PARTE I
INSTRUCCIONES GENERALES APLICABLES A LAS ENTIDADES VIGILADAS

TÍTULO II
PRESTACIÓN DE LOS SERVICIOS FINANCIEROS

CAPÍTULO I: CANALES, MEDIOS, SEGURIDAD Y CALIDAD EN EL MANEJO DE INFORMACIÓN EN LA PRESTACIÓN DE SERVICIOS FINANCIEROS

1. CANALES DE PRESTACIÓN DE SERVICIOS

1.1. Oficinas

Para efectos de lo dispuesto en el art. 92 del EOSF la apertura y cierre de oficinas de las entidades vigiladas por la SFC debe obedecer al conocimiento integral que los directores y administradores tengan de los mercados potenciales, de la situación de competencia en las zonas correspondientes, de la capacidad operativa de la respectiva institución y de la incidencia que tales decisiones tienen sobre su estructura económica y financiera, conocimiento éste que debe fundamentarse en estudios técnicos de factibilidad.

Las determinaciones que se adopten están bajo la responsabilidad de los administradores de las entidades en desarrollo de las políticas que sobre la materia establezca cada una de ellas y deben consultar el interés de la comunidad.

El cierre y traslado de oficinas debe ser informado a los clientes, a través de los canales habitualmente utilizados para la comunicación con estos y con una antelación no inferior a 30 días calendario. Se debe indicar expresamente los mecanismos mediante los cuales los consumidores podrán continuar accediendo a los servicios y trámites que realizaban en la oficina objeto de cierre o traslado. Con la misma antelación se informará al público en general, a través de cualquier medio publicitario.

1.1.1. Naturaleza de las oficinas

De conformidad con lo establecido en los arts. 263 y 264 del C.Cio, las oficinas de las instituciones vigiladas por la SFC sólo pueden tener la calidad de sucursales o agencias, en los términos de las disposiciones mencionadas.
xz
En consecuencia, cuando se pretenda abrir oficinas que tengan por objeto la prestación de servicios restringidos, la naturaleza de la correspondiente oficina debe ajustarse a alguna de las categorías citadas, sin perjuicio de que puedan tales oficinas ofrecer sus servicios de manera transitoria y temporal mediante el traslado de recursos humanos o técnicos para la prestación de sus servicios por fuera del local de las mismas, caso en el cual debe informarse previamente a la SFC, indicando el tipo de servicio que se ofrecerá, la oficina responsable de las operaciones que se realicen y el período en el cual se operará a través de esta modalidad.

1.2. Corresponsales

De conformidad con lo previsto en el artículo 2.36.9.1.1 del Decreto 2555 de 2010 las entidades allí señaladas podrán prestar a través de corresponsales los servicios referidos en los artículos 2.36.9.1.4 al 2.36.9.1.9 y el 2.36.9.1.17..
Se entiende por i) corresponsal físico aquel que presta sus servicios en las instalaciones físicas fijas en las cuales desarrolla su actividad económica, ii) corresponsal móvil aquel que presta servicios de manera ambulante, en nombre de la entidad financiera, utilizando dispositivos móviles conectados a ella en línea o fuera de línea y iii) corresponsal digital lo establecido en el artículo 2.36.9.1.21 del Decreto 2555 de 2010.

Un mismo corresponsal podrá prestar los servicios de la entidad financiera mediante una o varias de las modalidades definidas en el párrafo anterior.

1.2.1. Servicios que se pueden prestar a través de corresponsales

1.2.1.1. Establecimientos de crédito

Los establecimientos de crédito pueden prestar, por medio de corresponsales los servicios señalados en el artículo 2.36.9.1.4 del Decreto 2555 de 2010..

1.2.1.2. Sociedades comisionistas de bolsas de valores

Las sociedades comisionistas de bolsas de valores pueden prestar, por medio de corresponsales, los servicios señalados en el artículo 2.36.9.1.5 del Decreto 2555 de 2010.
1.2.1.3. Intermediarios del Mercado Cambiario - IMC

Los intermediarios del mercado cambiario pueden prestar, por medio de corresponsales, los servicios señalados en el artículo 2.36.9.1.7 del Decreto 2555 de 2010.
1.2.1.4. Sociedades administradoras de fondos de inversión colectiva

Las entidades autorizadas para administrar fondos de inversión colectiva pueden prestar, por medio de corresponsales, los servicios señalados en el artículo 2.36.9.1.6 del Decreto 2555 de 2010.
1.2.1.5. Sociedades administradoras de fondos de pensiones

Las entidades autorizadas para administrar fondos de pensiones pueden prestar, por medio de corresponsales, los servicios señalados en el artículo 2.36.9.1.8 del Decreto 2555 de 2010.

1.2.1.6. Sociedades fiduciarias

Las sociedades fiduciarias pueden prestar, por medio de corresponsales, los servicios señalados en el artículo 2.36.9.1.9 del Decreto 2555 de 2010.

1.2.1.7. Entidades aseguradoras

De acuerdo con lo establecido en los art. 2.36.9.1.17 y 2.36.9.1.18 del Decreto 2555 de 2010, las entidades aseguradoras, en desarrollo de su actividad, pueden prestar por medio de corresponsales uno o varios de los siguientes servicios:

1.2.1.7.1. Comercialización de las pólizas que cumplan con las condiciones de universalidad, sencillez, estandarización y comercialización masiva definidas en el art. 2.31.2.2.1 del Decreto 2555 de 2010 y que estén autorizadas para comercializarse por medio de corresponsales de acuerdo con el artículo 2.36.9.1.18 del referido Decreto.

1.2.1.7.2. Recaudo de primas y pago de indemnizaciones de cualquier ramo de seguros, así como la entrega de los soportes o comprobantes respectivos, lo cual en ningún caso implica que los corresponsales tomen la decisión de pago del siniestro. En ese sentido, se entienden autorizadas todas aquellas operaciones de recaudo, recepción, pago, transferencia y entrega de dinero. La entidad aseguradora debe definir con base en criterios técnicos, a partir de qué montos de indemnización el corresponsal deberá remitir al beneficiario a su sucursal más cercana con el fin de garantizar el pago de manera expedita.

1.2.1.7.3. Entrega y recepción de **solicitudes de seguros** y **sus** anexos, condiciones generales, particulares o extractos, certificaciones, documentos necesarios para la reclamación del siniestro, documentos informativos, informes, boletines y, en general, toda aquella información relacionada **con cualquier ramo de seguros.**

1.2.1.7.4. Entrega y recepción de solicitudes, documentos, informes, boletines, certificados y toda aquella información de los seguros comercializados a través del corresponsal.

1.2.2. Disposiciones generales para la prestación de servicios de las entidades vigiladas a través de sus corresponsales

1.2.2.1. Administración de los riesgos implícitos a la prestación de servicios a través de corresponsales.

1.2.2.1.1. Administración del riesgo **operacional**.

Las entidades vigiladas autorizadas para prestar sus servicios a través de corresponsales deben ajustar su gestión del riesgo operacional del Sistema Integral de Administración de Riesgos (SIAR) en todo aquello que resulte pertinente para la adecuada administración de ese riesgo. Especialmente se deben contemplar los siguientes aspectos:
negocio, planes de contingencia, **así como el recurso humano requerido**.

1.2.2.1.1.2. Complementar y/o ajustar sus políticas, procedimientos y mecanismos de control interno, con el fin de adaptarlos a las condiciones propias de la prestación de sus servicios a través de corresponsales.

1.2.2.1.1.3. Adoptar políticas y establecer procedimientos para la selección, vinculación, capacitación, acompañamiento, **monitoreo** y desvinculación de los corresponsales contratados para la prestación de los servicios autorizados. Dichas políticas deben ser aprobadas por la junta directiva u órgano que haga sus veces.

1.2.2.1.2. Condiciones operativas para la prestación de servicios a través de corresponsales

Con el fin de garantizar que la información de las operaciones realizadas a través de corresponsales se ejecute en condiciones de seguridad y calidad, las entidades vigiladas autorizadas para prestar sus servicios a través de corresponsales deben cumplir como mínimo los siguientes requerimientos, en relación con los medios tecnológicos **(hardware y software)** que utilicen para tal efecto:

1.2.2.1.2.1. Realizar las operaciones en línea y en tiempo real.

Por regla general las operaciones que se realicen a través de corresponsales deben ejecutarse en línea y en tiempo real.

No obstante, la prestación de servicios de pago, recaudo, envío de giro, depósitos en efectivo y cualquier otra relacionada con la recepción de recursos, independientemente de su denominación, podrán efectuarse fuera de línea, de manera excepcional, siempre que las mismas sean realizadas a través de un corresponsal móvil, en zonas con baja o limitada cobertura de redes de comunicación, para lo cual la entidad deberá asegurar que tales operaciones se registren y reflejen en los sistemas de la entidad a más tardar al final del día en que se entregan los recursos por parte del consumidor financiero.

En todo caso, es responsabilidad de cada entidad vigilada establecer mecanismos para garantizar la oportunidad en la transmisión de la documentación y/o información, y gestionar los riesgos operacionales asociados a esta modalidad.

1.2.2.1.2.2. Contar con mecanismos de identificación que permitan verificar que se trata de un **medio tecnológico** autorizad**o** para prestar los servicios a través de los corresponsales.

1.2.2.1.2.3. Disponer de mecanismos y/o procedimientos que impidan la captura, almacenamiento, procesamiento, visualización o transmisión de la información de las operaciones realizadas, para fines diferentes a los autorizados a las entidades vigiladas a través de los corresponsales.

1.2.2.1.2.4. Transmitir la información acerca de las operaciones realizadas, desde **un medio tecnológico** hasta la plataforma tecnológica de la entidad vigilada utilizando mecanismos de cifrado fuerte de conformidad con lo señalado en el subnumeral 2.3.4.1.5. del presente Capítulo.

1.2.2.1.2.5. Generar automáticamente el soporte de cada operación para ser entregado al cliente. En consecuencia, ante la falta de insumos o fallas técnicas que impidan la expedición del soporte, no puede prestarse ningún servicio a través del corresponsal. **Los soportes de las operaciones que se realicen fuera de línea deberán contar con mecanismos que garanticen el no repudio de las operaciones por parte de la entidad financiera.**

1.2.2.1.2.6. Se deben establecer procedimientos para informar a los clientes aquellos casos en los que las operaciones no sean exitosas.

1.2.2.1.2.7. Permitir su manejo bajo diferentes perfiles de usuario para efectos de su administración, mantenimiento y operación.

1.2.2.1.2.8. Garantizar que **l**os medios tecnológicos utilizados por los corresponsales para la realización de las operaciones cumplen los principios de atomicidad, consistencia, aislamiento y durabilidad, teniendo en cuenta las siguientes definiciones:

1.2.2.1.2.8.1. Atomicidad: Propiedad que asegura que una operación es indivisible y, por lo tanto, ante un fallo del sistema, no existe la posibilidad de que se ejecute sólo una parte.

1.2.2.1.2.8.2. Consistencia: Propiedad que asegura que únicamente se ejecutan aquellas operaciones que no van a romper las reglas y directrices de integridad de la base de datos.

1.2.2.1.2.8.3. Aislamiento: Propiedad que asegura que una transacción es una unidad de aislamiento, permitiendo que transacciones concurrentes se comporten como si cada una fuera la única transacción que se ejecuta en el sistema. Esto asegura que la realización de dos transacciones sobre la misma información sea independiente.

1.2.2.1.2.8.4. Durabilidad: Propiedad que asegura que una vez realizada la operación ésta persistirá y no se podrá deshacer aunque falle el sistema. Cuando una transacción termina de ejecutarse, toda la información debe grabarse en algún medio de almacenamiento, en donde se asegure que las actualizaciones no se perderán.

1.2.2.1.2.9. Disponer de centros de administración y monitoreo de **l**os medios tecnológicos utilizados por sus corresponsales.

1.2.2.1.2.10. Contar con los medios necesarios para brindar la atención y soporte requeridos por los corresponsales para la debida prestación de sus servicios.

1.2.2.1.2.11. Disponer de un registro detallado de todos los eventos (exitosos y fallidos) realizados **a través de** los medios tecnológicos utilizados por sus corresponsales.

1.2.2.1.2.12. Contar con políticas y procedimientos para el alistamiento, transporte, instalación, mantenimiento y administración de los medios tecnológicos **usados por los** corresponsales, así como para el retiro del servicio de los mismos.

1.2.2.1.2.13. Operar con sistemas de información que permitan realizar las operaciones bajo condiciones de seguridad, calidad y no repudio por parte del corresponsal.

1.2.2.1.2.14. Adoptar las medidas necesarias encaminadas a impedir que el corresponsal tenga acceso directo a la información de **los** clientes y de sus productos, salvo aquella que sea necesaria para el cumplimiento de sus obligaciones como corresponsal.

1.2.2.1.2.15. Contemplar una fase de acompañamiento por parte de la entidad, al inicio de la operación de cada corresponsal, así como la disposición de los medios que le suministren el soporte necesario para la prestación de los servicios convenidos.

1.2.2.1.2.16. Contar con mecanismos **fuertes** de autenticación para la realización de operaciones monetarias que impliquen el retiro de efectivo, transferencias de fondos, recepción de giros y desembolsos, así como la consulta de saldos, la expedición de extractos y cualquier otra operación no monetaria, autorizada para ser realizada a través de corresponsales, que conlleve a la consulta de información confidencial de los consumidores financieros.

Las consultas y/o pagos relacionados con el valor de cuotas de créditos sólo requieren un factor de autenticación.

En el caso de operaciones **efectuadas** desde la banca móvil, **el mecanismo fuerte de** autenticación se debe realizar en el origen de la transacción.

1.2.2.1.3. Condiciones de idoneidad moral, infraestructura física, técnica y de recursos humanos de los corresponsales

Las entidades vigiladas deben examinar y evaluar la idoneidad moral del corresponsal y son los directos responsables de la prestación del servicio a través de éstos. Por lo tanto, deben instruir claramente al corresponsal acerca de los lineamientos que le permitan mantener una adecuada infraestructura, técnica y de recursos humanos. Adicionalmente, deben velar porque los corresponsales que ostenten la calidad de persona natural, o sus representantes legales y administradores en general, tratándose de personas jurídicas, no estén incursos en los supuestos a que se refiere el inciso tercero del numeral 5 del art. 53 del EOSF.

Para efectos de establecer la idoneidad moral del corresponsal, cuando se trate de personas naturales, o de sus representantes legales y revisores fiscales cuando se trate de personas jurídicas, las entidades vigiladas deben realizar las averiguaciones pertinentes, tales como: la solicitud de antecedentes penales, medidas o sanciones administrativas impuestas por las diferentes Superintendencias por conductas asociadas al desarrollo o participación en la actividad financiera, bursátil y/o aseguradora, sin contar con la debida autorización estatal.

1.2.2.2. Reglas relativas a la administración del riesgo de lavado de activos y financiación del terrorismo

Las entidades vigiladas autorizadas para prestar sus servicios a través de corresponsales deben dar cumplimiento a las disposiciones del Capítulo IV, Título IV de la Parte I de la presente Circular, en lo que resulte aplicable.

Dentro del sistema de administración del riesgo de lavado de activos y financiación del terrorismo (SARLAFT) se deben definir los deberes del corresponsal, dentro de los cuales se puede incluir la posibilidad de brindar soporte a la entidad en las gestiones necesarias para el conocimiento del cliente.

1.2.3. Contratos con los corresponsales

Sin perjuicio de lo dispuesto en el artículo 2.36.9.1.15 del Decreto 2555 de 2010, las entidades vigiladas deben mantener a disposición de la SFC la siguiente información y documentos relacionados con la prestación de servicios a través de corresponsales:

1.2.3.1. Descripción de las características técnicas de **los medios tecnológicos** con las cuales operará.

1.2.3.2. Infraestructura de comunicaciones que soportará la red de corresponsales.

1.2.3.3. Medidas de seguridad que protegerán la información de las operaciones realizadas.

1.2.3.4. Recursos dispuestos para la operación de los centros de administración, monitoreo y soporte.

1.2.3.5. Descripción del proceso adoptado por la entidad vigilada para la identificación y autenticación del cliente a través del corresponsal.

1.2.3.6. Procedimiento adoptado para el registro y conservación de la información de las operaciones realizadas.

1.2.3.7. Identificación de los riesgos **operacionales** asociados a la prestación del servicio a través del corresponsal y las medidas adoptadas para su mitigación.

1.2.3.8. Para el caso de las entidades aseguradoras, los modelos de las pólizas de seguros que se comercializarán a través de los corresponsales, los cuales deben cumplir con los principios de los seguros de comercialización masiva estipulados en el art. 2.31.2.2.1 del Decreto 2555 de 2010 y con las instrucciones establecidas para la comercialización de seguros a través de corresponsales.

1.2.4. Disposiciones relacionadas con la prestación de servicios de varias entidades vigiladas a través de un mismo corresponsal.

En el evento en que un mismo corresponsal preste sus servicios a varias entidades vigiladas, de conformidad con lo establecido en el numeral 14 del artículo 2.36.9.1.11 del Decreto 2555 de 2010, y se trate de un corresponsal digital, tanto la entidad como el corresponsal deben asegurar que en la interfaz de las aplicaciones (Apps), plataformas o medios tecnológicos, se identifique de forma clara y expresa la entidad que presta cada uno de los servicios y, adicionalmente, se asegure la debida diferenciación de los servicios prestados por cada una de ellas.

1.2.5. Reglas para la prestación de los servicios de las entidades aseguradoras a través de corresponsales

1.2.5.1. Las entidades aseguradoras deben garantizar el cumplimiento de las siguientes condiciones para la prestación de los servicios establecidos en el subnumeral 1.2.1.7.1. del presente Capítulo:

1.2.5.1.1. Capacitación.

Las personas naturales que trabajen para los corresponsales de las entidades aseguradoras o presten servicio a los mismos, deben estar capacitadas para la ejecución de las labores relacionadas con la comercialización de pólizas de seguros. Por lo anterior, las entidades aseguradoras deben velar por que dichas personas tengan conocimiento suficiente sobre el proceso de celebración del contrato de seguro y el rol que deben cumplir en cada una de las etapas de dicho proceso, incluyendo la promoción del producto, la recepción de la solicitud de seguro, la realización del mecanismo de comprobación de asegurabilidad, si lo hay, la entrega de todos los documentos que hagan parte del contrato de seguro, el recaudo de la prima y la entrega de los demás documentos que haya dispuesto la entidad aseguradora para informar al consumidor financiero sobre instrucciones que se deben tener en cuenta para la efectividad del seguro (instrucciones en materia de reclamaciones, de mantenimiento del estado del riesgo o de evitar la extensión o propagación del siniestro). El corresponsal también debe estar en capacidad de brindar información sobre los mecanismos habilitados por la entidad aseguradora para la presentación y atención de quejas y reclamos.

Las entidades aseguradoras deben actualizar periódicamente los conocimientos de las personas naturales que trabajen o presten servicio a los corresponsales, especialmente cuando hay modificaciones a los productos de seguro comercializados a través de corresponsales, tales como: el alcance de los amparos, los requisitos de asegurabilidad, así como aspectos procedimentales relacionados con la reclamación.

1.2.5.1.2. Verificación de actividades de los corresponsales

Las entidades aseguradoras deben verificar que los corresponsales realicen las siguientes actividades:

1.2.5.1.2.1. Entrega y explicación al consumidor financiero de la póliza y demás documentos que hacen parte del contrato de seguro al momento de la celebración del contrato.

1.2.5.1.2.2. Entrega de indicaciones que el tomador o asegurado debe tener en cuenta para proteger la validez y eficacia del contrato de seguro.

1.2.5.1.2.3. Indicación de la forma en que el consumidor financiero puede tener acceso al contenido mínimo de información al que hace referencia el art. 9 de la Ley 1328 de 2009.

1.2.5.1.3. Material publicitario de productos o servicios prestados a través del corresponsal.

Las entidades aseguradoras deben dotar a los corresponsales con el material comercial y publicitario idóneo y suficiente que otorgue al consumidor financiero información clara, sencilla y completa sobre los productos de seguro comercializados o los servicios prestados a través de este canal. El material publicitario o informativo también debe incluir las recomendaciones e información adicional que la entidad aseguradora estima pertinente que el consumidor conozca, especialmente en materia de procedimientos relacionados con la reclamación y efectividad del seguro, y las indicaciones de las que trata el subnumeral 1.2.5.1.2.2. de este Capítulo. Adicionalmente, el material publicitario que se utilice debe contener información sobre las obligaciones que debe cumplir el consumidor financiero para que la cobertura de un seguro se mantenga y se haga efectivo el pago de la indemnización en caso de siniestro, si es el caso.

Para el efecto el material publicitario o informativo puede ser redactado en forma didáctica y, en la medida de lo posible, propenderá por otorgar al consumidor financiero un resumen de la normatividad aplicable al contrato de seguro que debe ser tenida en cuenta por el tomador o asegurado.

1.2.5.1.4. Mecanismos de atención a los corresponsales

Las entidades aseguradoras deben contar con mecanismos de atención a sus corresponsales tales como una línea telefónica, acceso a un portal web específico o acceso a un chat especializado, que permitan al corresponsal acceder a la información de los productos y contar con el apoyo de la entidad aseguradora al momento en que se está ofreciendo un producto de seguro, en caso de requerirlo.

1.2.5.1.5. Las entidades deben dotar al corresponsal con los mecanismos necesarios para la transmisión de información y documentos hacia la entidad aseguradora en condiciones de seguridad y calidad. Las entidades aseguradoras deben definir los tiempos máximos para la remisión de información y documentación por parte del corresponsal y demás condiciones para garantizar que la transmisión de la misma sea oportuna.

1.2.5.2. Las entidades aseguradoras deben garantizar el cumplimiento de las siguientes condiciones especiales en relación con los seguros que se comercialicen a través de corresponsales de acuerdo con lo establecido en el subnumeral 1.2.1.7.1. del presente Capítulo:

1.2.5.2.2. Los modelos de pólizas de seguro comercializados a través de corresponsales deben estar a disposición del consumidor financiero a través de este canal y en la página web de la entidad, claramente diferenciados de los modelos de seguros comercializados por otros canales.

1.2.5.2.3. En las pólizas de seguro se debe reflejar, como mínimo, la siguiente información:

1.2.5.2.3.1. El valor o monto asegurado exacto.

1.2.5.2.3.2. El valor de la prima comercial del producto.

1.2.5.2.3.3. Los amparos y exclusiones del contrato de seguro, bajo acápites denominados “Qué cubre este seguro” y “Qué no cubre este seguro”.

En las pólizas de seguro comercializadas a través de corresponsales, la delimitación del riesgo asegurado debe realizarse de manera clara, de tal forma que permita a los consumidores financieros identificar si el riesgo que quieren asegurar se encontraría amparado por la póliza, sin tener que acudir a las exclusiones, límites de cobertura o restricciones de ley. En los seguros que se comercialicen a través de corresponsales no se pueden incluir exclusiones, salvo que se cumpla con los criterios establecidos en el subnumeral 1.2.5.3 de este capítulo.

1.2.5.2.3.4. Indicación de la fecha y hora exacta desde la cual empieza y termina la cobertura.

1.2.5.2.3.5. La identificación del corresponsal a través del cual accede a la información o a través del cual adquiere la póliza.

1.2.5.2.4. En el contrato de seguro adquirido a través de corresponsales no se podrán exigir condiciones previas para el inicio del amparo de la póliza o para la subsistencia de la misma, salvo el pago de la prima correspondiente. De la misma manera, las entidades aseguradoras no pueden modificar unilateralmente un contrato de seguro adquirido mediante este canal, salvo que las modificaciones sean incluidas en beneficio del tomador o beneficiario de la póliza.

1.2.5.2.5. Procedimiento simplificado de reclamación.

De acuerdo con el parágrafo 1 del artículo 2.36.9.1.17 del Decreto 2555 de 2010, los seguros que se comercialicen a través de corresponsales deben tener un procedimiento simplificado de radicación y resolución de reclamación de siniestros. Por lo anterior, la entidad aseguradora debe contar con instancias especiales para la recepción, estudio y respuesta de reclamaciones y que propendan por el establecimiento de plazos de solución de reclamaciones menores al establecido en el art. 1080 del C.Cio.

Las entidades aseguradoras pueden disponer de mecanismos alternativos para la recepción de reclamaciones.

1.2.5.3. Exclusiones aplicables a los seguros comercializados a través de corresponsales.

Las pólizas comercializadas a través de corresponsales únicamente pueden contener exclusiones en alguno de los siguientes casos:

1.2.5.3.1. Cuando no sea posible limitar la cobertura mediante la redacción del amparo.

1.2.5.3.2. Cuando el evento a excluir no pueda identificarse mediante los mecanismos de comprobación de asegurabilidad, de acuerdo con lo indicado en el segundo inciso del subnumeral 1.2.5.4 de este capítulo.

Las exclusiones deben estar redactadas de forma sencilla, clara y precisa. Adicionalmente deben tener un impacto sustancial en el valor de la prima. Las entidades aseguradoras deben tener a disposición de la SFC, un documento actuarial donde se sustente la exclusión y sus efectos en la prima pura de riesgo.

La SFC, en cualquier momento, podrá determinar si las exclusiones incluidas en el modelo de póliza se adecúan a las instrucciones de este capítulo.

1.2.5.4. Mecanismos de comprobación de la asegurabilidad.

En los seguros que se comercialicen a través de corresponsales, las entidades aseguradoras deben implementar mecanismos para identificar el estado del riesgo y la asegurabilidad del consumidor financiero. Para tal efecto, no se pueden realizar preguntas abiertas sobre el estado del riesgo que impliquen declaraciones espontáneas. No 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 deben promover el uso de canales digitales para la prestación de los servicios demandados por los consumidores financieros, los cuales deben contar con condiciones adecuadas de seguridad y calidad para la realización de operaciones. En ningún caso, podrán limitar el uso de los canales tradicionales para aquellos consumidores financieros que prefieran y decidan realizar sus operaciones a través de estos.

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 primero 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.
1.4.1.1.1.4. Los mecanismos que aseguran que la prestación del servicio al menos equipara los estándares de eficiencia, oportunidad y seguridad a los ofrecidos por la entidad usuaria de la red a sus consumidores financieros.
1.4.1.1.1.5. Los mecanismos para mitigar adecuadamente los riesgos asociados a la validación de la identidad de los consumidores financieros y el registro, conservación y seguridad de la información de las operaciones realizadas, garantizando su independencia frente a la información o bases de datos propios del prestador de la red.
1.4.1.1.1.6. Las medidas que se adoptarán para garantizar que los consumidores financieros identifiquen que el usuario de la red es una persona jurídica distinta de la entidad prestadora de la red.
1.4.1.1.1.7. El manejo que la entidad prestadora le dará a los recursos recibidos de los clientes de la entidad usuaria.
1.4.1.1.1.8. Los mecanismos que se adoptarán para capacitar al personal involucrado en la atención al consumidor financiero en virtud del contrato de uso de red.
1.4.1.1.1.9. Los mecanismos habilitados por la entidad usuaria de la red para la atención de quejas y la definición sobre si las mismas pueden canalizarse a través de la entidad prestadora.
1.4.1.1.1.10. El término de duración y las causales de terminación.
1.4.1.1.1.11. Remuneración por el uso de la red, en caso de que así se pacte

1.4.1.1.2. Modificaciones a los contratos de uso de red

Las modificaciones respecto a la información contenida en los subnumerales 1.4.1.1.1.1 a 1.4.1.1.1.7 de este Capítulo deben ser remitidas a la SFC, previamente a su entrada en vigencia entre las partes.

Los contratos objeto de modificación que no deban ser remitidos, deben estar a disposición de la SFC.

1.4.1.1.3. Administración de los conflictos de interés

Las entidades deben identificar los conflictos de interés que puedan surgir en desarrollo del contrato de uso de red así como establecer las medidas que se adoptarán para su manejo, administración y revelación según cada caso e incorporarlos en los respectivos códigos de conducta.

1.4.1.1.4. Identificación

El personal que en desarrollo del contrato de uso de red haga la promoción y gestión de operaciones debe identificarse claramente ante el consumidor financiero y manifestar de manera expresa y sencilla que está actuando en nombre de la entidad usuaria de la red.

Las entidades usuarias de la red deben tomar las medidas necesarias para que el público las identifique como una entidad autónoma, independiente y diferente de la entidad prestadora de la red. Para el efecto, la entidad prestadora de la red debe adoptar los procedimientos y mecanismos, así como realizar las adecuaciones correspondientes, que permitan a los consumidores financieros identificar la entidad usuaria, de acuerdo con las características de cada uno de los distintos canales. Dentro de los mecanismos utilizados debe existir la identificación de manera visible, clara y completa de la razón social o denominación social de la entidad usuaria de la red o la sigla que la identifique de conformidad con sus estatutos sociales, acompañada siempre de la denominación genérica del tipo de entidad.

1.4.1.1.5. Administración de riesgos

Previamente a la comercialización de productos a través del uso de red, las entidades vigiladas deben ajustar sus políticas y procedimientos de administración de riesgos, de tal forma que se garantice una adecuada gestión de los riesgos inherentes a los canales utilizados y a los productos comercializados a través de los mismos. Estas políticas y procedimientos deben permitir el seguimiento y control de los canales utilizados, indicando expresamente las áreas o personas responsables de cada actividad.

1.4.1.1.5.1. Administración del riesgo operacional

En desarrollo del contrato de uso de red, las entidades vigiladas deben cumplir las disposiciones sobre administración del riesgo operacional definidas en el Capítulo XXXI de la CBCF y lo establecido en el numeral 2 de este Capítulo, respecto de los requerimientos mínimos de seguridad y calidad para la realización de operaciones.

Todas las operaciones que se desarrollen con ocasión del contrato deben ejecutarse bajo parámetros que aseguren la prestación del servicio al menos, con los mismos estándares de eficiencia, oportunidad y seguridad a los ofrecidos por la entidad usuaria de la red a sus consumidores financieros.

1.4.1.1.5.2. Administración del riesgo de lavado de activos y financiación del terrorismo

En desarrollo del contrato de uso de red, las entidades vigiladas deben cumplir las disposiciones establecidas en el Capítulo IV del Título IV de la Parte I de la CBJ.

1.4.1.1.6. Capacitación y recursos

Las entidades que comercialicen productos a través del uso de red deben:

1.4.1.1.6.1. Capacitar al personal involucrado en la comercialización de los productos a través del uso de red. Para tal efecto, deben implementar mecanismos verificables que garanticen que el personal conoce:

1.4.1.1.6.1.1. El alcance de sus obligaciones contractuales.
1.4.1.1.6.1.2. Las características del producto comercializado.
1.4.1.1.6.1.3. Los procedimientos de recaudo, atención de solicitudes, pago y demás aspectos relevantes para la comercialización de cada producto.

Con respecto a productos de seguros, las entidades aseguradoras deben velar porque el personal involucrado en la comercialización de los productos a través del uso de red conozca y pueda verificar los requisitos de asegurabilidad conforme a lo establecido en el numeral 1.4.1.1.8.1.2 del presente Capítulo.

1.4.1.1.6.2. Actualizar periódicamente al personal involucrado en la comercialización de los productos, informando modificaciones a los mismos, así como el régimen legal relacionado con los mismos.

1.4.1.1.6.3. Contar con mecanismos, tales como una línea de atención especializada, acceso a un portal web específico o acceso a un chat especializado, que permitan al personal acceder inmediatamente a dicha información y contar con el apoyo comercial de la entidad usuaria, en caso de requerirlo.

1.4.1.1.7. Requisitos de información

1.4.1.1.7.1 Información al consumidor financiero

Las entidades vigiladas deben cumplir las instrucciones específicas para la comercialización mediante el uso de red, establecidas en el Capítulo I, Título III de la Parte I de la CBJ.

1.4.1.1.7.2. Comprobantes de las operaciones

De acuerdo con lo dispuesto en el art. 2.34.1.1.5 Decreto 2555 de 2010, en los comprobantes de las transacciones, que adelanten las entidades prestadoras por cuenta de las entidades usuarias de su red, debe incluirse en forma visible y claramente legible, la siguiente indicación:

(Aquí el nombre de la entidad usuaria de la red) ASUME EXCLUSIVAMENTE LA RESPONSABILIDAD DEL CUMPLIMIENTO DE LAS OBLIGACIONES RELACIONADAS CON EL PRESENTE CONTRATO FRENTE AL CONSUMIDOR FINANCIERO.

Estos comprobantes deben contener por lo menos, la información que identifique con precisión la operación de que se trate, incluyendo como mínimo la fecha, hora y monto de la transacción.

1.4.1.1.7.3. Recepción de quejas y reclamos

La entidad prestadora debe informar a los consumidores financieros, de manera clara y precisa, sobre todos los mecanismos que tienen habilitados los usuarios de la red para la presentación y atención de quejas y reclamos.

La entidad usuaria de la red puede permitir la recepción de quejas y reclamos a través del prestador de la red en virtud del contrato de uso de red. Con el fin de garantizar la oportuna y eficaz atención de las quejas o reclamos del consumidor financiero, tanto la entidad prestadora como la entidad usuaria de la red deben establecer el procedimiento necesario para que las quejas y reclamos sean entregados de manera eficiente y oportuna al usuario de la red. Adicionalmente, tanto el prestador como el usuario de la red deben establecer un mecanismo apropiado para que los consumidores financieros puedan hacer seguimiento a su petición.

1.4.1.1.8. Comercialización de seguros

En virtud de lo dispuesto en la Ley 389 de 1997 y en el art. 2.31.2.2.5 del Decreto 2555 de 2010, las entidades aseguradoras y los intermediarios de seguros vigilados por la SFC pueden ser usuarias de las redes de los establecimientos de crédito, las sociedades de servicios financieros, las sociedades comisionistas de bolsa de valores, las comisionistas independientes de valores, las sociedades administradoras de inversión, las sociedades administradoras de depósitos centralizados de valores y las Sociedades Especializadas en Depósitos y Pagos Electrónicos (SEDPE)**, para lo cual se debe dar cumplimiento a las condiciones establecidas en este Capítulo.**

1.4.1.1.8.1. Requisitos de los seguros comercializados a través del uso de red

Además de lo dispuesto en el art. 2.31.2.2.1 del Decreto 2555 de 2010, para la comercialización de seguros a través del uso de red se debe cumplir con los siguientes requisitos:

1.4.1.1.8.1.1. La entidad aseguradora debe establecer mecanismos para asegurar que el consumidor financiero conozca, previamente a la adquisición del producto, la importancia de declarar sinceramente el estado del riesgo y las sanciones por inexactitud o reticencia, de acuerdo con lo establecido en el art. 1058 del C.Cio.

1.4.1.1.8.1.2. Las entidades aseguradoras deben otorgar herramientas y establecer mecanismos para que las entidades prestadoras puedan verificar que los tomadores y/o los asegurados tengan un interés asegurable que corresponda con la póliza de seguro comercializada a través de este canal y que los consumidores financieros cumplen con los requisitos de asegurabilidad establecidos en el contrato de seguro. Para dar cumplimiento a lo anterior, las partes deben establecer en el contrato de uso de red una cláusula de responsabilidad en donde se fijen las implicaciones de la inobservancia de tal verificación.

1.4.1.1.8.1.3. Las entidades aseguradoras deben cerciorarse que las pólizas de seguros comercializadas a través del uso de red tengan exclusiones y amparos claros, concisos y redactados en un lenguaje que no sea vago ni ambiguo.

1.4.1.1.8.1.4. Las pólizas de seguro que se comercialicen a través de uso de red deben tener un procedimiento simplificado de reclamación de siniestros. Por lo anterior, la entidad aseguradora debe contar con instancias para el trámite y resolución de reclamaciones que propendan por el establecimiento de plazos de solución de reclamaciones menores al establecido en el art. 1080 del C.Cio.

El procedimiento simplificado de radicación y resolución de la reclamación debe ser informado al consumidor financiero al momento de la celebración del contrato de seguro y al asegurado y beneficiario de la póliza de seguro cuando este lo solicite.

1.4.1.1.8.1.5. En línea con lo establecido en el numeral 3 del art. 2.31.2.2.1 del Decreto 2555 de 2010, el clausulado de las pólizas de seguros comercializadas por medio de uso de red no debe ser susceptible de modificación según el sujeto que la adquiera ni pactar condiciones particulares.

1.4.1.1.8.1.6. Dentro de los 15 días hábiles siguientes a la fecha de la celebración del contrato de seguro, las entidades aseguradoras deben entregar en físico o por correo electrónico al tomador la póliza de seguro contentiva del mismo.

1.4.1.1.8.1.7. De acuerdo con el parágrafo 1 del art. 2.31.2.2.2 del Decreto 2555 de 2015, las entidades aseguradoras no pueden exigir condiciones previas para el inicio del amparo de la póliza de seguro o para la subsistencia de la misma. En este sentido, las entidades aseguradoras se deben abstener de exigir cualquier tipo de condición suspensiva para iniciar la cobertura de la póliza de seguro que implique una actividad posterior del tomador o el asegurado.

1.4.1.1.8.1.8. La entidad aseguradora no puede modificar unilateralmente el contrato de seguro, con posterioridad a su celebración, salvo que las modificaciones sean incluidas en beneficio del tomador o beneficiario de la póliza.

1.4.1.1.8.2. Ramos autorizados para su comercialización a través de uso de red

Siempre y cuando el contrato de seguro cumpla lo establecido en el art. 2.31.2.2.1 del Decreto 2555 de 2010 y en el numeral 1.4.1.1.8.1 de este Capítulo, las entidades aseguradoras pueden comercializar, a través del uso de red, los ramos establecidos en el art. 2.31.2.2.2 del citado Decreto **y en el subnumeral 1.2.1.7.1. de este capítulo.**

1.4.1.2. Modalidad de uso de red de oficinas del art. 93 del EOSF.

De acuerdo con la citada disposición, las entidades vigiladas pueden permitir mediante contrato el uso de su red de oficinas por parte de sociedades de servicios financieros, entidades aseguradoras, sociedades comisionistas de bolsa, sociedades de capitalización e intermediarios de seguros, para la promoción y gestión de las operaciones autorizadas a la entidad usuaria de la red y bajo la responsabilidad de esta última.

Corresponde a los prestadores de la red de oficinas, garantizar la existencia de una independencia locativa y operativa que evite cualquier posible confusión de los usuarios del servicio sobre la identidad corporativa de las instituciones.

En la celebración del respectivo contrato, las entidades deben aplicar las disposiciones establecidas en el subnumeral 1.4.1.1.1 del presente Capítulo, siempre que las mismas le resulten aplicables a esta modalidad y tener en cuenta los siguientes requisitos:

1.4.1.2.1. Independencia operativa de los servicios

El personal de las entidades prestadoras no puede participar en las labores de promoción y gestión que las entidades usuarias adelanten en las dependencias del prestador de la red de oficinas. Para efectos de esta modalidad de uso de red de oficinas, las entidades usuarias deben ubicar su propio personal para el desarrollo de las labores de gestión y promoción de sus operaciones.

1.4.1.2.2. Identificación locativa del servicio

Las entidades usuarias de la red deben adoptar las medidas necesarias para que el público las identifique como una persona jurídica autónoma e independiente del prestador de la red.

El área para la ubicación del personal dependiente de las entidades usuarias de la red debe adecuarse de forma tal que se garantice una apropiada independencia de las demás áreas propias de la entidad prestadora. El área debe estar identificada con un aviso que se destaque frente a los demás del local en donde se encuentra ubicada, en el cual se debe indicar de manera clara y completa la razón o denominación social de la entidad usuaria o la sigla que la identifique de conformidad con sus estatutos sociales, acompañada siempre de la denominación genérica del tipo de entidad.

1.4.1.2.3. Normas aplicables a la modalidad de uso de red de oficinas

A la modalidad de uso de red de oficinas del art. 93 del EOSF le aplicará lo establecido en los numerales 1.4.1.1.1 a 1.4.1.1.8 de este Capítulo. No obstante lo anterior, en caso de existir un régimen especial de idoneidad o habilitación de las personas involucradas en la comercialización de productos de la entidad usuaria, dicho régimen prevalecerá sobre lo establecido en este Capítulo

1.4.2. Redes de distribución y promoción de productos de las entidades administradores del Sistema General de Pensiones - SGP, autorizadas mediante el Decreto 1833 de 2016.

Las redes de distribución y la promoción de productos de las entidades administradoras del sistema general de pensiones, cualquiera que sea su modalidad, se encuentran sujetas a las siguientes instrucciones específicas:

1.4.2.1. Destinatarios: De conformidad con el Decreto 1833 de 2016 y en los arts. 2.6.10.2.1 y siguientes del Decreto 2555 de 2010, son destinatarias de las presentes instrucciones, las entidades administradoras del SGP, es decir, que las mismas comprenden tanto a las administradoras del régimen de prima media con prestación definida como a las sociedades administradoras del régimen de ahorro individual con solidaridad.

Igualmente son destinatarios los entes habilitados para la explotación de planes de pensiones y complementarios y las entidades aseguradoras de vida que cuenten con capacidad legal para la explotación de planes alternativos de pensiones, según lo prevé el art. 2.32.1.1.6 del Decreto 2555 de 2010.

1.4.2.2. Exclusividad: Conforme al inciso tercero del art. 2.2.7.2.2 del Decreto 1833 de 2016, la labor de promoción de los vendedores personas naturales, con o sin vinculación laboral, se desarrolla en beneficio de la sociedad administradora del SGP con la cual se hubiere celebrado el respectivo convenio. Es sancionable por la respectiva sociedad, en los términos contractuales, el incumplimiento de esta obligación por parte de los vendedores personas naturales. Sin embargo, en los temas relacionados con promotores, se debe observar las condiciones establecidas en el Decreto 1833 de 2016.

1.4.2.3. Entidades habilitadas para la distribución: La distribución de productos puede efectuarse por conducto de instituciones financieras, intermediarios de seguros -sujetos o no a supervisión permanente- y por entidades distintas a unas y otros, siempre que cuenten con capacidad legal para el ejercicio del comercio. En este caso, es necesaria la autorización previa de la SFC para la celebración de los respectivos convenios.

En los eventos de distribución por conducto de instituciones financieras o intermediarios de seguros no es indispensable la autorización previa impartida por la SFC para la celebración de los respectivos convenios.

1.4.2.4. Convenios: Los convenios que se celebren para la promoción de los servicios que prestan las entidades administradoras del SGP por conducto de las instituciones financieras de que trata el art. 2.2.7.2.1 y siguientes del Decreto 1833 de 2016, están sujetas a las siguientes condiciones:

1.4.2.4.1. Los convenios aludidos, cuyo propósito consiste en la precisión de las condiciones bajo las cuales se realizarán las operaciones de recaudo, pago y traslado de los correspondientes recursos, quedan a disposición de la SFC en las propias instalaciones de la administradora, sin que sea indispensable su remisión a la SFC.

1.4.2.4.2. Los convenios pueden prever actividades a desarrollar respecto de los afiliados y de los trabajadores, tales como promoción, vinculación y, en general, labores de asesoría en los términos del art. 2.6.10.2.3 del Decreto 2555 de 2010, comprendiendo el empleo y diligenciamiento de formularios de vinculación o de pago de aportes. En todo caso, los convenios deben contener, cuando menos, la información a que hace alusión el art. 2.2.7.3.2 del Decreto 1833 de 2016 y su modificación es procedente, entre otros motivos, cuando los costos de los mismos o algunas de sus previsiones afecten a los afiliados.

1.4.2.4.3. En ningún caso los costos que genere el empleo de las instituciones financieras por parte de las sociedades administradoras pueden ser trasladados, directa o indirectamente, a los afiliados, conforme lo señala el inciso 2 del art. 2.2.7.3.1. del Decreto 1833 de 2016.

1.4.2.4.4. Las instituciones financieras deben disponer lo pertinente para la separación de las actividades propias de su objeto respecto de aquellas derivadas de la gestión de los aludidos convenios.

1.4.2.5. Información a los usuarios: En desarrollo de los deberes que se le imponen a los promotores de las sociedades administradoras de pensiones, éstos deben cumplir con las obligaciones contenidas en el Capítulo 2 del Título 10 del Libro 6 de la Parte 2 del Decreto 2555 de 2010, para lo cual deben sujetarse a los parámetros técnicos definidos por cada sociedad administradora, como elementos de referencia para el suministro de información al momento de afiliación. La omisión de esta obligación implica para el promotor la posibilidad de suspensión de la actividad correspondiente, y para la sociedad administradora en cuyo beneficio se haya efectuado la labor de afiliación, la asunción de los respectivos perjuicios sin que ello impida la posibilidad de repetición con que cuenta la sociedad administradora respecto del promotor.

En todo caso, en desarrollo de los objetivos señalados en el art. 325, numeral 1, literales c. y e. del EOSF, en particular la necesidad de garantizar la eficiencia en la prestación del servicio y de prevenir la ocurrencia de situaciones que pueda generar

la pérdida de confianza en el público, esta Superintendencia califica como práctica no autorizada el omitir el suministro de la información oportuna, amplia y suficiente a la cual tiene derecho el afiliado, tanto al momento de su vinculación como durante la vigencia de la misma, con ocasión de las prestaciones debidas por virtud de la mencionada afiliación.

Las sociedades administradoras del SGP, cualquiera sea su modalidad, deben disponer lo pertinente para que fundamentalmente en las áreas de capacitación se difunda con suficiencia la calificación de no autorizada la práctica consistente en no informar adecuadamente a los posibles afiliados, al momento de efectuar la respectiva labor de promoción para su vinculación y, en general, las sanciones que corresponden por el incumplimiento de cualquiera de las obligaciones que les son propias a los promotores.

1.4.2.6. Libertad de selección del asegurador de la renta vitalicia: Las sociedades administradoras y, en su caso, los promotores deben sujetarse a lo previsto en el art. 2.2.6.2.2 del Decreto 1833 de 2016 y las normas que lo desarrollen, cuando se trate de cumplir con la obligación de asesoría acerca de la selección de la entidad aseguradora de vida del contrato de renta vitalicia, cualquiera que sea la modalidad como lo que prevé el literal b. del art. 60 de la Ley 100 de 1993 y el literal j. del art. 14 del Decreto Ley 656 de 1994.

1.4.3. Instrucciones aplicables de manera específica a los promotores de las sociedades administradoras del SGP

1.4.3.1. Remuneración: La remuneración de los promotores de las sociedades administradoras del SGP consiste en el reconocimiento de la comisión que se hubiere pactado por su labor de mediación en la afiliación y, en tal sentido, su reconocimiento no debe estar atado al volumen de afiliaciones sino a una labor idónea y suficiente con la protección al consumidor del SGP.

1.4.3.2. Mecanismos de información sobre promotores: Con sujeción a lo dispuesto en el art. 2.6.10.3.2 del Decreto 2555 de 2010 y atendiendo los principios de la ley estatutaria de protección de datos, 1581 de 2012, las administradoras del SGP pueden disponer mecanismos privados de difusión acerca de los promotores que empleen, con el fin de constatar la existencia de inhabilidades, incompatibilidades, sanciones contractuales precedentes y, en general, cualquier información que resulte relevante para la operatividad de las redes de distribución del mencionado sistema.

1.4.3.3. Prohibiciones aplicables a los promotores: Los promotores deberán dar cumplimiento a las disposiciones previstas en el art. 207 del EOSF, en lo que resulte aplicable

1.4.3.4. Régimen sancionatorio: En virtud de lo previsto en el art. 2.2.7.7.4 y del Decreto 1833 de 2016, el régimen sancionatorio aplicable a los promotores de las sociedades administradoras del SGP es el previsto en el EOSF, por lo cual resultan aplicables las previsiones contenidas en la parte séptima del mencionado Estatuto.

2. SEGURIDAD Y CALIDAD PARA LA REALIZACIÓN DE OPERACIONES

2.1. Alcance

Las instrucciones de que trata el presente numeral deben ser adoptadas por todas las entidades sometidas a la inspección y vigilancia de la SFC, con excepción de Fondo de Garantías de Instituciones Financieras -FOGAFÍN-., Fondo de Garantías de Entidades Cooperativas -FOGACOOP-, Fondo Nacional de Garantías-FNG-, Fondo Financiero de Proyectos de Desarrollo-FONADE-, los Almacenes Generales de Depósito, los Fondos de Garantía que se constituyan en el mercado de valores, los Fondos Mutuos de Inversión, 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 numeral, citadas en el párrafo anterior, deben dar cumplimiento a los criterios de seguridad y calidad de la información, establecidos en los subnumerales 2.3.1. y 2.3.2. subsiguientes.

La obligación relacionada con la elaboración del perfil de las costumbres transaccionales de cada uno de sus clientes debe ser **cumplida** únicamente por los establecimientos de crédito, sin perjuicio de que las demás entidades, cuando lo consideren conveniente, **la** pongan en práctica.

El subnumeral correspondiente al análisis de vulnerabilidades debe ser aplicado únicamente por los establecimientos de crédito, los administradores de sistemas de pago de bajo valor**, las sociedades especializadas en depósitos y pagos electrónicos y las entidades vigiladas que permitan la ejecución de órdenes electrónicas para la transferencia de fondos, la compra, venta o transferencia de títulos valores y la emisión de pólizas de seguros, por sistemas de acceso remoto para clientes, Internet o dispositivos móviles,** sin perjuicio de que las demás entidades, cuando lo consideren conveniente, pongan en práctica las instrucciones allí contenidas.

Las entidades vigiladas que presten sus servicios a través de corresponsales deben sujetarse, para el uso de este canal de distribución, a las instrucciones contenidas en el subnumeral 1.2. del presente Capítulo.

En todo caso las entidades vigiladas destinatarias de las instrucciones aquí contenidas, deben implementar los requerimientos exigidos atendiendo la naturaleza, objeto social y demás características particulares de su actividad.

Las entidades vigiladas deben incluir en sus políticas y procedimientos relativos a la administración de la información, las siguientes definiciones, criterios y requerimientos mínimos relativos a seguridad y calidad de la información que se maneja a través de canales e instrumentos para la realización de operaciones.

2.2. Definiciones aplicables

2.2.1. 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.

2.2.2. Cifrado fuerte: Técnicas de codificación para protección de la información que utilizan algoritmos reconocidos internacionalmente, que se encuentren vigentes y que sus tamaños de llave no hayan sido vulnerados.

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. Participante no vigilado: Se refiere a quien haya sido autorizado por una Entidad Administradora de Sistemas de Pago de Bajo Valor (EASPBV) para tramitar órdenes de pago y de transferencia de fondos a través de su sistema y que no sea una entidad vigilada por la SFC, de conformidad con el numeral 16 del artículo 2.17.1.1.1 del Decreto 2555 de 2010).

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 **operación**, generado por software en tiempo real).

Los códigos QR pueden ser adaptados para **operaciones monetarias y no monetarias.**

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.

2.3.3.1.11. 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.

2.3.3.1.12. 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.

2.3.3.1.13. 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.

2.3.3.1.14. 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 deben establecer los procedimientos y controles para el alistamiento, transporte, instalación y mantenimiento de los dispositivos usados en los canales de distribución de servicios.

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

2.3.3.1.16. Sincronizar todos los relojes de los sistemas de información de la entidad involucrados en los canales de distribución. Se debe tener como referencia la hora oficial suministrada por la autoridad encargada de suministrar la hora legal, de conformidad con las normas aplicables.

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

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

2.3.3.1.19. Incluir en el informe de gestión a que se refiere el art. 47 de la Ley 222 de 1995 –modificado por el art. 1 de la Ley 603 de 2000-, un análisis sobre el cumplimiento de las obligaciones enumeradas en la presente Circular.

2.3.3.1.20. 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.

2.3.3.1.21. Los establecimientos de crédito deben adoptar mecanismos que le permitan atender las operaciones de los consumidores financieros, por los canales que resulten necesarios y por las cuantías que determine razonables, para garantizar un nivel mínimo de prestación de sus servicios a los consumidores financieros, cuando la entidad opere fuera de línea.

2.3.3.1.22. Los establecimientos de crédito deben enviar trimestralmente a la SFC, a la dirección de correo riesgooperativo@superfinanciera.gov.co, un informe sobre la disponibilidad mensual de cada uno de los canales por medio de los cuales presta sus servicios en el que se incluya el detalle de la metodología utilizada para el cálculo de la disponibilidad. Se entiende por disponibilidad el porcentaje de tiempo que durante el mes el canal estuvo habilitado para la prestación del servicio.

2.3.3.1.23. Las entidades vigiladas deben informar a la SFC a la dirección de correo riesgooperativo@superfinanciera.gov.co, los eventos que afecten de manera significativa la confidencialidad, integridad o disponibilidad de la información manejada en los sistemas que soportan los canales de atención al cliente, haciendo una breve descripción del incidente y su impacto. Los incidentes se deben reportar tan pronto se presenten. Así mismo, deben remitir la información de la que trata el subnumeral 3.5.1. del Capítulo I del Título III de la Parte I de la CBJ.

2.3.3.1.24. Las bolsas de valores, bolsas de bienes y productos agropecuarios, agroindustriales o de otros commodities, los depósitos centralizados de valores, las cámaras de riesgo central de contraparte, los sistemas de compensación y liquidación de valores, los sistemas de compensación y liquidación de divisas, los proveedores de precios para valoración, los administradores de sistemas de negociación de valores y/o registro de operaciones sobre valores, los administradores de sistemas de negociación de divisas y/o registro de operaciones sobre divisas, y las sociedades de financiación colaborativa deben reportar a la SFC a la dirección de correo riesgooperativo@superfinanciera.gov.co, los siguientes eventos:

2.3.3.1.24.1. Fallas en los sistemas administrados que afecten y/o tengan el potencial de afectar la prestación de los servicios y/o que generen errores o falta de oportunidad en la información suministrada al mercado y/o al público en general. Dicha información se debe reportar a más tardar al día hábil siguiente y debe contener una breve descripción del evento o incidente y de la afectación.

2.3.3.1.24.2. La descripción de las pruebas de contingencia y/o continuidad realizadas a los sistemas que implementen o no la participación de los afiliados o usuarios y que tengan el potencial de generar afectación en la prestación de los servicios. Esta información se debe reportar el día hábil anterior al inicio de las pruebas.

2.3.3.1.24.3. Actualizaciones y/o modificaciones técnicas o tecnológicas que tengan el potencial de generar interrupciones en la prestación de los servicios o en la correcta y oportuna generación de información. Esta información se debe reportar por lo menos con ocho (8) días calendario de antelación y en ella se deben especificar los servicios que se podrían ver afectados y los medios alternos que se utilizarán para dar continuidad a la operación en condiciones de normalidad.

Cuando no sea posible reportar la información respecto de las actualizaciones y/o modificaciones técnicas o tecnológicas con la antelación de ocho (8) días a la que se refiere el inciso anterior, esta información se debe reportar a más tardar al día hábil siguiente de la realización de la actualización y/o modificación, otorgando las explicaciones suficientes sobre la razón por la cual el reporte se está realizando en un término inferior.

2.3.3.1.24.4. Proyectos relativos a nuevos servicios o productos y/o renovaciones estructurales de la plataforma tecnológica que tengan el potencial de generar impactos en los servicios e información suministrada al mercado. Esta información se debe reportar en la fecha de inicio de la implementación del proyecto y debe contener el cronograma de actividades, en donde se incluyan, entre otros, las fechas previstas para la realización de las pruebas o ejercicios, capacitaciones al mercado, ajustes reglamentarios y entrada en producción.

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.

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.

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, software de propósito específico, o una combinación de los anteriores. 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.

Adicionalmente, contar con mecanismos que permitan reversar el cobro realizado a consumidores financieros por operaciones fallidas en cajeros automáticos. Para estos efectos se entiende por operaciones fallidas cuando el consumidor financiero no recibe el servicio que demandó por cualquier razón. De igual forma debe informar al consumidor financiero, por cualquier medio expedito, que la entidad procederá a realizar la reversión del cobro, la cual deberá realizarse a más tardar dentro de los 2 días hábiles (en el caso de operaciones realizadas en territorio nacional) y 5 días hábiles (en el caso de operaciones realizadas por fuera del territorio nacional) siguientes a la realización del mismo.

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.

2.3.4.4. Receptores de dinero en efectivo

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

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

2.3.4.4.2. 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.

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

2.3.4.4.4. Los billetes no aceptados no pueden ser retenidos y deben ser retornados inmediatamente al cliente o usuario.

2.3.4.5. POS (incluye PIN Pad)

Deben cumplir, como mínimo, con los siguientes requerimientos:

2.3.4.5.1. La lectura de tarjetas solo debe hacerse a través de la lectora de los datáfonos y los PIN Pad.

2.3.4.5.2. Cumplir el estándar EMV (Europay MasterCard VISA).

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

2.3.4.5.4. 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.

2.3.4.5.5. 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.

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

2.3.4.6. Sistemas de audio respuesta (IVR)

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

2.3.4.6.1. Permitir al cliente confirmar la información suministrada en la realización de la operación monetaria.
2.3.4.6.2. Permitir transferir la llamada a un operador, al menos en los horarios hábiles de atención al público.
2.3.4.6.3. Las entidades que permitan realizar operaciones monetarias por este canal, deben ofrecer a sus clientes mecanismos fuertes de autenticación**.**

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

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

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

2.3.4.7.2. 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.

2.3.4.7.3. 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 debe bloquear cualquier tipo de conexión a red distinta a la usada para la prestación del servicio.

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

2.3.4.7.5. En los equipos de cómputo usados en los centros de atención telefónica no se debe permitir 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 deben ser conservados por lo menos 6 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.

2.3.4.7.6. Las entidades también podrán prestar los servicios del Centro de atención telefónica (Call Center, Contact Center) a través de colaboradores ubicados por fuera de las instalaciones exclusivas a las que hace referencia el subnumeral 2.3.4.7.1, previo el análisis de riesgo y la implementación de las medidas de control para:

- **a. Preservar la confidencialidad, integridad y disponibilidad de la información.**
- **b. Mitigar el riesgo de: i) extracción, almacenamiento o copia de la información manejada y ii) uso de dispositivos o medios de comunicación que no sean suministrados por la entidad para la prestación del servicio.**

c. Impedir: i) el uso o conexión a redes distintas a las autorizadas para la prestación del servicio y ii) que se destinen los dispositivos y medios de comunicación para actividades distintas a la prestación de los servicios por este canal.
d. Fortalecer el monitoreo sobre las operaciones realizadas con productos cuya información haya sido gestionada en estas áreas.

En aquellos eventos en que los equipos de cómputo permitan el envío o recepción de correo electrónico, mensajería instantánea, o cualquier otro servicio que permita el intercambio de información, las entidades deben contar con un sistema de registro de la información enviada y recibida, y conservar dichos registros por un periodo mínimo de 6 meses. En el caso en que la información respectiva sea objeto o soporte de una reclamación, queja o forme parte de un proceso judicial o una actuación extrajudicial, se deberá conservar hasta el momento en que la reclamación o queja se resuelva, o el proceso o actuación finalice.

Para efectos del presente subnumeral, se entiende por colaboradores el personal que preste los servicios del Centro de atención telefónica (Call Center, Contact Center) en cualquiera de las modalidades contratadas por la entidad vigilada para la atención parcial o total de sus consumidores financieros a través de este canal.

2.3.4.8. Sistemas de acceso remoto para clientes (RAS)

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

Las entidades que ofrezcan servicio de acceso remoto para la realización de operaciones monetarias deben 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 debe 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.

2.3.4.9. Internet

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

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

2.3.4.9.2. Realizar como mínimo 2 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, debe realizarse una prueba adicional.

2.3.4.9.3. 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.

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

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

2.3.4.9.6. 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.

2.3.4.9.7. Contar con mecanismos 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.

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

2.3.4.10. 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, debe adelantar el respectivo análisis de riesgos del nuevo canal. Dicho análisis debe ser puesto en conocimiento de la junta directiva y los órganos de control.

La entidad debe remitir a la SFC, con al menos 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:

2.3.4.10.1. Descripción del procedimiento que se adoptará para la prestación del servicio.
2.3.4.10.2. Tecnología que utilizará el nuevo canal.
2.3.4.10.3. Análisis de riesgos y medidas de seguridad y control del nuevo canal.
2.3.4.10.4. Planes de contingencia y continuidad para la operación del canal.
2.3.4.10.5. 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.

2.3.4.11. Banca Móvil

Canal en el cual el dispositivo móvil es utilizado para realizar operaciones bien sea asociando su número de línea al servicio**, o empleando apps (aplicaciones informáticas diseñadas para ser ejecutadas en teléfonos celulares, tabletas y otros dispositivos móviles).**

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

La prestación de servicios a través de banca móvil debe cumplir con los siguientes requerimientos:

2.3.4.11.1. Contar con mecanismos de autenticación de 2 factores para la realización de operaciones monetarias y no monetarias.

2.3.4.11.2. Para operaciones monetarias individuales o que acumuladas mensualmente por cliente superen 52,63 UVT (Unidades de Valor Tributario), implementar mecanismos de cifrado fuerte de extremo a extremo para el envío y recepción de información confidencial de las operaciones realizadas, tal como: clave, número de cuenta, número de tarjeta, etc. Esta información, en ningún caso, puede ser conocida por los proveedores de redes y servicios de telecomunicaciones ni por cualquier otra entidad diferente a la entidad financiera que preste el servicio a través de este canal.

2.3.4.11.3. Cualquier comunicación que se envíe al teléfono móvil como parte del servicio de alertas o notificación de operaciones no requiere ser cifrada, salvo que incluya información confidencial.

2.3.4.11.4. Para las operaciones monetarias individuales o que acumuladas mensualmente por cliente sean inferiores a 52,63 UVT y que no cifren la información de extremo a extremo, la entidad debe adoptar las medidas necesarias para mitigar el riesgo asociado a esta forma de operar, el cual debe considerar los mecanismos de seguridad en donde la información no se encuentre cifrada. La SFC puede suspender el uso del canal cuando se advierta que existen fallas que afecten la seguridad de la información.

2.3.4.11.5. 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, entre otras.

2.3.4.11.6. Los servicios que se presten para la realización de operaciones a través de Internet, en sesiones originadas desde el dispositivo móvil, deben cumplir con los requerimientos establecidos en el subnumeral 2.3.4.9. de Internet.

2.3.4.12. Obligaciones específicas para tarjetas débito y crédito

2.3.4.12.1. 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.

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 52,63 UVT Dichas tarjetas deben 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 52,63 UVT.

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 operaciones monetarias en los términos del subnumeral 2.2.4 del presente Capítulo a través de códigos QR, tales como: pagos, transferencias interbancarias, operaciones de recaudo, débitos automáticos, transferencias inmediatas, transferencias de solicitudes de pago, recaudo en línea, retiro en efectivo o recargas, entre otras,** deben **adoptar** como referencia el estándar internacional EMVCo LLC, **última versión** EMV® QR Code Specification for Payment Systems (EMV QRCPS) Merchant-Presented Mode **or Consumer-Presented Mode**, 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 **operaciones** 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.

En el caso de operaciones no monetarias que se realicen mediante el uso de códigos QR, las entidades vigiladas podrán decidir si adoptan o no la última versión del estándar EMV® QR Code Specification for Payment Systems (EMV QRCPS) Merchant-Presented Mode or Consumer-Presented Mode.

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.

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

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

2.3.5.5. Contar con interfaces 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.

2.3.5.6. 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.

2.3.6. 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, deben cumplir, además de lo establecido en el subnumeral 4.3.1.3.1 del Capítulo XXXI de la CBCF, como mínimo, con los siguientes requerimientos:

2.3.6.2. Incluir en los contratos que se celebren con terceros, por lo menos, los siguientes aspectos:

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 , software de propósito específico, o una combinación de los anteriores, 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 Participantes a las EASPBV

Las EASPBV que vinculen a los Participantes no vigilados a los que se refiere el subnumeral 2.2.10 de este Capítulo, que prestan servicios de aplicación de comercio electrónico para almacenar, procesar y/o transmitir el pago correspondiente a operaciones de venta en línea con tarjetas débito o crédito, deben incluir en los contratos que celebren con estos, la obligación de contar, mantener y entregar la certificación PCI-DSS, emitida por una entidad que ostente la categoría QSA (Qualified Security Assessor), y soportada por el documento AoC ("Attestation of Compliance") correspondiente. Así mismo, las EASPBV deben verificar que la certificación PCI-DSS a que hace referencia el inciso anterior este vigente. Si el participante obligado a contar con la certificación no la mantiene vigente, no podrá continuar prestando los servicios señalados en el inciso anterior.

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.

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 o aquellos que lo modifiquen, sustituyan o adicionen.

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.