**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**

CONTENIDO

1. CANALES DE PRESTACIÓN DE SERVICIOS

1.1. Oficinas

1.2. Corresponsales locales

1.3. Otros canales e instrumentos de prestación de servicios financieros

1.4. Uso de redes

2. SEGURIDAD Y CALIDAD PARA LA REALIZACIÓN DE OPERACIONES

2.1. Alcance

2.2. Definiciones aplicables

2.3. Criterios

**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. O****ficinas

Para efectos de lo dispuesto en el art. 92 del EOSF la apertura, traslado, cierre y conversión de oficinas de las entidades vigiladas por la SFCdebe necesariamente 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.

1.1.1. Régimen de autorización general

Las entidades vigiladas, con excepción de aquellas sometidas al régimen de autorización individual previsto en el numeral 1.1.2 del presente Capítulo, pueden abrir, trasladar o cerrar sus oficinas, sucursales o agencias, sin autorización previa de la SFC, cuando reúnan los siguientes requisitos:

1.1.1.1. Cumplan con las obligaciones establecidas en el Decreto 2150 de 1995, modificado por el Decreto 19 de 2012, y demás disposiciones que lo modifiquen, aclaren o complementen, en especial con las disposiciones contenidas en el art. 46 y siguientes.

1.1.1.2. Cuenten con las seguridades necesarias para la oportuna y correcta prestación del servicio al público.

Prueba del cumplimiento de los requisitos anteriores debe permanecer en la presidencia o en la secretaría general de la entidad, o en el órgano que haga sus veces, a disposición de esta Superintendencia.

Todas las aperturas, traslados o cierres de oficinas, sucursales o agencias deben ser informadas a la SFC con destino a la oficina de registro, a más tardar dentro de los 5 días hábiles siguientes a la inscripción en la Cámara de Comercio de la novedad correspondiente.

1.1.2. Régimen de autorización individual

Tratándose de entidades sometidas a vigilancia especial o que se encuentren adelantando programas de recuperación, saneamiento o adecuación de capital, la SFC determinará, en cada caso, si requieren obtener de manera individual y previa autorización para la apertura, traslado o cierre de sus oficinas.

1.1.2.1. Condiciones de la solicitud: En los eventos en que se haga necesaria la autorización individual antedicha, la entidad interesada debe presentar solicitud escrita que contenga, al menos, la información señalada en la lista de chequeo identificada con el código M-LC-AUT-025, por esta Superintendencia.

1.1.2.2. Información a la SFC con posterioridad a la apertura o el traslado de oficinas: Dentro de los 5 días hábiles siguientes a la apertura o traslado de una oficina, debe informarse a la SFC sobre tal circunstancia y adjuntarse certificación de la Cámara de Comercio correspondiente que acredite el registro respectivo, lo cual debe surtirse dentro del término que al efecto señale esta entidad en el acto de autorización.

En caso de no llevarse a cabo la apertura o traslado de la oficina dentro del término indicado, la entidad debe informar tal hecho igualmente a la SFC solicitando la prórroga del término inicialmente concedido en caso en que aún persista el interés de la entidad en la solicitud inicialmente autorizada.

1.1.3. 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.

En consecuencia, cuando se pretendan 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.

La instalación de cajeros automáticos debe informarse oportunamente a la SFC, debiendo expresarse el lugar de ubicación del cajero que se pretende instalar.

1.1.4. Conversión de oficinas

Toda modificación que se efectúe a la naturaleza jurídica de una oficina en funcionamiento debe ser previamente informada a la SFC, indicándose la nueva dependencia contable o administrativa de la oficina objeto de conversión.

1.1.5. Cierre de oficinas

El cierre de oficinas puede producirse dentro del sistema de autorización general. En consecuencia, los cierres pueden hacerse conforme a la decisión adoptada por el órgano social competente. De esta decisión deben ser informados por escrito y con una antelación no inferior a 30 días calendario todos los clientes de la oficina que se va a cerrar, con indicación expresa de los trámites a seguir respecto de los depósitos y las obligaciones contraídas por cada uno de ellos. Durante el mismo tiempo se informará a través de cualquier medio publicitario al público en general.

## 1.2. Corresponsales locales

Se refiere a las clases de servicios que pueden prestar los establecimientos de crédito, las sociedades administradoras de inversión, las sociedades comisionistas de bolsas de valores, las sociedades administradoras de fondos de pensiones, las sociedades fiduciarias y las sociedades intermediarias del mercado cambiario.

1.2.1. Servicios que se pueden prestar a través de corresponsales

1.2.1.1. Establecimientos de crédito

En desarrollo de lo dispuesto en el art. 2.36.9.1.4 del Decreto 2555 de 2010, los establecimientos de crédito pueden prestar por medio de corresponsales, uno o varios de los siguientes servicios:

1.2.1.1.1. Recaudo, pagos y transferencia de fondos.

1.2.1.1.2. Envío o recepción de giros en moneda legal colombiana dentro del territorio nacional.

1.2.1.1.3. Depósitos y retiros en efectivo y transferencias de fondos que afecten dichos depósitos, incluyendo los depósitos electrónicos.

1.2.1.1.4. Consultas de saldos.

1.2.1.1.5. Expedición y entrega de extractos, documentos e información sobre cualquier tipo de producto.

1.2.1.1.6. Desembolsos y pagos en efectivo por concepto de operaciones activas de crédito, al igual que la activación de productos pre-aprobados de crédito.

1.2.1.1.7. También pueden recibir o entregar recursos en moneda legal colombiana correspondiente a las operaciones de compra y venta de divisas provenientes de operaciones de cambio obligatoriamente canalizables a través del mercado cambiario; y recibir o entregar recursos en moneda legal colombiana correspondiente a la compra y venta de divisas de operaciones de envío o recepción de giros no obligatoriamente canalizables a través del mercado cambiario, siempre y cuando el establecimiento de crédito respectivo ostente la calidad de intermediario del mercado cambiario y con sujeción a las disposiciones del régimen cambiario en lo pertinente.

1.2.1.1.8. La promoción y gestión de las operaciones de otras entidades vigiladas, usuarias de su red de oficinas, en desarrollo de lo dispuesto en el art. 93 del EOSF y en el art. 5 de la Ley 389 de 1997.

1.2.1.1.9. Cualquier otra operación que se enmarque en uno o varios de los servicios consagrados en el art. 2.36.9.1.4 del Decreto 2555 de 2010.

Los corresponsales pueden recolectar y entregar documentación e información relacionada con los servicios señalados, incluyendo aquella relativa a la apertura y cancelación de cuentas, a la realización y cancelación de depósitos, la entrega de los instrumentos que permiten la disposición o manejo de los recursos depositados (tales como tarjetas, entre otros) y la relacionada con solicitudes de crédito, así como promover y publicitar tales servicios.

1.2.1.2. Sociedades comisionistas de bolsas de valores

En desarrollo de lo dispuesto en el art. 2.36.9.1.5 del Decreto 2555 de 2010, las sociedades comisionistas de bolsas de valores, pueden prestar por medio de corresponsales los siguientes servicios:

1.2.1.2.1. La recepción de dinero para o como resultado de operaciones realizadas a través de intermediarios de valores.

1.2.1.2.2. El pago de los dividendos o rendimientos de los títulos administrados por una sociedad comisionista de bolsa de valores, así como de los recursos derivados de la venta de las inversiones.

1.2.1.2.3. La entrega y recepción de las constancias o certificados de los valores que se manejen a través de los depósitos centralizados de valores.

1.2.1.2.4. La recepción de recursos destinados a ser invertidos en un fondo de inversión colectiva, así como su devolución.

1.2.1.2.5. En desarrollo de lo dispuestoen los numerales 5 y 6 del art. 2.36.9.1.5del Decreto 2555 de 2010 también pueden recibir o entregar recursos en moneda legal colombiana correspondiente a las operaciones de compra y venta de divisas provenientes de operaciones de cambio obligatoriamente canalizables a través del mercado cambiario y recibir o entregar recursos en moneda legal colombiana correspondiente a la compra y venta de divisas de operaciones de envío o recepción de giros no obligatoriamente canalizables a través del mercado cambiario, siempre y cuando la sociedad comisionista de bolsa de valores respectiva ostente la calidad de intermediario del mercado cambiario y con sujeción a las disposiciones del régimen cambiario en lo pertinente.

Los corresponsales de sociedades comisionistas de bolsas de valores no pueden prestar ningún tipo de asesoría para la vinculación de clientes ni para la realización de inversiones respecto de clientes ya vinculados con la sociedad comisionista de bolsa de valores. No obstante, podrán recolectar y entregar documentación e información relacionada con los servicios previstos en el presente subnumeral.

1.2.1.3. Intermediarios del Mercado Cambiario - IMC

En desarrollo de lo dispuesto en el art. 2.36.9.1.7 del Decreto 2555 de 2010, los IMC pueden prestar, por medio de corresponsales exclusivamente los siguientes servicios:

1.2.1.3.1. Recibir o entregar recursos en moneda legal colombiana correspondiente a las operaciones de compra y venta de divisas provenientes de operaciones de cambio obligatoriamente canalizables a través del mercado cambiario.

1.2.1.3.2. Recibir o entregar recursos en moneda legal colombiana correspondiente a la compra y venta de divisas de operaciones de envío o recepción de giros no obligatoriamente canalizables a través del mercado cambiario.

Los corresponsales cambiarios no pueden desarrollar operaciones de compra y venta de divisas a nombre o por cuenta del IMC. El corresponsal del IMC sólo está obligado a atender solicitudes de recursos en moneda legal colombiana de operaciones realizadas por el IMC, a que se refiere el presente subnumeral, en la medida en que cuente con recursos suficientes, sin perjuicio de la exigibilidad de las obligaciones a cargo del IMC, las cuales, en todo caso, deben ser atendidas oportunamente, a través de su propia red de oficinas.

1.2.1.4. Sociedades administradoras de fondos de inversión colectiva

Atendiendo lo dispuesto en el art. 2.36.9.1.6 del Decreto 2555 de 2010, las entidades autorizadas para administrar fondos de inversión colectiva, en desarrollo de dicha actividad pueden prestar por medio de corresponsales los siguientes servicios:

1.2.1.4.1. Recaudo, pago y transferencia de dineros asociados a la normal operación de fondos de inversión colectiva.

1.2.1.4.2. Expedición y entrega de extractos.

1.2.1.4.3. Recolección y entrega de documentación e información relacionada con los fondos de inversión colectiva administrados.

Los corresponsales de sociedades administradoras de fondos de inversión colectiva no pueden prestar ningún tipo de asesoría para la vinculación de clientes e inversión en dichos fondos, ni para la realización de inversiones respecto de clientes ya vinculados con la sociedad administradora. No obstante, pueden recolectar y entregar documentación e información relacionada con los servicios previstos en el presente numeral.

1.2.1.5. Sociedades administradoras de fondos de pensiones

En virtud de lo establecido en el art. 2.36.9.1.8 del Decreto 2555 de 2010, las entidades autorizadas para administrar fondos de pensiones, en desarrollo de dicha actividad pueden prestar por medio de corresponsales los siguientes servicios:

1.2.1.5.1. Recaudo y pago de recursos asociados a la vinculación a fondos de pensión voluntaria.

1.2.1.5.2. Recolección y entrega de documentación e información relacionada con la vinculación a fondos de pensión voluntaria.

1.2.1.5.3. Expedición y entrega de extractos de fondos de pensión voluntaria.

Los corresponsales de sociedades administradoras de fondos de pensiones no pueden vincular ni prestar ningún tipo de asesoría para la vinculación de clientes.

1.2.1.6. Sociedades fiduciarias

Según lo establecido en el art. 2.36.9.1.9 del Decreto 2555 de 2010, las sociedades fiduciarias en desarrollo de su actividad pueden prestar por medio de corresponsales los siguientes servicios:

1.2.1.6.1. Recaudo y pago de recursos asociados a las operaciones autorizadas a las sociedades fiduciarias.

1.2.1.6.2. Recolección y entrega de documentación e información relacionada con las operaciones autorizadas a las sociedades fiduciarias.

1.2.1.6.3. Expedición y entrega de extractos.

Los corresponsales de sociedades fiduciarias no pueden vincular ni prestar ningún tipo de asesoría para la vinculación de clientes.

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 operativo.

Las entidades vigiladas autorizadas para prestar sus servicios a través de corresponsales deben ajustar su sistema de administración de riesgo operativo (SARO) en todo aquello que resulte pertinente para la adecuada administración de ese riesgo. Como mínimo se deben contemplar los siguientes aspectos:

1.2.2.1.1.1. Los procesos, procedimientos, planes estratégicos, planes de continuidad del negocio, planes de contingencia.

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 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 las terminales o medios tecnológicos que utilicen para tal efecto:

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

1.2.2.1.2.2. Contar con mecanismos de identificación que permitan verificar que se trata de un equipo autorizado 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 el terminal 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.

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 diferenciados para efectos de su administración, mantenimiento y operación.

1.2.2.1.2.8. Garantizar que las terminales o 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 las terminales o 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 en las terminales o 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 las terminales de sus 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 las cuentas de los clientes de la entidad vigilada, salvo tratándose de aquella información 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 de autenticación de 2 factores 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 originadas desde la banca móvil, la autenticación de 2 factores 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 física, 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 las 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 los representantes legales y revisores fiscales, tratándose de personas jurídicas, las entidades vigiladas deben realizar las averiguaciones pertinentes, tales como 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.

Tratándose de los corresponsales cambiarios de que trata el art. 2.36.9.1.3. del Decreto 2555 de 2010, deben acreditar el cumplimiento de lo dispuesto en el parágrafo del art. 100 de la Ley 1328 de 2009.

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

Las entidades vigiladas deben enviar a la SFC para su aprobación, de forma previa a su celebracióne implementación,los modelos de contratos con los corresponsales en las condiciones de que trata el art. 2.36.9.1.11 del Decreto 2555 de 2010, así como la siguiente información:

1.2.3.1. Descripción de las características técnicas de los terminales 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 operativos asociados a la prestación del servicio a través del corresponsal y las medidas adoptadas para su mitigación.

1.2.3.8. Modificaciones de los contratos.

De conformidad con el art. 2.36.9.1.15 del Decreto 2555 de 2010, esta Superintendencia autoriza de manera general aquellas modificaciones que se relacionen con los siguientes aspectos:

1.2.3.8.1. Establecimiento de límites para la prestación de los servicios, monto por transacción, número de transacciones por cliente o usuario y tipo de transacción.

1.2.3.8.2. La remuneración a favor del corresponsal y a cargo de la entidad que lo contrata para la prestación de sus servicios, y la forma de pago.

1.2.3.8.3. Los horarios de atención al público, los cuales pueden ser acordados libremente entre las partes.

1.2.3.8.4. La asignación del respectivo corresponsal a una agencia, sucursal o dependencia del establecimiento de crédito, sociedad administradora de inversión, sociedad comisionista de bolsa de valores, sociedad administradora de fondos de pensiones, sociedad fiduciaria o IMC, así como los canales y procedimientos que puede emplear el corresponsal para comunicarse con aquellas.

1.2.3.8.5. La indicación de si el corresponsal se encuentra autorizado para emplear el efectivo recibido de los clientes y usuarios del establecimiento de crédito, sociedad administradora de inversión, sociedad comisionista de bolsa de valores, sociedad administradora de fondos de pensiones, sociedad fiduciaria o IMC, para transacciones relacionadas con su propio negocio y, en tal caso, los términos y condiciones en que el efectivo puede emplearse, sin perjuicio de la responsabilidad de la entidad que presta sus servicios a través del corresponsal frente a los clientes y usuarios, y del corresponsal frente a la entidad, por tales recursos.

1.2.3.8.6. La obligación del corresponsal de consignar en una agencia o sucursal de la entidad contratante o de otro establecimiento de crédito el efectivo recibido, con una determinada periodicidad, o si se exceden ciertos límites, la contratación de seguros, la forma de custodia del efectivo en su poder, entre otros.

1.2.3.8.7. Las condiciones bajo las cuales los corresponsales pueden o no utilizar su red de oficinas, agencias, sucursales o franquicias para prestar los servicios autorizados en el presente Capítulo, con indicación expresa de la responsabilidad que asume el establecimiento de crédito, sociedad administradora de inversión, sociedad comisionista de bolsa de valores, sociedad administradora de fondos de pensiones, sociedad fiduciaria o IMC, de verificar de manera directa la idoneidad y la calidad en la prestación de los servicios por parte de su corresponsal

1.2.3.8.8. La descripción técnica de los medios tecnológicos y/o terminales electrónicos situados en las instalaciones del corresponsal y con los que éste cuente para la prestación del servicio, así como la obligación de éste de velar por su debida conservación y custodia.

Sin perjuicio de la autorización general de que trata el presente subnumeral, las anteriores modificaciones deben ser informadas a esta Superintendencia una vez sean acordados entre las partes.

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

En desarrollo de lo dispuesto en el numeral 14 del art. 2.36.9.1.11 del Decreto 2555 de 2010 una persona natural o jurídica puede ser corresponsal de una o varias entidades facultadas para prestar sus servicios a través de corresponsales. En estos casos, se deben establecer los mecanismos que aseguren una adecuada diferenciación de los servicios prestados por cada entidad vigilada, así como la obligación del corresponsal de abstenerse de realizar actos de discriminación o preferencia entre las entidades, o que impliquen competencia desleal entre los mismos.

## 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 a los canales señalados, se reconocen dentro de los instrumentos adecuados en la prestación de estos servicios las tarjetas, debito, crédito, los móviles y las órdenes electrónicas para la transferencia de fondos, 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

## 1.4. Uso de redes

1.4.1. Modalidad prevista en el art. 93 del EOSF

De acuerdo con la citada disposición, las entidades vigiladas pueden permitir mediante contrato remunerado, 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, el deber de garantizar la existencia de una rigurosa independencia tanto locativa como operativa que evite cualquier posible confusión de los usuarios del servicio sobre la identidad corporativa de las instituciones. En tal sentido, las entidades vigiladas deben tener en cuenta las siguientes condiciones:

1.4.1.1. Independencia operativa de los servicios

Los funcionarios de los establecimientos de crédito no pueden participar en las labores de promoción y gestión que las entidades usuarias adelanten en las dependencias del prestador de la red, salvo para el caso de negocios y operaciones de los fondos de inversión colectiva abiertos, evento en el cual debe observarse lo dispuesto para este tipo de productos, en el literal b del art. 2.34.1.1.2 del Decreto 2555 de 2010 y en el art. 5 del Decreto 2239 de 1991.

Para efectos de esta modalidad de uso de red, las entidades usuarias deben ubicar su propio personal en las labores de gestión y promoción de sus operaciones.

1.4.1.2. Identificación locativa del servicio

Las entidades usuarias de la red deben 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 del establecimiento de crédito, así como 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.

1.4.1.3. Comprobantes de las operaciones

En los comprobantes de las operaciones que se realicen en desarrollo del contrato de uso de red, se debe indicar que el prestador de la red actúa bajo la exclusiva responsabilidad de usuario de la misma y que, por lo tanto, no asume obligación alguna relacionada con la ejecución de los negocios celebrados en su nombre.

Para tal efecto, los comprobantes de las operaciones deben incluir en forma destacada y claramente legible, en letra de molde y en negrilla la siguiente leyenda:

ADVERTENCIA: EL(LA) (aquí el nombre de la entidad prestadora de la red) ACTUA BAJO LA EXCLUSIVA RESPONSABILIDAD DE (aquí el nombre de la entidad usuaria) Y, POR LO TANTO, NO ASUME NINGUNA OBLIGACION FRENTE AL CLIENTE RELACIONADA CON LA EJECUCION DEL NEGOCIO QUE DA ORIGEN A ESTA TRANSACCION.

Los comprobantes a que hace referencia este subnumeral deben contener por lo menos, la información que identifique con precisión la operación de que se trate.

1.4.1.4. Contratos sobre fondos de inversión colectiva abiertos

Los contratos que celebren las entidades prestadoras de la red por cuenta de una sociedad fiduciaria o mediante los cuales se efectúe la vinculación de fideicomitentes a un fondo de inversión colectivo abierto, deben tener impreso en la carátula del mismo con caracteres destacados, en letra de molde y en negrilla la siguiente leyenda:

EN LAS OPERACIONES QUE SE REALICEN A TRAVÉS DE LA RED DE OFICINAS DE(L) (LA) (aquí el nombre del establecimiento de crédito), ESTE(A) ACTUA EN NOMBRE Y POR CUENTA DE (aquí el nombre de la Sociedad Fiduciaria) Y NO ASUME RESPONSABILIDAD EN LA GESTIÓN FIDUCIARIA ENCOMENDADA POR EL CLIENTE A ELLA. SUS OBLIGACIONES SE LIMITAN AL CORRECTO CUMPLIMIENTO DE LAS INSTRUCCIONES IMPARTIDAS POR (aquí el nombre de la sociedad fiduciaria) PARA LA PRESTACIÓN DEL SERVICIO DE DICHA RED. SOBRE LOS RECURSOS QUE LAS SOCIEDADES FIDUCIARIAS RECIBEN, DIRECTAMENTE O A TRAVÉS DEL USO DE LAS REDES DE OFICINAS DE ESTABLECIMIENTOS DE CRÉDITO, LA LEY NO CONTEMPLA AMPARO DEL SEGURO DE DEPÓSITO.

1.4.2. Redes de distribución y promoción de productos de las entidades administradores del Sistema General de Pensiones - SGP, autorizadas mediante el Decreto 720 de 1994

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 720 de 1994 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 Decreto 2555 de 2010.

1.4.2.2. Exclusividad: Conforme al inciso tercero del art. 4 del Decreto 720 de 1994, 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 720 de 1994.

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 Decreto 720 de 1994, 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. 9 del Decreto 720 de 1994 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. 8 del Decreto 720 de 1994.

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 Decreto 719 de 1994 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: De conformidad con los art. 17 y 19 del Decreto 720 de 1994, son aplicables a los promotores de las sociedades administradoras del SGP las mismas facultades con que cuenta la SFC respecto de los intermediarios de seguros.

En virtud de tal remisión, les resultan aplicables, entre otras disposiciones, las previstas en el art. 207 del EOSF en particular la contenida en el numeral 3 que prevé como una prohibición la cesión de comisiones a favor del afiliado, el ofrecimiento de beneficios no garantizados o la exageración de los mismos, así como la sugestión tendiente a dañar negocios celebrados por competidores, el hacerse pasar por representante de una entidad sin serlo y, en general, todo acto de competencia desleal.

1.4.3.4. Régimen sancionatorio: En virtud de lo previsto en el art. 21 del Decreto 720 de 1994, 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, los Fondos Ganaderos, las Sociedades Calificadoras de Valores y/o Riesgo, las Oficinas de Representación de Instituciones Financieras y de Reaseguros del Exterior, los Corredores de Seguros y de Reaseguros, los Comisionistas Independientes de Valores, las Sociedades Comisionistas de Bolsas Agropecuarias y los Organismos de Autorregulación.

Sin embargo, las entidades exceptuadas de la aplicación del presente 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 aplicado únicamente por los establecimientos de crédito, sin perjuicio de que las demás entidades, cuando lo consideren conveniente, pongan en práctica las instrucciones allí contenidas.

El subnumeral correspondiente al análisis de vulnerabilidades debe ser aplicado únicamente por los establecimientos de crédito y los administradores de sistemas de pago de bajo valor, sin perjuicio de que las demás entidades, cuando lo consideren conveniente, pongan en práctica las instrucciones allí contenidas.

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, brindando al menos los niveles de seguridad ofrecidos por 3DES o AES.

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

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

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

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

2.2.6.1. Biometría.

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.

## 2.3. 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, 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 Superintendencia de Industria y Comercio.

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.

2.3.3.2. En materia de documentación

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

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

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

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

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

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

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

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

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

2.3.3.2.8. Dejar constancia del cumplimiento de la obligación de informar adecuadamente a los clientes respecto de las medidas de seguridad que deben tener en cuenta para la realización de operaciones por cada canal, así como los procedimientos para el bloqueo, inactivación, reactivación y cancelación de los productos y servicios ofrecidos.

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

La información a que se refieren los subnumerales 2.3.3.2.1., 2.3.3.2.6 y 2.3.3.2.9. debe ser conservada por lo menos por 2 años. En el caso en que la información respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

2.3.4. Requerimientos especiales por tipo de canal

2.3.4.1. En oficinas

La prestación de servicios financieros 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 8 meses o en el caso en que la imagen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

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 8 meses o en el caso en que la imagen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

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

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

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

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

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

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

2.3.4.3. 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 ellos, 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 equiposde 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 8 meses o en el caso en que la información respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

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 monetariasdeben 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 darse 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

Entendido como el canal en el cual el dispositivo móvil es utilizado para realizar operaciones y su número de línea es asociado al servicio.

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

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 2 SMMLV, 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. Dicha información tampoco puede ser almacenada en el teléfono móvil.

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 2 SMMLV 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 haya sido asignada por la entidad vigilada, esta debe ser cambiada por el cliente antes de realizar su primera operación.

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

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

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

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

2.3.4.12.11. Entregar a sus clientes tarjetas débito y/o crédito que manejen internamente mecanismos fuertes de autenticación, siempre que los cupos aprobados superen 2 SMMLV. Dichas 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 SMMLV.

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, como mínimo, con los siguientes requerimientos:

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

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

2.3.6.2.1. Niveles de servicio y operación.

2.3.6.2.2. Acuerdos de confidencialidad sobre la información manejada y sobre las actividades desarrolladas.

2.3.6.2.3. Propiedad de la información.

2.3.6.2.4. Restricciones sobre el software empleado.

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

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

2.3.6.2.7. Procedimientos y controles para la entrega de la información manejada y la destrucción de la misma por parte del tercero una vez finalizado el servicio.

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

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

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

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

2.3.7 Análisis de vulnerabilidades

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

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

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

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

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

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

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