos en que la operación se efectúe de manera presencial no se requerirá el uso de un segundo factor de autenticación.**

2.2.6.2. Certificados de firma digital de acuerdo a lo establecido en la Ley 527 de 1999 y sus decretos reglamentarios.

2.2.6.3. OTP (One Time Password), en combinación con un segundo factor de autenticación.

2.2.6.4. Tarjetas que cumplan el estándar EMV, en combinación con un segundo factor de autenticación.

2.2.6.5. Registro y validación de algunas características de los computadores o equipos móviles desde los cuales se realizarán las operaciones, en combinación con un segundo factor de autenticación.

2.2.7. Proveedores de redes y servicios de telecomunicaciones: Son las empresas reguladas por la Comisión de Regulación de Comunicaciones y debidamente habilitadas por el Ministerio de Tecnologías de la Información y las Comunicaciones, responsables de la operación de redes y/o de la provisión de servicios de telecomunicaciones a terceros, de acuerdo a lo establecido en el art 1. de la Resolución 202 de 2010.

2.2.8. Ambiente de venta presente: transacciones en las cuales el instrumento de pago interactúa con el dispositivo de captura de información.

2.2.9. Ambiente de venta no presente: transacciones en las cuales el instrumento de pago no interactúa con el dispositivo de captura de información.

2.2.10. Entidades administradoras de pasarelas de pago: entidades que prestan servicios de aplicación de comercio electrónico para almacenar, procesar y/o transmitir el pago correspondiente a operaciones de venta en línea.

2.2.11. Código QR (Quick Response Code): Es un código de respuesta rápida, bidimensional, con estructura cuadrada. Tiene la capacidad de almacenar datos codificados, es de fácil lectura y tiene mayor capacidad de almacenamiento que los códigos universales de productos (UPC por sus siglas en inglés) o códigos de barras. Puede ser estático (su contenido no cambia, generalmente impreso) o dinámico (cambia su contenido para cada compra, generado por software en tiempo real).

Los códigos QR pueden ser adaptados para transacciones tales como pagos, transferencias P2P o P2B .

**2.2.12. Tokenización: Proceso de remplazar un dato confidencial por otro equivalente que no lo es (no confidencial), el cual garantiza la misma operatividad y no tiene un valor intrínseco.**

**2.2.13. Característica biométrica: Atributo biológico o comportamental de un individuo del cual se pueden extraer propiedades distintivas y repetibles para su reconocimiento.**

**2.2.14. Muestra biométrica: Representación que se obtiene de una característica biométrica capturada mediante un dispositivo vinculado a un sistema biométrico, como una imagen facial, una grabación de voz o una imagen de huella digital.**

**2.2.15. Plantilla biométrica: Representación de una o varias muestras biométricas utilizadas para la comparación, reconocimiento e individualización de una persona, las cuales pueden construirse a través de métodos tales como vectores, datos numéricos y algoritmos criptográficos.**

**2.2.16. Omnicanalidad: Estrategia que busca mejorar la experiencia del consumidor y la eficiencia operativa, proporcionando la mayor homogeneidad posible en los diferentes canales y el uso de varios de ellos en la ejecución de las operaciones, cuando esto resulte procedente.**

**2.2.17. Pagos sin contacto (*contactless*): Sistema que permite pagar una compra mediante tecnologías de identificación por radiofrecuencia o lectura electrónica, incorporadas en tarjetas de crédito o débito, llaveros, tarjetas inteligentes, teléfonos móviles u otros dispositivos.**

## 2.3. Criterios

2.3.1. Respecto de la seguridad de la información

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

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

2.3.1.3. 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.

2.3.2. Respecto de la calidad de la información

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

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

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

2.3.3 Requerimientos generales

2.3.3.1. En materia de seguridad y calidad de la información

A fin de dar debida aplicación a los criterios antes indicados las entidades deben adoptar, al menos, las medidas que se relacionan a continuación:

2.3.3.1.1. 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.

2.3.3.1.2. Gestionar la seguridad de la información, para lo cual pueden tener como referencia el estándar ISO 27000, o el que lo sustituya.

2.3.3.1.3. 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, mensajería instantánea o cualquier otra modalidad de comunicación electrónica, ésta debe estar cifrada.

2.3.3.1.4. Dotar de seguridad la información confidencial de los clientes que se maneja en los equipos y redes de la entidad.

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

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

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

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

2.3.3.1.9. 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.

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

**2.3.3.1.25. Promover estrategias de omnicanalidad que tengan en cuenta las políticas de gestión de riesgos y modelo de negocio de la entidad, así como las particularidades de cada tipo de operación.**

**2.3.3.1.26. Establecer los parámetros a partir de los cuales las entidades requerirán mecanismos fuertes de autenticación para las transacciones realizadas mediante pago con o sin contacto, en consideración al análisis de riesgo asociado a esta tecnología. Estos parámetros deben ser informados a los consumidores financieros.**

**2.3.3.1.27. Establecer mecanismos fuertes de autenticación para las operaciones que, de acuerdo con el análisis de riesgo de cada entidad, generen mayor exposición al riesgo de fraude o suplantación. El análisis debe estar documentado y a disposición de la SFC. Igualmente, este análisis debe tener en cuenta aspectos como el perfil transaccional del cliente, monto de operaciones, tipo de producto, canal, etc.**

**En todo caso, será obligatorio implementar mecanismos fuertes de autenticación para las siguientes operaciones:**

**2.3.3.1.27.1. La actualización de datos del cliente para la notificación de operaciones monetarias o generación de alertas (p.ej. correo electrónico, celular).**

**2.3.3.1.27.2.** **Las operaciones realizadas con tarjeta débito y crédito, en territorio nacional, en ambiente presente, cuando el emisor sea colombiano, y se superen los parámetros establecidos en cumplimiento de lo dispuesto en el subnumeral 2.3.3.1.26. del presente capítulo.**

**2.3.3.1.28. Contar con soporte para los sistemas informáticos empleados en la prestación de servicios, el cual puede ser prestado por el fabricante, proveedor o sus distribuidores autorizados.**

**2.3.3.1.29. Promover alternativas, conforme a su modelo de negocio, para realizar operaciones de comercio electrónico con cargo a productos distintos a las tarjetas de crédito aprobadas a sus clientes y plataformas tecnológicas como los botones de pago.**

2.3.3.2. En materia de documentación

Las entidades deben cumplir, como mínimo, con los siguientes requerimientos:

2.3.3.2.1. Dejar constancia de todas las operaciones que se realicen a través de los distintos canales, la cual debe 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 debe dejar constancia del costo al que se refiere el presente numeral, cuando ello sea posible.

2.3.3.2.2. 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.

2.3.3.2.3. Generar informes trimestrales sobre la disponibilidad y número de operaciones realizadas en cada uno de los canales de distribución. Esta información debe ser conservada por un término de 2 años.

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

2.3.3.2.5. 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 prestan sus servicios. Se debe dejar evidencia documentada de que los clientes las han conocido y aceptado. Esta información debe ser conservada por lo menos por 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.

2.3.3.2.6. 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 deben 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.

2.3.3.2.7. 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.

2.3.3.2.8. Dejar constancia del cumplimiento de la obligación de informar adecuadamente a los clientes respecto de las medidas de seguridad que deben 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.

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

La información a que se refieren los subnumerales 2.3.3.2.1., 2.3.3.2.6 y 2.3.3.2.9. debe ser conservada por lo menos por 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.

2.3.4. Requerimientos especiales por tipo de canal

2.3.4.1. En oficinas

La realización de operaciones monetarias a través de oficinas conlleva el cumplimiento, como mínimo, de los siguientes requerimientos de seguridad:

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

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

2.3.4.1.3. Contar con cámaras de video, las cuales deben cubrir al menos el acceso principal y las áreas de atención al público. Las imágenes deben ser conservadas por lo menos 6 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.

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

2.3.4.1.5. La información que viaja entre las oficinas y los sitios centrales de las entidades debe 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 deben 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 debe emplear cifrado fuerte. Las entidades deben evaluar con regularidad la efectividad y vigencia de los mecanismos de cifrado adoptados.

2.3.4.1.6. 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 deben ser informadas oportunamente a los clientes y usuarios.

2.3.4.1.7. 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.

2.3.4.2. Cajeros automáticos (ATM)

Deben cumplir, como mínimo, con los siguientes requerimientos:

2.3.4.2.1. Contar con sistemas de video grabación que asocien los datos y las imágenes de cada operación monetaria. Las imágenes deben ser conservadas por lo menos 6 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.

2.3.4.2.2. 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 debe proteger utilizando cifrado fuerte, empleando para ello hardware de propósito específico independiente. Las entidades deben evaluar con regularidad la efectividad y vigencia del mecanismo de cifrado adoptado.

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

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

2.3.4.2.5. Los sitios donde se instalen los cajeros automáticos deben 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.

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

2.3.4.2.7. Estar en capacidad de operar con las tarjetas a que aluden el subnumeral 2.3.4.12.11 del presente Capítulo.

**2.3.4.2.8. Contar con mecanismos que permitan a la entidad emisora del instrumento de pago reversar automáticamente los retiros realizados en cajeros, en territorio nacional, cuando el dinero no haya sido entregado por causas que sean atribuibles al funcionamiento del mismo y que sean conocidas por la entidad.**

**En este caso se debe informar al consumidor financiero, por cualquier medio expedito, que la entidad procederá a realizar la reversión. En ningún caso la entidad podrá cobrar por la operación ni debitar ningún concepto asociado a la misma.**

**2.3.4.2.9. Adoptar los procedimientos necesarios para permitir, en su red de cajeros, el retiro en una sola operación del monto máximo diario establecido por la entidad según su evaluación de riesgos correspondiente, o por el cliente cuando éste sea menor al establecido por la entidad.**

2.3.4.3. Receptores de cheques

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

2.3.4.3.1. 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.

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

2.3.4.3.3. Una vez el cliente o usuario deposite el cheque, el sistema debe 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 debe devolver el cheque o documento, dejando un registro de la operación.

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

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

2.3.4.12.3. 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.

2.3.4.12.4. Velar porque en los centros donde se realicen los procesos citados en el subnumeral 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 deben aplicar a los sobreflex.

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

2.3.4.12.6. Cuando la clave (PIN) asociada a una tarjeta débito **o crédito** haya sido asignada por la entidad vigilada, esta debe ser cambiada por el cliente antes de realizar su primera operación **con este PIN**.

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

**2.3.4.12.8. Establecer los procedimientos, controles y medidas para la notificación al cliente de la inscripción de pagos en la entidad financiera o por parte de terceros con cargo a sus cuentas o tarjetas de crédito.  
Las entidades deben notificar a sus clientes acerca de la inscripción de pagos por parte de terceros con cargos a sus cuentas o tarjetas de crédito siempre que el tercero le informe a la entidad acerca de la inscripción de dicho pago.**

**2.3.4.12.9. Emitir tarjetas personalizadas que contengan al menos la siguiente información: nombre del cliente, nombre de la entidad emisora y fecha de expiración. Las entidades pueden emitir tarjetas innominadas cuando el análisis de riesgo realizado por ellas lo estime procedente.**

2.3.4.12.10. Al momento de la entrega de la tarjeta a los clientes, ésta debe estar inactiva. Las entidades deben definir un procedimiento para su respectiva activación, el cual contemple, al menos, dos de tres factores de autenticación. En cualquier caso, se deben entregar las tarjetas exclusivamente al cliente o a quien este autorice.

2.3.4.12.11. Entregar a sus clientes tarjetas débito y/o crédito que manejen internamente mecanismos fuertes de autenticación, siempre que los cupos aprobados superen 2 SMMLV.Dichas tarjetasdeben 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 son obligatorios en tarjetas débito asociadas a productos utilizados para canalizar recursos provenientes de programas de ayuda y/o subsidios otorgados por el Estado Colombiano siempre que estos no superen 2 SMMLV.

Lo dispuesto en los numerales 2.3.4.12.1., 2.3.4.12.2., 2.3.4.12.3., 2.3.4.12.4. y 2.3.4.12.8. de este Capítulo no debe ser cumplido cuando se trate de tarjetas virtuales.

**2.3.4.12.12. Adoptar mecanismos de seguridad para la realización de operaciones en ambiente no presente, adicionales a la validación del número de la tarjeta, la fecha de vencimiento y un código de verificación estático, tales como autorización por parte del consumidor financiero desde la app, CVV dinámico, tokenización y 3DSecure, entre otros.**

2.3.4.13. Operaciones por medio de códigos QR

Las entidades que ofrezcan la realización de pagos utilizando códigos QR deben tener como referencia el estándar internacional para aceptar pagos EMVCo LLC, versión 1.0 EMV® QR Code Specification for Payment Systems (EMV QRCPS) Merchant-Presented Mode, emitido en julio de 2017, o aquellos que lo modifiquen, sustituyan o adicionen y deben cumplir con los siguientes requerimientos:

2.3.4.13.1. Proporcionar al consumidor financiero, directamente o a través de terceros, aplicaciones de software que permitan leer el código QR y enrutar la operación.

2.3.4.13.2. Facilitar que los datos que no puedan ser obtenidos con la lectura del código QR estático y sean necesarios para la transacción (p.ej. monto), sean capturados por la aplicación del consumidor financiero que realiza la operación.

2.3.4.13.3. Cumplir con los requerimientos establecidos en los sub numerales 2.3.4.9, 2.3.4.11 y 2.3.5 del presente capítulo para la implementación del software para realizar pagos o generar los códigos QR dinámicos.

2.3.4.13.4. Gestionar los riesgos que se puedan derivar de la realización de este tipo de operaciones.

2.3.4.13.5 Con el propósito de promover la interoperabilidad, las entidades administradoras de los sistemas de Pago de Bajo Valor (SPBV) deben concertar y definir de manera conjunta la estructura de los campos donde debe enviarse la información, adicional al estándar, que resulte necesaria para la realización de las operaciones (p.ej. el código identificador del comercio y la discriminación de los impuestos). Cualquier modificación a la estructura definida debe ser informada y socializada a los participantes del sistema de pagos 3 meses antes de su implementación.

La información de los campos definidos debe estar a disposición de la SFC y ser publicada en el sitio web de la entidad administradora para consulta de todos los interesados.

2.3.5 Requerimientos en materia de actualización de Software

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

2.3.5.1. 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 pueden influir en los demás.

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

2.3.6.2.3. Propiedad de la información.

2.3.6.2.4. Restricciones sobre el software empleado.

2.3.6.2.5. Normas de seguridad informática y física a ser aplicadas.

2.3.6.2.6. Procedimientos a seguir cuando se encuentre evidencia de alteración o manipulación de dispositivos o información.

2.3.6.2.7. 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 deben contar con los procedimientos necesarios para verificar el cumplimiento de las obligaciones señaladas en el presente subnumeral, los cuales deben ser informados previamente a la auditoría interna o quien ejerza sus funciones.

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

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

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

2.3.7 Análisis de vulnerabilidades

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

2.3.7.1. 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.

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

2.3.7.3. Las entidades deben tomar las medidas necesarias para remediar las vulnerabilidades detectadas en sus análisis.

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

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

2.3.7.6. Para la generación de los informes solicitados se debe tomar como referencia la lista de nombres de vulnerabilidades CVE publicada por la corporación Mitre.

2.3.8. Vinculación de entidades administradoras de pasarelas de pago y establecimientos de comercio

Los establecimientos de crédito y los administradores de sistemas de pago de bajo valor que vinculen a entidades administradoras de pasarelas de pago o establecimientos de comercio que realizan las actividades señaladas en el subnumeral 2.2.10. de este Capítulo, deben cumplir, como mínimo, con los siguientes requerimientos:

2.3.8.1. Incluir en los contratos que celebren con dichos establecimientos de comercio o entidades administradoras de pasarelas de pago:

2.3.8.1.1. La obligación por parte de los establecimientos de comercio o entidades administradoras de pasarelas de pago de contar, mantener y entregar la certificación PCI-DDS emitida por una entidad que ostente la categoría QSA (Qualified Security Assessor).

2.3.8.1.2. La obligación por parte de los establecimientos de comercio o entidades administradoras de pasarelas de pago de contar con una política de tratamiento y protección de datos personales de los consumidores, de acuerdo con lo dispuesto en la Ley 1581 de 2012 y en la Ley 1266 de 2008, en lo que resulte pertinente.

2.3.8.1.3. La obligación por parte de los establecimientos de comercio o entidades administradoras de pasarelas de pago de contar con políticas y procedimientos relacionados con la prevención y el control del riesgo de lavado de activos y financiación del terrorismo.

2.3.8.1.4. La obligación por parte de los establecimientos de comercio o entidades administradoras de pasarelas de pago de adelantar campañas informativas sobre las medidas de seguridad que deben adoptar los compradores y vendedores para la realización de operaciones de comercio electrónico.

2.3.8.1.5. La obligación por parte de los establecimientos de comercio o entidades administradoras de pasarelas de pago de informar al consumidor financiero sobre la manera como se realiza el procedimiento de pago.

2.3.8.2. Verificar, al menos una vez al año, la vigencia de la certificación PCI-DSS a que hace referencia el subnumeral 2.3.8.1.1. del presente Capítulo.

**2.3.9 Requerimientos mínimos para la implementación y uso de biometría como factor de autenticación electrónica.**

**En aquellos eventos en que las entidades usen biometría como factor de autenticación electrónica, deben realizar el proceso de verificación de la identidad del cliente contra las bases de datos de la Registraduría Nacional del Estado Civil, los operadores de servicios ciudadanos digitales o de identidad digital autorizados, o contra sus propias bases de datos.**

**Las entidades deben establecer mecanismos alternativos que permitan completar los procesos de autenticación, cuando por razones médicas o físicas el cliente no pueda hacer uso de la biometría.**

**En aquellos eventos en que se utilicen bases de datos propias las entidades deben:**

**2.3.9.1. Almacenar las plantillas biométricas utilizando sistemas de tokenización o algoritmos de cifrado fuertes como AES256, RSA, 3DES o superiores.**

**2.3.9.2. Abstenerse de almacenar muestras biométricas que hayan sido tomadas con el propósito de realizar procesos de autenticación, salvo que se cuente con la autorización explicita referida en el literal a del artículo 6 de la Ley 1581 de 2012 o aquellas normas que lo reglamenten, modifiquen o adicionen y siempre que sean necesarias en la ejecución de programas de inclusión financiera en sectores apartados del territorio nacional. En todo caso, el almacenamiento debe realizarse bajo estándares en materia de seguridad de datos biométricos, tales como ISO 24741:2007 y 24745:2011.**

**2.3.9.3. Almacenar la información demográfica del cliente de manera separada de las plantillas biométricas, relacionándolas entre sí por medio de códigos generados por algoritmos matemáticos que no sean fácilmente descifrados.**

**2.3.9.4. En la implementación de factores biométricos se deben contemplar mecanismos de prueba de vida para fortalecer la confiabilidad y seguridad del sistema tales como: i) medición de propiedades fisiológicas del individuo, ii) identificación de respuestas de comportamiento humano o iii) protocolos de desafío-respuesta.**

**2.3.9.5. Establecer controles en la captura inicial de las muestras biométricas de los clientes que aseguren que la información se obtenga directamente del titular del dato.**

**2.3.9.6. Realizar una adecuada gestión de los riesgos asociados, verificar regularmente la efectividad de los controles implementados y dar cumplimiento a las normas vigentes en materia de protección de datos y habeas data.**

**2.3.10. Domiciliación**

**2.3.10.1. Las entidades deben establecer procedimientos que incentiven la domiciliación de los pagos y adelantar campañas para dar a conocer este servicio.**