SUPERINTENDENCIA FINANCIERA DE COLOMBIA

CIRCULAR EXTERNA 008 DE 2018

(Junio 05)

Señores

REPRESENTANTES LEGALES Y REVISORES FISCALES DE LAS ENTIDADES VIGILADAS.

Referencia: Imparte instrucciones en materia de requerimientos mínimos de seguridad y calidad para la realización de operaciones.

Apreciados señores:

Esta Superintendencia, en ejercicio de las facultades señaladas en el numeral 5º del artículo 11.2.1.4.2 del Decreto 2555 de 2010, imparte las siguientes instrucciones en materia de requerimientos de seguridad y calidad para la realización de operaciones:

PRIMERA: Modificar los subnumerales 1.2.2.1.2.7., 1.3., 2.1., 2.3.3.1.3., 2.3.3.1.12., 2.3.3.1.16., 2.3.4.1., 2.3.4.1.3., 2.3.4.2.1., 2.3.4.5.3., 2.3.4.7.5., 2.3.4.9.4., 2.3.4.11., 2.3.4.11.2. y 2.3.4.12.11. del Capítulo I, Título II, Parte I de la Circular Básica Jurídica (CBJ), relacionados con los canales, medios, seguridad y calidad en el manejo de información en la prestación de servicios financieros y realización de operaciones.

SEGUNDA: Modificar el subnumeral 3.2.4.6. del Capítulo I, Título III, Parte I, de la CBJ relacionado con el soporte al momento de la realización de operaciones monetarias.

TERCERA: Adicionar los subnumerales 2.2.8., 2.2.9., 2.2.10. y 2.3.8. al Capítulo I, Título II, Parte I de la CBJ, con el fin de introducir los conceptos de ambiente de venta presente, ambiente de venta no presente y entidades administradoras de pasarelas de pago, y fijar los requerimientos mínimos que deben cumplir los establecimientos de crédito y los administradores de sistemas de pago de bajo valor que vinculen administradores de pasarelas de pago para la realización de operaciones en ambiente de venta no presente.

CUARTA: Las modificaciones contenidas en los subnumerales señalados en la instrucción primera y segunda de la presente Circular Externa rigen a partir del 1 de diciembre de 2018.

Las instrucciones contenidas en el subnumeral 2.3.8. del Capítulo I, Título II, Parte I de la CBJ deben ser cumplidas a partir del 2 de junio de 2018.

Circular Externa, deberán adecuarse a las instrucciones impartidas a más tardar el 31 de diciembre de 2018.

Se anexan las páginas objeto de modificación.

Cordialmente,

JORGE CASTAÑO GUTIERREZ

Superintendente Financiero de Colombia

/050000

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

CIRCULAR EXTERNA 007 DE 2018

(Junio 05)

Señores
REPRESENTANTES LEGALES Y REVISORES FISCALES DE LAS ENTIDADES VIGILADAS Y LOS OPERADORES DE INFORMACIÓN DE LA PILA.

Referencia: Imparte instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad

Apreciados señores:

Teniendo en cuenta que el auge de la digitalización de los servicios financieros, la mayor interconectividad de los agentes y la masificación en el uso de canales electrónicos, entre otros elementos, han derivado en un incremento de la exposición a riesgos cibernéticos, esta Superintendencia en ejercicio de sus facultades, en especial las conferidas en el numeral 9 del artículo 11.2.1.4.2 del Decreto 2555 de 2010 y en aras de fortalecer la gestión relativa a este riesgo en las entidades vigiladas, imparte las siguientes instrucciones en complemento de aquellas relacionadas con la administración de los riesgos operativos y la seguridad de la información:

PRIMERA: Adicionar el Capítulo V “Requerimientos mínimos para la gestión del riesgo de ciberseguridad” al Título IV de la Parte I de la Circular Básica Jurídica (C.E. 029 de 2014).

SEGUNDA: La presente Circular entra a regir seis meses después del momento de su publicación, con lo cual la obligación contenida en el subnumeral 1 para las entidades exceptuadas, debe ser cumplida dentro de este término.

No obstante, lo anterior, las entidades deben dar cumplimiento a los requerimientos establecidos en los subnumerales 3.10., 4.1., 4.2., 4.3. y 4.4., un año después y los requerimientos establecidos en los subnumerales 3.2.8., 4.1.6. y 4.1.7., dieciocho meses después de la publicación.

Se anexan las páginas correspondientes.

Cordialmente,

JORGE CASTAÑO GUTIÉRREZ
Superintendente Financiero de Colombia
/050000

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

PARTE I
INSTRUCCIONES GENERALES APLICABLES A LAS ENTIDADES VIGILADAS

TÍTULO IV
DEBERES Y RESPONSABILIDADES

CAPÍTULO V:
REQUERIMIENTOS MÍNIMOS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD

CONTENIDO

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

PARTE I
INSTRUCCIONES GENERALES APLICABLES A LAS ENTIDADES VIGILADAS

TÍTULO IV
DEBERES Y RESPONSABILIDADES

CAPÍTULO V:
REQUERIMIENTOS MÍNIMOS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD

1. ÁMBITO DE APLICACIÓN

Las instrucciones de que trata el presente Capitulo deben ser adoptadas por las entidades sometidas a la inspección y vigilancia de la Superintendencia Financiera de Colombia (SFC) y operadores de información de la PILA, con excepción del 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. En todo caso, las entidades exceptuadas deben hacer periódicamente una autoevaluación del riesgo de ciberseguridad y seguridad de la información, que incluya una identificación de las mejoras a implementar en su Sistema de Administración de Riesgo Operativo.

Los resultados de la autoevaluación, así como el plan de acción para implementar los ajustes a que haya lugar, deben estar a disposición de la SFC.

2. DEFINICIONES

Para efectos del presente Capítulo, se establecen las siguientes definiciones:

2.1. Activo de información

Conocimiento o datos que tienen valor para la entidad o el individuo.

2.2. Ciberamenaza o amenaza cibernética

Aparición de una situación potencial o actual que pudiera convertirse en un ciberataque.

2.3. Ciberataque o ataque cibernético

Acción criminal organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objetivo de la misma o donde el ciberespacio es fuente o herramienta de comisión de un crimen.

2.4. Ciberespacio

Entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física.

2.5. Ciberiesgo o riesgo cibernético

Posibles resultados negativos derivados de fallas en la seguridad de los sistemas tecnológicos o asociados a ataques cibernéticos.

2.6. Ciberseguridad

Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la entidad.

2.7. CSIRT (*Computer Security Incident Response Team*)

Equipo responsable del desarrollo de medidas preventivas y de respuesta ante incidentes informáticos.

2.8. Evento de ciberseguridad

Ocurrencia de una situación que podría afectar la protección o el aseguramiento de los datos, sistemas y aplicaciones de la entidad que son esenciales para el negocio.

2.9. Incidente de ciberseguridad

Ocurrencia de una situación que afecta la protección o el aseguramiento de los datos, sistemas y aplicaciones de la entidad que son esenciales para el negocio.

2.10. Información en reposo

Datos guardados en dispositivos de almacenamiento persistente (por ejemplo, cintas, copias de seguridad externas, dispositivos móviles, discos duros, entre otros).

2.12. Resiliencia

Es la capacidad de un mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que pudo estar sometido.

2.13. Seguridad de la información

Es el conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para proteger, asegurar y preservar la confidencialidad, integridad y disponibilidad de la información que se almacene, reproduzca o procese en los sistemas informáticos de la entidad.

2.14. SIEM (*Security Information and Event Management*)

Sistema de información que proporciona análisis en tiempo real de las alertas de seguridad generadas por las aplicaciones, dispositivos de seguridad y los elementos de red. Suelen ser sistemas de centralización de *logs*.

2.15. SOC (*Security Operation Center*)

Unidad encargada de monitorear, evaluar y defender los sistemas de información empresarial (sitios web, aplicaciones, bases de datos, centros de datos, servidores, redes, escritorios y otros dispositivos).

2.16. Terceros críticos

Terceros con quien se vincula la entidad y que, de acuerdo con los parámetros establecidos por la propia entidad, pueden tener incidencia directa en la seguridad de su información.

2.17. Vulnerabilidad

Debilidad de un activo o control que puede ser explotado por una amenaza. Se tienen en cuenta todas aquellas amenazas que surgen por la interacción de los sistemas en el ciberespacio.

3. OBLIGACIONES GENERALES EN MATERIA DE CIBERSEGURIDAD

Las entidades deben contar con políticas, procedimientos y recursos técnicos y humanos necesarios para gestionar efectivamente el riesgo de ciberseguridad. En ese sentido, deben adoptar, como mínimo, las medidas que se relacionan a continuación en materia de ciberseguridad:

3.1. Establecer una política que contenga los principios, procedimientos y lineamientos para la gestión de la seguridad de la información y riesgo de ciberseguridad en la entidad. Esta política debe tener las siguientes características:

3.1.1. Ser aprobada por la junta directiva.

3.1.2. Documentar las responsabilidades, procesos, procedimientos, etapas y la gestión que se realiza frente a la ciberseguridad.

3.1.3. Establecer las funciones de la unidad de seguridad de la información y la ciberseguridad.

3.1.4. Establecer los principios y lineamientos para promover una cultura de ciberseguridad que incluya actividades de difusión, capacitación y concientización tanto al interior de la entidad como frente a usuarios y terceros que esta considere relevantes dentro de la política de ciberseguridad. Estas actividades deben realizarse periódicamente y pueden incluirse, adicionalmente, en los cursos sobre riesgo operativo que realice la entidad.

3.2. Establecer una unidad que gestione los riesgos de seguridad de la información y la ciberseguridad. Esta unidad debe tener, al menos, las siguientes características y responsabilidades:

3.2.1. Se debe conformar considerando aspectos tales como la estructura, tamaño, canales de atención, volumen transaccional, número de clientes, evaluación del riesgo y servicios prestados por la entidad.

3.2.2. Debe realizar una gestión efectiva de la seguridad de la información y la ciberseguridad en la entidad.

3.2.3. Debe reportar a la junta directiva y a la alta dirección, los resultados de su gestión, especialmente en la evaluación que haga de la confidencialidad, integridad y disponibilidad de la información, identificación de ciberamenazas, resultados de la evaluación de efectividad de los programas de ciberseguridad, propuestas de mejora en materia de ciberseguridad y resumen de los incidentes de ciberseguridad que afectaron la entidad. La periodicidad de los reportes debe ser, al menos, semestralmente.

3.2.4. Debe actualizarse permanentemente y de manera especializada para que esté al tanto de las nuevas modalidades de ciberataques que pudieran llegar a afectar a la entidad, según las políticas que establezca la entidad de acuerdo con su evaluación de riesgo y atendiendo criterios de razonabilidad.

3.2.5. Debe sugerir las capacitaciones que deben recibir regularmente los funcionarios de la entidad en temas relacionados con ciberseguridad y mantenerlos actualizados sobre las nuevas ciberamenazas.

3.2.6. Ser la principal responsable en el monitoreo y verificación del cumplimiento de las políticas y procedimientos que se establezcan en materia de ciberseguridad, sin perjuicio a aquellas tareas que realiza la auditoría interna.

3.2.7. Asesorar a la alta gerencia y la junta directiva en temas que considere necesarios sobre seguridad de la información y

3.2.9 Sugerir los presupuestos de seguridad de la información y ciberseguridad. Dichos presupuestos deben manejarse de manera diferenciada a los de operaciones y tecnología de la información.

3.2.10. Verificar el cumplimiento de las obligaciones contenidas en el Capítulo I del Título II de la Parte I de la CBJ, en lo que sea pertinente con sus funciones.

3.2.11. Debe realizar las demás actividades establecidas en este Capítulo que por su naturaleza les sean asignadas

Sin perjuicio de las funciones que debe realizar la unidad de la que trata este subnumeral 3.2., las funciones de gestión de riesgos relacionadas con respuesta a incidentes pueden ser desagregadas en diferentes áreas de la entidad.

3.3. Contar con un sistema de gestión para la ciberseguridad, para lo cual se pueden tomar como referencia el estándar ISO 27032, NIST con sus publicaciones SP800 y SP1800, ISF (*Information Security Forum*), CIS *Critical Security Controls* (CSC) o *Cobit 5 for Information Security,* y sus respectivas actualizaciones.

3.4. Implementar controles para mitigar los riesgos que pudieran afectar la seguridad de información confidencial, en reposo o en tránsito.

3.5. Emplear mecanismos para la adecuada autenticación y segregar las funciones y responsabilidades de los usuarios con privilegios de administrador o que brindan soporte remoto, para mitigar los riesgos de seguridad de la información.

3.6. Establecer procedimientos para la retención y destrucción final de la información, sin que se desconozca lo establecido en el Artículo 96 del EOSF y demás normas aplicables.

3.7. Establecer una estrategia de comunicación e información que contemple los siguientes ejes, sin perjuicio de las obligaciones de reporte a la SFC y demás autoridades de acuerdo con la normatividad aplicable:

3.7.1. Información que reportará a la SFC, sobre incidentes de ciberseguridad que afecten de manera significativa la confidencialidad, integridad o disponibilidad de la información de la entidad, haciendo una breve descripción del incidente, su impacto y las medidas adoptadas para gestionarlo.

3.7.2. Información que reportará a las autoridades que hacen parte del modelo nacional de gestión de incidentes cibernéticos, sobre incidentes cibernéticos.

3.7.3. Información que reportará a los consumidores financieros, sobre incidentes cibernéticos que hubiesen afectado la confidencialidad o integridad de su información, así como las medidas adoptadas para remediar la información.

3.8. Incluir dentro del ciclo de vida del desarrollo del software, incluyendo servicios web y *apps*, que procesan la información confidencial de la entidad o de los consumidores financieros (desde las etapas iniciales tales como levantamiento de requerimientos hasta las pruebas de seguridad pertinentes y producción), aspectos relativos con la seguridad de la información que permitan mitigar dicho riesgo.

3.9. Incluir en los contratos que se celebren con terceros críticos, las medidas y obligaciones pertinentes para la adopción y el cumplimiento de políticas para la gestión de los riesgos de seguridad de la información y ciberseguridad.

3.10. Verificar periódicamente el cumplimiento de las obligaciones y medidas establecidas conforme al subnumeral 3.9. de este Capítulo, para lo cual pueden implementar los mecanismos adecuados para el efecto.

3.11. Contar con indicadores para medir la eficacia y eficiencia de la gestión de la seguridad de la información y la ciberseguridad.

3.12. Gestionar la seguridad de la información y la ciberseguridad en los proyectos que impliquen la adopción de nuevas tecnologías.

3.13. Considerar la conveniencia de contar con un seguro que cubra los costos asociados a ataques cibernéticos.

4. ETAPAS

Para la gestión de la seguridad de la información y la ciberseguridad las entidades deberán considerar, como mínimo, las siguientes etapas:

4.1. Prevención

Las entidades deben desarrollar e implementar los controles adecuados para velar por la seguridad de la información y la gestión de la ciberseguridad. La función de prevención admite la capacidad de limitar o contener el impacto de un posible incidente de ciberseguridad. En esta etapa, las entidades deben cuando menos:

4.1.1. Establecer, mantener y documentar los controles de acceso (lógicos, físicos y procedimentales) y gestión de identidades bajo la premisa que las personas solo pueden disponer de los recursos que demande su trabajo, durante el tiempo que ello sea necesario.

4.1.2. Adoptar políticas, procedimientos y mecanismos para evitar la fuga de datos e información.

4.1.3. Gestionar y documentar la seguridad de la plataforma tecnológica.

4.1.4. La unidad de la que trata el subnumeral 3.2. de este Capítulo debe contar con los recursos necesarios para realizar una adecuada gestión de la seguridad de la información y la ciberseguridad.

4.1.7. Realizar pruebas del plan de continuidad del negocio que simulen la materialización de ataques cibernéticos.

4.1.8. Contar con herramientas o servicios que permitan hacer correlación de eventos que puedan alertar sobre incidentes de seguridad, tal como un SIEM.

4.1.9. De acuerdo con la estructura, canales de atención, volumen transaccional y número de clientes, monitorear diferentes fuentes de información tales como sitios web, blogs y redes sociales, con el propósito de identificar posibles ataques cibernéticos contra la entidad.

4.1.10. Colaborar con las autoridades que hacen parte del modelo nacional de gestión de ciberseguridad en los proyectos que se adelanten con el propósito de fortalecer la gestión de la ciberseguridad en el sector financiero y a nivel nacional.

4.1.11. Informar a los consumidores financieros de la entidad sobre las medidas de seguridad y recomendaciones que deberán adoptar para su ciberseguridad.

4.2. Protección y detección

Las entidades deben desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad. La función de protección y detección permite el descubrimiento oportuno de eventos e incidentes de ciberseguridad y cómo protegerse ante los mismos. Las entidades deben:

4.2.1. Adoptar procedimientos y mecanismos para identificar y analizar los incidentes de ciberseguridad que se presenten.

4.2.2. Gestionar las vulnerabilidades de aquellas plataformas que soporten activos de información críticos y que estén expuestos en el ciberespacio.

4.2.3. Realizar un monitoreo continuo a su plataforma tecnológica con el propósito de identificar comportamientos inusuales que puedan evidenciar ciberataques contra la entidad.

4.3. Respuesta y comunicación

Aún con las medidas de seguridad adoptadas, las entidades deben desarrollar e implementar actividades para mitigar los incidentes relacionados con ciberseguridad. Para hacerle frente a esta situación las entidades deben:

4.3.1. Establecer procedimientos de respuesta a incidentes cibernéticos tales como: desconexión automática de equipos, cambios de contraseñas, actualizar la base de firmas del antivirus, bloqueo de direcciones IP o cualquier otro que determine la entidad.

4.3.2. Evaluar los elementos de la red para identificar otros dispositivos que pudieran haber resultado afectados.

4.3.3. Establecer los procedimientos para reportar, cuando se considere pertinente, al Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT) o quien haga sus veces, directamente o a través de CSIRT sectoriales, los ataques cibernéticos que requieran de su gestión.

4.3.4. Adoptar los mecanismos necesarios para recuperar los sistemas de información al estado en que se encontraban antes del ataque cibernético.

4.3.5. En la medida de lo posible, preservar las evidencias digitales para que las áreas de seguridad o las autoridades puedan realizar las investigaciones correspondientes.

4.4. Recuperación y aprendizaje

Desarrollar e implementar actividades apropiadas para mantener los planes de resiliencia y restaurar cualquier capacidad o servicio que se haya deteriorado debido a un incidente de ciberseguridad. Las entidades deben:

4.4.1. Ajustar sus sistemas de gestión de riesgo y de seguridad de la información como consecuencia de los incidentes presentados, adoptando los controles que resulten pertinentes.

4.4.2. Socializar, cuando la entidad lo considere pertinente, las lecciones aprendidas al interior de la organización y con las entidades de su sector.

3.2.2. Requisitos de la información

La información que divulguen o suministren las entidades vigiladas debe cumplir con la finalidad prevista en el subnumeral precedente y para ello, como mínimo, debe:

3.2.2.1. Ser cierta, suficiente y corresponder a lo ofrecido o previamente publicitado.
3.2.2.2. Ser clara y comprensible.
3.2.2.3. Ser divulgada o suministrada oportunamente.
3.2.2.4. Encontrarse vigente al momento en que se suministre o divulgue, indicándose el tiempo de vigencia y la fecha de la última actualización.
3.2.2.5. Ser entregada o estar permanentemente disponible para los consumidores financieros, como mínimo en los sitios web de las entidades vigiladas y en sus oficinas.

3.2.3. Difusión de la información

Las entidades vigiladas deben atender las siguientes instrucciones en la difusión de la información a los consumidores financieros:

3.2.3.1. La información debe ser divulgada a través de mecanismos que garanticen la observancia de los requisitos señalados en el subnumeral precedente. Los criterios empleados para la selección de tales mecanismos deben estar debidamente documentados.

3.2.3.2. Las entidades vigiladas deben divulgar las medidas, canales e instrumentos que implementen para la atención a personas con cualquier tipo de discapacidad y adultos mayores.

3.2.3.3. La información que suministren las entidades vigiladas a los consumidores financieros directamente o a través de terceros (asesores, agentes comerciales, entre otros) debe ser concordante con aquella contenida en los contratos correspondientes y la divulgada o publicitada por la entidad a través de los diferentes medios y/o canales; y ajustarse a la realidad jurídica y económica del servicio promovido.

3.2.4. A través de los diversos canales de prestación de servicios

La información que se suministre a través de los distintos canales de prestación u ofrecimiento de los productos o servicios de las entidades vigiladas debe cumplir con las siguientes condiciones:

3.2.4.1. Dar a conocer a sus clientes y usuarios, en forma previa a la realización de la operación, el costo de la misma, si lo hay, brindándoles la posibilidad de efectuarla o no. En este evento sin generación de cobro alguno. Tratándose de cajeros automáticos la obligación sólo aplica para operaciones realizadas en el territorio nacional y cuyo autorizador tenga domicilio en Colombia.

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

3.2.4.3. 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.

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

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

3.2.4.6. Generar un soporte al momento de la realización de cada operación monetaria. Dicho soporte debe contener al menos la siguiente información: fecha, hora (hora y minuto), código del dispositivo (para Internet: la dirección IP desde la cual se hizo la misma; para dispositivos móviles: el número desde el cual se hizo la conexión), número de la operación, costo para el cliente o usuario, tipo de operación, entidades involucradas (si a ello hay lugar) y número de las cuentas que afectan. Se deben ocultar los números de las cuentas con excepción de los últimos 4 caracteres, salvo cuando se trate de la cuenta que recibe una transferencia. Cuando no se pueda generar el soporte, se debe advertir previamente al cliente o usuario de esta situación. Para el caso de IVR y dispositivos móviles se entenderá cumplido el requisito establecido en este numeral cuando se informe el número de la operación. Tratándose de pagos inferiores a **3** salarios mínimos legales diarios vigentes SMLDV, no será obligatoria la generación del soporte al que se refiere el presente numeral.

3.2.4.7. La prestación de servicios a través de corresponsales exige el diseño de una estrategia que le permita a la entidad vigilada informar a los clientes y usuarios, las características del servicio prestado a través de los corresponsales, las operaciones realizadas a través de éstos, las medidas de seguridad que deben tomar para su realización y los medios a través de los cuales podrá comunicar a la entidad vigilada cualquier falla o irregularidad en la prestación del servicio.

En todo caso, las entidades vigiladas son las únicas responsables de que las actividades de promoción y publicidad que efectúen los corresponsales se adelanten conforme a lo establecido en el EOSF, a lo dispuesto en el Título 9 del Libro 36 de la Parte 2 del Decreto 2555 de 2010, así como en los instructivos expedidos por la SFC.

3.2.5. A través de los sitios web de las entidades

Las entidades vigiladas deben observar las siguientes reglas, en sus respectivos sitios web:

3.2.5.1. Todas las entidades deben implementar en la página de inicio de sus sitios web un vínculo con el nombre

En ese sentido, se entienden autorizadas las actividades de promoción de productos, así como la entrega y recepción de solicitudes de seguro y la implementación de mecanismos de comprobación de la asegurabilidad, de los productos asociados a los ramos indicados anteriormente.

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 copias de pólizas y 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 los seguros comercializados a través de corresponsales.

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 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

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.

1.4. Uso de red

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

1.4.1. Modalidades de uso de red

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

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

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

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

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

1.4.1.1.1. Contrato de uso de red

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

1.4.1.1.1.1. Identificación de las partes y objeto del contrato.

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

1.4.1.1.1.3. Las obligaciones de las partes asociadas al intercambio de información que permita garantizar un adecuado suministro de información a los consumidores financieros para cada producto específico; así como las que correspondan a

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, 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

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.

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

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

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

2.3. 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

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 **expeditos** para el bloqueo de canales o de instrumentos para la realización de operaciones, **cuando lo solicite el cliente,** cuando existan situaciones o hechos que lo ameriten o después de un número de intentos de accesos fallidos, 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 **el Instituto Nacional de Metrología de Colombia**.

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.

2.3.3.2. 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

identificación del equipo, fecha y hora. En desarrollo de lo anterior, se deben establecer mecanismos que restrinjan el acceso a dicha información, para que solo pueda ser usada por el personal que lo requiera en función de su trabajo.

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

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

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

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

2.3.4. Requerimientos especiales por tipo de canal

2.3.4.1. En oficinas

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

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

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

2.3.4.1.3. Contar con cámaras de video, las cuales deben cubrir al menos el acceso principal y las áreas de atención al público. Las imágenes deben ser conservadas por lo menos **6** meses o en el caso en que la imagen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

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

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

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

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

2.3.4.2. Cajeros automáticos (ATM)

Deben cumplir, como mínimo, con los siguientes requerimientos:

2.3.4.2.1. Contar con sistemas de video grabación que asocien los datos y las imágenes de cada operación monetaria. Las imágenes deben ser conservadas por lo menos **6** meses o en el caso en que la imagen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

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

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

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

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

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

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

2.3.4.3. 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.

2.3.4.4. 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.

2.3.4.8. 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 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.

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

2.3.4.12.2. 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.

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.

2.3.5 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.

2.3.6.2.3. Propiedad de la información.

2.3.6.2.4. Restricciones sobre el software empleado.

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

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

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

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

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

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

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

2.3.7 Análisis de vulnerabilidades

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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