004

CIRCULAR EXTERNA DE

(07 FEB 2024)

Señores
REPRESENTANTES LEGALES DE LAS ENTIDADES VIGILADAS

Referencia: Instrucciones relativas a las finanzas abiertas y comercialización de tecnología e infraestructura a terceros

Apreciados señores:

Como es de su conocimiento, mediante el Decreto 1297 de 2022, incorporado en el Decreto 2555 de 2010, se expidió, entre otros, el marco regulatorio de las finanzas abiertas en Colombia. De conformidad con el Documento Técnico «Arquitectura Financiera Abierta en Colombia», documento soporte del Decreto 1297 de 2022, se entiende por finanzas abiertas la práctica en la cual las entidades vigiladas por la Superintendencia Financiera de Colombia (SFC) abren sus sistemas para que la información de los consumidores financieros pueda ser compartida de forma estandarizada con otras entidades vigiladas o con terceros, con la autorización del consumidor financiero y con el objetivo de que dichas entidades provean servicios a dichos clientes.

Dicha normativa radicó en cabeza de la SFC el deber de definir los estándares tecnológicos relacionados con la seguridad de la información y demás necesarios para promover la interoperabilidad y el desarrollo de las finanzas abiertas. De igual forma, el citado Decreto autorizó a las entidades vigiladas por esta Entidad a comercializar a terceros la tecnología e infraestructura que utilicen para la prestación de sus servicios.

Ahora bien, el artículo 4 del Decreto 0052 del 30 de enero de 2024 «*Por medio del cual se corrigen unos yerros en el Decreto 1533 de 2022 y se dictan otras disposiciones*» dispuso lo siguiente: «*(…) Plazo para la definición de estándares. La Superintendencia Financiera de Colombia impartirá instrucciones a sus vigiladas, respecto de los estándares a los que hace referencia el artículo 2.35.10.1.1. del Decreto 2555 de 2010, dentro de cuatro (4) meses siguientes a la entrada en vigencia del presente Decreto*».

Cabe destacar que las finanzas abiertas, además de promover la competencia en los mercados financieros, fomentan la profundización de la inclusión financiera y crediticia al incentivar el ingreso de nuevos participantes, propiciar la creación de nuevos productos y servicios financieros y mejorar el conocimiento y perfilamiento de los consumidores financieros.

En cumplimiento de lo anterior, esta Superintendencia considera necesario consolidar la arquitectura para el desarrollo de las finanzas abiertas en Colombia, teniendo en cuenta la importancia de la digitalización de la economía a través del uso de nuevas tecnologías y del rol de los datos de los consumidores financieros en el ofrecimiento de productos y servicios innovadores que atiendan sus necesidades e incentiven la inclusión financiera.

En virtud de lo expuesto, esta Superintendencia por medio de la presente Circular imparte instrucciones para: i) definir los estándares tecnológicos, de seguridad y demás necesarios que deben adoptar las entidades vigiladas para el desarrollo de las finanzas abiertas en condiciones de interoperabilidad, ii) establecer las obligaciones que deben cumplir las entidades vigiladas para que el tratamiento de los datos de los consumidores financieros se realice en condiciones de seguridad,

transparencia y eficiencia, atendiendo lo dispuesto en las Leyes 1266 de 2008 y 1581 de 2012 y normas que las reglamenten, sustituyan, modifiquen o adicionen, y iii) señalar los lineamientos que deben cumplir las entidades vigiladas cuando comercialicen a terceros la tecnología e infraestructura que utilicen para la prestación de sus servicios.

De conformidad con lo establecido en el artículo 7 de la Ley 1340 de 2009, esta Entidad solicitó concepto a la Superintendencia de Industria y Comercio mediante oficio 2022173349-112 del 13 de junio de 2023, con el fin de conocer la incidencia del proyecto sobre la libre competencia económica en el marco de la función de abogacía de la competencia. Como consecuencia de lo anterior, el 29 de junio de 2023, la Superintendencia de Industria y Comercio remitió concepto de abogacía de la competencia mediante radicado número 23-274447-1, en el que formuló cuatro recomendaciones, las cuales fueron acogidas en la Circular por parte de esta Superintendencia.

Con posterioridad a la expedición del concepto de abogacía de la competencia referido, esta Superintendencia llevó a cabo modificaciones a las instrucciones con ocasión de algunos comentarios externos recibidos. No obstante, ninguna de las modificaciones a las instrucciones altera las respuestas que en su momento se dieron en el diligenciamiento del cuestionario de abogacía de la competencia contenido en la Resolución 44649 de 2010. Por lo anterior, el análisis llevado a cabo por la Autoridad de Competencia tiene plena aplicación y no se hace necesario surtir de nuevo el trámite de abogacía de la competencia ante la Superintendencia de Industria y Comercio.

En desarrollo de lo anterior, y en virtud de las facultades previstas en el literal a) del numeral 3° del artículo 326 del Estatuto Orgánico del Sistema Financiero, así como el artículo 2.35.10.1.1 y el numeral 4 del artículo 11.2.1.4.2 del Decreto 2555 de 2010, esta Entidad imparte las siguientes instrucciones:

PRIMERA: Crear el Capítulo IX en el Título I de la Parte I de la Circular Básica Jurídica denominado «*Reglas relativas a las finanzas abiertas*» con el fin de definir los estándares tecnológicos, de seguridad y demás necesarios que deben adoptar las entidades vigiladas para el desarrollo de las finanzas abiertas en condiciones de interoperabilidad, así como impartir instrucciones para que el tratamiento de los datos de los consumidores financieros se realice en condiciones de seguridad, transparencia y eficiencia, atendiendo lo dispuesto en las Leyes 1266 de 2008 y 1581 de 2012 y demás normas que las reglamenten, sustituyan, modifiquen o adicionen, en el marco de las de finanzas abiertas.

SEGUNDA: Crear el Capítulo X del Título I de la Parte I de la Circular Básica Jurídica denominado «*Comercialización de Tecnología e Infraestructura a Terceros*», con el fin de definir los lineamientos que deben atender las entidades vigiladas cuando desarrollen la actividad de comercialización de tecnología e infraestructura que utilicen en la prestación de sus servicios y desarrollo de sus actividades conexas.

TERCERA: Modificar el subnumeral 3.2.3.4. del Capítulo I del Título III de la Parte I de la Circular Básica Jurídica denominado «*Acceso e información al consumidor financiero*» con el fin de armonizarlo con las finanzas abiertas que se regulan a través de la presente Circular.

CUARTA: Derogar el numeral 6 «*Uso de información*» del Capítulo IX del Título IV de la Parte III de la Circular Básica Jurídica denominado «*Entidades*

Administradoras de Sistemas de Pago de Bajo Valor - EASPBV» con el fin de actualizarlo atendiendo a lo previsto en el numeral 4 del artículo 2.17.2.1.14 modificado por el artículo 2 del Decreto 1297 de 2022. Así mismo, se reenumera el actual numeral 7 «*Estándares Operativos, Técnicos y de Seguridad*» como numeral 6 del citado Capítulo.

QUINTA: Las entidades vigiladas que tienen implementados modelos de finanzas abiertas a través de estándares de arquitectura, tecnología y seguridad diferentes a los previstos en el subnumeral 3.2 del Capítulo IX del Título I de la Parte I de la Circular Básica Jurídica denominado «*Reglas relativas a las finanzas abiertas*» tendrán un plazo máximo de 18 meses contados a partir de la expedición de la presente Circular para llevar a cabo la adopción de la totalidad de los estándares de arquitectura, tecnología y seguridad establecidos en el referido numeral.

Dichas entidades vigiladas deberán remitir a la delegatura institucional correspondiente de la Superintendencia Financiera de Colombia un plan de adopción a más tardar el 1 de agosto de 2024.

SEXTA: RÉGIMEN DE TRANSICIÓN. Las entidades vigiladas que participen en modelos de finanzas abiertas deberán atender los siguientes plazos para dar cumplimiento a las instrucciones contenidas en la presente Circular:

- 18 meses contados a partir de la fecha de expedición de la presente Circular en lo relacionado con el numeral 3.2 del Capítulo IX del Título I de la Parte I de la Circular Básica Jurídica denominado «*Reglas relativas a las finanzas abiertas*».

- 6 meses contados a partir de la fecha de expedición de la presente Circular en lo relacionado con las demás instrucciones contenidas en el Capítulo IX del Título I de la Parte I de la Circular Básica Jurídica denominado «*Reglas relativas a las finanzas abiertas*».

- Las entidades vigiladas que se encuentren comercializando la tecnología e infraestructura empleada para el desarrollo de su actividad, deberán dar cumplimiento a las instrucciones contenidas en el Capítulo X del Título I de la Parte I de la Circular Básica Jurídica denominado «*Comercialización de Tecnología e Infraestructura a Terceros*» en un plazo no mayor a 12 meses contados a partir de la fecha de su expedición.

SÉPTIMA: VIGENCIA. La presente Circular rige a partir de su publicación, sin perjuicio de lo previsto en la instrucción sexta.

Se anexan las páginas objeto de modificación.

Cordialmente,

CÉSAR FERRARI Ph.D.
Superintendente Financiero
50000

Elaboró: AMPH, MABR, GFB, LPM, JBCG, EAPJ y AMZT.
Revisó: CGR
Aprobó: JRH

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

PARTE I
INSTRUCCIONES GENERALES APLICABLES A LAS ENTIDADES VIGILADAS

TÍTULO I
ASPECTOS GENERALES

CAPÍTULO IX. REGLAS RELATIVAS A LAS FINANZAS ABIERTAS

CONTENIDO

1. CONSIDERACIONES GENERALES

2. TERCEROS RECEPTORES DE DATOS

3. ESTÁNDARES TECNOLÓGICOS Y DE SEGURIDAD

4. TRATAMIENTO DE LOS DATOS DE LOS CONSUMIDORES FINANCIEROS EN FINANZAS ABIERTAS

5. DEBERES DE REVELACIÓN DE INFORMACIÓN

PARTE I
INSTRUCCIONES GENERALES APLICABLES A LAS ENTIDADES VIGILADAS

TÍTULO I
ASPECTOS GENERALES

CAPÍTULO IX: REGLAS RELATIVAS A LAS FINANZAS ABIERTAS

1. CONSIDERACIONES GENERALES

En desarrollo de las facultades previstas en el artículo 2.35.10.1.1. del Decreto 2555 de 2010, incorporado por el Decreto 1297 de 2022, la Superintendencia Financiera de Colombia (SFC) determina los estándares tecnológicos, de seguridad y demás necesarios para el desarrollo de las finanzas abiertas regulados por el Título 8 del Libro 35 de la Parte 2 del Decreto 2555 de 2010.

De conformidad con el Documento Técnico «Arquitectura Financiera Abierta en Colombia», documento soporte del Decreto 1297 de 2022, se entiende por finanzas abiertas la práctica en la cual las entidades vigiladas por la Superintendencia Financiera de Colombia (SFC) abren sus sistemas para que la información de los consumidores financieros pueda ser compartida de forma estandarizada con otras entidades vigiladas o con terceros, con la autorización del consumidor financiero y con el objetivo de que dichas entidades provean servicios a dichos clientes. Las entidades vigiladas que participen en finanzas abiertas deben cumplir con las instrucciones previstas en el presente Capítulo.

2. TERCEROS RECEPTORES DE DATOS

Las entidades vigiladas que participen en finanzas abiertas deben vincular a los terceros receptores de datos. Para el efecto, las entidades vigiladas deben adoptar políticas y procedimientos para la vinculación de los terceros receptores de datos que cumplan los requisitos establecidos en el presente numeral. Dichas políticas deben ser aprobadas por la junta directiva u órgano que haga sus veces. Las mencionadas políticas y procedimientos deben estar disponibles en la página web de la respectiva entidad vigilada.

Se entiende por terceros receptores de datos aquellas personas jurídicas que tratan los datos personales de los consumidores financieros en el marco de las finanzas abiertas.

2.1. Para la vinculación del tercero receptor de datos las entidades vigiladas deben verificar que estos:

a) Estén inscritos en el Registro Nacional de Bases de Datos. En el evento en que los terceros receptores de datos no estén inscritos en el mencionado registro, las entidades vigiladas deben verificar que los mismos cuenten con políticas y procedimientos para el tratamiento de datos personales.

b) Cuenten con procedimientos para la atención de consultas y reclamos, de conformidad con las normas aplicables.

c) Cuenten con mecanismos que les permitan:

i) Gestionar los riesgos asociados al tratamiento de los datos personales del consumidor financiero, en particular, el de seguridad de la información y ciberseguridad, así como fallas en la infraestructura tecnológica y en los sistemas de información donde se procesan y almacenan los datos. Para el efecto, las entidades vigiladas pueden tener en cuenta marcos de referencia, tales como: ISO 27001, NIST Cybersecurity Framework, OWASP ASVS, última versión o cualquiera que los modifique, sustituya o adicione. En caso de que cualquiera de los marcos de referencia sea declarado obsoleto por parte del organismo que lo establece o soporta, la entidad vigilada debe tener en cuenta aquel que lo modifique, sustituya o adicione.

ii) Mantener cifrados los datos personales de los consumidores financieros que estén en almacenamiento o circulación usando para el efecto estándares y algoritmos reconocidos internacionalmente que briden al menos la seguridad ofrecida por AES o RSA.

iii) Contar con sistemas de monitoreo de la información para el desarrollo de finanzas abiertas.

iv) Gestionar las vulnerabilidades de aquellas plataformas que hagan uso de los datos suministrados en el marco de finanzas abiertas.

v) Contar con la certificación PCI-DSS emitida por una entidad que ostente la categoría QSA (Qualified Security Assessor) y soportada por el documento AoC (Attestation of Compliance) correspondiente, en el evento en que el tercero receptor de datos pretenda almacenar, procesar y/o transmitir datos contenidos en tarjetas débito y crédito.

vi) Informar a las entidades vigiladas, en el menor tiempo posible, sobre cualquier evento o situación que pueda comprometer la seguridad de los datos personales de los consumidores financieros.

En relación con las entidades vigiladas que actúen como terceros receptores de datos y estén obligadas a cumplir con las instrucciones en materia de seguridad de la información y ciberseguridad previstas en el Capítulo V del Título IV de la Parte I de la Circular Básica Jurídica, se entenderán verificados los requisitos previstos en el literal c) del presente numeral.

d) Cuenten con procedimientos para la revocatoria y supresión de los datos personales de los consumidores financieros, de conformidad con las normas aplicables.

2.2. Las entidades vigiladas deben aplicar el tratamiento previsto para los clientes o potenciales clientes a los terceros receptores de datos, de conformidad con las medidas adoptadas por la respectiva entidad para la administración del riesgo de lavado de activos y financiación del terrorismo en desarrollo de lo dispuesto en los artículos 102 y siguientes del Estatuto Orgánico del Sistema Financiero y del Capítulo IV del Título IV de la Parte I de la Circular Básica Jurídica.

004

2.3. Las entidades vigiladas deben establecer controles para verificar periódicamente que el tercero receptor de datos cumpla los requisitos señalados en el subnumeral 2.1. del presente Capítulo durante la vigencia de la relación contractual. Dicha periodicidad debe ser razonable y definida por la entidad vigilada, atendiendo al perfil de riesgo del tercero receptor de datos y a las características de la relación con este.

2.4. Las entidades vigiladas deben dejar constancia de la verificación de los requisitos señalados en el subnumeral 2.1. del presente Capítulo por cada tercero receptor de datos con el que tengan una relación contractual, la cual debe quedar a disposición de la SFC.

2.5. En ningún caso las entidades vigiladas pueden restringir la vinculación de terceros receptores de datos que cumplan con lo establecido en el subnumeral 2.1. del presente Capítulo.

2.6. En el marco de las finanzas abiertas, las entidades vigiladas no pueden dar un trato discriminatorio a los terceros receptores de datos que vinculen. Para el efecto, deben abstenerse de incurrir en tratos discriminatorios relacionados, entre otros, con:

a) Los requisitos de vinculación de los terceros receptores de datos.

b) Los controles para monitorear el cumplimiento de los requisitos por parte del tercero receptor de datos, de acuerdo con lo previsto en el subnumeral 2.3 del presente Capítulo.

c) Las tarifas, precios, comisiones, cargos, cobros o cualquier otra retribución aplicable a los terceros receptores de datos.

3. ESTÁNDARES TECNOLÓGICOS Y DE SEGURIDAD

3.1. Principios generales

Las entidades vigiladas que participen en finanzas abiertas deben contar con políticas, procedimientos y recursos técnicos y humanos para monitorear que los datos personales de los consumidores financieros se traten en condiciones de seguridad. Para el efecto, las entidades vigiladas deben cumplir con las siguientes instrucciones:

a) Mantener los sistemas relacionados con finanzas abiertas en una red interna separada lógicamente de las demás redes.

b) Monitorear que la información que circula en el marco de las finanzas abiertas se ajuste a las especificaciones establecidas entre las entidades vigiladas y los terceros receptores de datos.

c) Abstenerse de exponer públicamente los repositorios de información que se utilicen para el desarrollo de las finanzas abiertas.

d) Mantener registros de auditoría de información (*logs*), por el término de 5 años, por cada solicitud de datos realizada en desarrollo de las finanzas abiertas que permitan determinar, como mínimo: el origen desde el cual se realizó la solicitud, el momento en el que se realizó el consumo de la información, el usuario que ejecutó la solicitud, la información objeto de circulación y el estado del proceso. En todo caso, según el nivel de criticidad de la información, esta se deberá enmascarar o cifrar.

e) Propender por la disponibilidad y accesibilidad de los sistemas de información en todo momento y contar con mecanismos de redundancia, balanceo de carga y tolerancia a fallos para garantizar su disponibilidad continua.

3.2. Estándares de arquitectura, seguridad y tecnología

Las entidades vigiladas deben implementar protocolos de intercambio automático de información para atender las solicitudes de acceso a datos personales presentadas por los terceros receptores de datos en el desarrollo de las finanzas abiertas. Los protocolos de intercambio automático de información que implementen las entidades vigiladas en desarrollo de las finanzas abiertas deben cumplir, como mínimo, con los siguientes requisitos:

3.2.1. En materia de arquitectura:

a) Ejecutar el intercambio de información bajo el formato JSON (JavaScript Object Notation).

b) Cumplir con el marco de referencia REST y su implementación debe ser RESTful.

3.2.2. En materia de administración de datos, cumplir con el estándar ISO 20022 en lo relacionado con el diccionario de datos y utilizar el diccionario de campos que establece el referido estándar. El cumplimiento del referido estándar aplicará en aquellos campos financieros que corresponda.

3.2.3. En materia de seguridad:

a) Cumplir con el marco FAPI 2.0 desarrollado por The OpenID Foundation (OIDF) para los perfiles de seguridad.

b) Ejecutar la autorización sobre el protocolo OAuth 2.0 desarrollado por el IETF OAuth Working Group. Para el efecto, se debe hacer uso de mecanismos seguros para la implementación del Token de Acceso (Access Token), tales como: Client Credentials (RFC 6749), Authorization Code (RFC 6749), Authorization Code con PKCE (RFC 7636) o Refresh Token (RFC 6749), entre otros. El Token de Acceso debe generarse haciendo uso del estándar JWT (JSON Web Token), debe firmarse utilizando algoritmos seguros tales como: PS256 o superiores, y debe utilizar private_key_jwt como método de autenticación.

c) Realizar el intercambio de información bajo el protocolo TLS garantizando el proceso de autenticación mutua o recíproca (mutual authentication), haciendo uso de certificados digitales vigentes, de acuerdo con lo establecido en la Ley 527 de 1999 y normas que la sustituyan, modifiquen o reglamenten, para

lo cual deben utilizar cualquiera de las siguientes suites de cifrado:

i) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
ii) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

En caso de que cualquiera de los formatos, marcos de referencia, estándares o protocolos establecidos en el numeral 3.2. sea declarado obsoleto por parte del organismo que lo establece o soporta, la entidad vigilada deberá adoptar aquel que lo modifique, sustituya o adicione.

4. TRATAMIENTO DE LOS DATOS PERSONALES DE LOS CONSUMIDORES FINANCIEROS EN FINANZAS ABIERTAS

4.1. En el marco de las finanzas abiertas, las entidades vigiladas deben cumplir con las siguientes obligaciones para el tratamiento de los datos personales de los consumidores financieros:

a) Verificar, de forma previa a la circulación de la información, que el tercero receptor de datos cuente con la autorización previa, expresa e informada del consumidor financiero para el tratamiento de sus datos personales.

b) Autenticar al consumidor financiero para realizar cualquier acción que busque otorgar, modificar y/o revocar su autorización de tratamiento de datos personales en el marco de las finanzas abiertas a través de mecanismos fuertes de autenticación de conformidad con lo dispuesto en el Capítulo I del Título II de la Parte I de la Circular Básica Jurídica, así como en el numeral 3 del artículo 2.17.4.1.3. del Decreto 2555 de 2010, y demás normas que lo modifiquen, sustituyan o adicionen.

c) Contar con la autorización previa, expresa e informada del consumidor financiero para el tratamiento de sus datos personales dando estricto cumplimiento a las Leyes 1266 de 2008 y 1581 de 2012, y demás normas que las reglamenten, modifiquen, sustituyan o adicionen. Para el efecto, la solicitud de autorización requerida al consumidor financiero debe estar expresada en forma sencilla, clara y precisa, de tal manera que sea de fácil comprensión, y debe contener, como mínimo, la siguiente información:

i) La identificación del tercero receptor de datos, indicando como mínimo su razón social y su domicilio.
ii) Los datos específicos cuyo tratamiento autoriza el consumidor financiero.
iii) El tratamiento al cual serán sometidos los datos personales del consumidor financiero por parte del tercero receptor de datos.
iv) La finalidad específica para la cual el consumidor financiero autoriza el tratamiento de sus datos personales. En el evento en que se vayan a comercializar los datos personales de los consumidores financieros, la solicitud de autorización debe advertir además de forma expresa dicha situación. Adicionalmente, debe informarse al consumidor financiero si se le remunerará por esta actividad, así como si trae consigo algún costo.
v) El tiempo de la finalidad para la cual el consumidor financiero autoriza el tratamiento de sus datos personales, de conformidad con el artículo 11 del Decreto 1377 de 2013 incorporado en el Decreto 1074 de 2015 y demás normas que las modifiquen, sustituyan o adicionen.

Las entidades vigiladas deben abstenerse de solicitar autorizaciones generales o abiertas que les impidan a los consumidores financieros conocer la finalidad, su término y el tratamiento que los terceros receptores de datos darán a los mismos.

En ningún caso las entidades vigiladas pueden condicionar la prestación de un producto o servicio financiero que no surja en desarrollo de las finanzas abiertas al otorgamiento de la autorización para el tratamiento de datos personales en el marco de las finanzas abiertas.

d) Permitir al consumidor financiero consultar de manera accesible y permanente las autorizaciones de que trata el literal c) del presente subnumeral.

e) Permitir al consumidor financiero revocar la autorización otorgada para el tratamiento de sus datos personales en el marco de las finanzas abiertas de la que trata el literal c) del presente subnumeral, cuando resulte aplicable de conformidad con las Leyes 1266 de 2008 y 1581 de 2012, y demás normas que las reglamenten, modifiquen, sustituyan o adicionen.

f) Permitir al consumidor financiero actualizar, en todo momento, la autorización otorgada para el tratamiento de sus datos personales en el desarrollo de las finanzas abiertas de la que trata el literal c) del presente subnumeral.

g) Permitir que el consumidor financiero se abstenga de autorizar el tratamiento de su información en el marco de las finanzas abiertas.

5. DEBERES DE REVELACIÓN DE INFORMACIÓN

Las entidades vigiladas que vinculen terceros receptores de datos en el marco de las finanzas abiertas deben publicar, en una sección de fácil acceso en su página web, la información actualizada que le permita a los consumidores financieros conocer las condiciones de implementación de las finanzas abiertas, sin perjuicio de que lo hagan en cualquier canal adicional.

Para el efecto, las entidades vigiladas deben informar de forma sencilla, clara y precisa, como mínimo, los siguientes aspectos:

a) El procedimiento para consultar de manera accesible y permanente las autorizaciones otorgadas para el tratamiento de los datos personales del consumidor financiero de que trata el literal c) del subnumeral 4.1. del presente Capítulo.

b) El procedimiento para actualizar la autorización para el tratamiento de los datos personales del consumidor financiero.

c) El procedimiento para revocar la autorización para el tratamiento de los datos personales del consumidor financiero cuando resulte aplicable de conformidad con las Leyes 1266 de 2008 y 1581 de 2012, y demás normas que las reglamenten, modifiquen, sustituyan o adicionen.

d) La información actualizada de contacto de los terceros receptores de datos para la atención de consultas y reclamos presentados por los consumidores financieros como titulares de los datos.

e) Los canales dispuestos por la entidad vigilada para la atención de consultas y reclamos relacionados con el tratamiento de los datos personales del consumidor financiero, de conformidad con lo dispuesto en la normativa aplicable.

f) Los procedimientos que permitan la supresión de los datos personales de los consumidores financieros, según aplique, de conformidad con la normatividad vigente.

De igual forma, las entidades vigiladas deben adelantar programas de educación financiera para informar a los consumidores financieros sobre los derechos, obligaciones y responsabilidades derivados del tratamiento de sus datos en el marco de las finanzas abiertas.

PARTE I
INSTRUCCIONES GENERALES APLICABLES A LAS ENTIDADES VIGILADAS

TÍTULO I
ASPECTOS GENERALES

CAPÍTULO X. COMERCIALIZACIÓN DE TECNOLOGÍA E INFRAESTRUCTURA A TERCEROS

CONTENIDO

1. ÁMBITO DE APLICACIÓN

2. REGLAS PARA LA COMERCIALIZACIÓN DE TECNOLOGÍA E INFRAESTRUCTURA A TERCEROS

PARTE I
INSTRUCCIONES GENERALES APLICABLES A LAS ENTIDADES VIGILADAS

TÍTULO I
ASPECTOS GENERALES

CAPÍTULO X. COMERCIALIZACIÓN DE TECNOLOGÍA E INFRAESTRUCTURA A TERCEROS

1. ÁMBITO DE APLICACIÓN

Las entidades vigiladas por la Superintendencia Financiera de Colombia que comercialicen a terceros y entidades vigiladas la tecnología e infraestructura que utilizan o hayan utilizado para el ofrecimiento o prestación de sus servicios y desarrollo de sus actividades conexas, de conformidad con el artículo 2.35.9.3.1. del Decreto 2555 de 2010, incorporado por el Decreto 1297 de 2022, deben cumplir las instrucciones previstas en el presente Capítulo.

2. REGLAS PARA LA COMERCIALIZACIÓN DE TECNOLOGÍA E INFRAESTRUCTURA A TERCEROS

La tecnología e infraestructura objeto de comercialización debe corresponder a aquella que haya sido o sea utilizada por la entidad vigilada para el ofrecimiento o prestación de sus servicios y desarrollo de sus actividades conexas, con independencia de si ha sido desarrollada por esta o por un tercero.

La junta directiva o el órgano que haga sus veces de las entidades vigiladas que lleven a cabo la actividad de comercialización de tecnología e infraestructura a terceros debe definir las políticas para el desarrollo de esta actividad y la gestión de los riesgos derivados de la misma. Además, corresponde a las entidades vigiladas definir y adoptar procedimientos para verificar las condiciones, términos y requisitos bajo los cuales se desarrolla esta actividad.

Las entidades vigiladas deben dar cumplimiento a las siguientes instrucciones:

a) Evaluar de forma previa a la celebración del contrato los riesgos asociados a la comercialización de tecnología e infraestructura a terceros.

b) Establecer salvaguardas, tales como seguros o garantías, para cubrir el riesgo de incumplimiento de las obligaciones derivadas de los contratos.

c) Administrar el riesgo reputacional asociado al uso del nombre o imagen de la entidad vigilada por parte de quienes adquieran o usen la tecnología o infraestructura.

d) Administrar el riesgo sistémico asociado a la falla de la tecnología o infraestructura objeto de la comercialización, en el evento en que dicha tecnología o infraestructura haya sido adquirida por otras entidades vigiladas.

e) Implementar controles de calidad sobre la tecnología e infraestructura objeto de la comercialización.

Las entidades vigiladas deben dejar constancia de la verificación de los requisitos establecidos en el presente numeral, y dicha constancia debe quedar a disposición de la SFC. Adicionalmente, las entidades vigiladas mantendrán a disposición de esta Superintendencia los documentos en los cuales consten las condiciones, términos y requisitos bajo los cuales desarrollan la actividad de comercialización de tecnología e infraestructura a terceros.

Las entidades vigiladas deben utilizar sus recursos propios para cubrir el incumplimiento de las obligaciones derivadas de los contratos mediante los cuales se instrumentaliza la comercialización.

004

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.

3.2.3.4 La información actualizada de los productos, canales, puntos de atención, servicios y tarifas, puede ser puesta a disposición de terceros desarrolladores de API (Application Programming Interface) o de cualquier otro mecanismo que permita el intercambio automático de información, en las condiciones que cada entidad determine y con la debida gestión de los riesgos asociados a este intercambio.

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.

Las entidades que presten servicios a través de corresponsales móviles deben implementar estrategias para informar a los consumidores financieros sobre la manera de identificarlos. Así mismo, deben contar con mecanismos que les permita a los clientes confirmar si quien ofrece el servicio está autorizado para tal propósito.

Para la prestación del servicio fuera de línea, las entidades deben informar a los consumidores financieros sobre esta alternativa, explicándoles las características de estas operaciones, las condiciones de registro de las mismas, y las medidas de seguridad que se deben adoptar para su realización.

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.

Para la prestación de servicios a través de corresponsales móviles, la entidad debe mantener, permanentemente y a disposición de los consumidores financieros, el listado actualizado de los corresponsales habilitados por la entidad para la prestación de servicios.

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 lacuenta 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. Para los pagos sin contacto no será obligatoria la entrega al cliente del soporte impreso de la operación, salvo que sea solicitado por el cliente.

Las operaciones que se realicen fuera de línea, a través de un corresponsal móvil, deben contar con un soporte físico que garantice el no repudio por parte de la entidad y que dé cuenta de la operación efectuada por el consumidor financiero. Dicho soporte debe contener al menos la fecha, hora, código del corresponsal, número de la operación, costo para el consumidor y tipo y monto de operación y debe servir como mecanismo de confirmación de la misma.

3.2.4.7. La prestación de servicios a través de corresponsales exige el diseño de una estrategia que le permita a la entidad

iv) Garantizar que la selección, aprobación, renovación y sustitución de sus miembros sea un proceso estratégico al interior de la EASPBV, y cuente con normas internas que establezcan los perfiles y calidades para ser miembro, los procesos de nominación y remoción, y esquemas de sustitución de liderazgo.

5. ACTIVIDADES CONEXAS DE LAS EASPBV

Las actividades conexas que desarrollen las EASPBV deben guardar relación directa con aquellas definidas en su objeto social exclusivo, consagrado en el parágrafo 1 del art. 2.17.2.1.1 del Decreto 2555 de 2010. Se consideran actividades conexas de las EASPBV aquellas que tienen como propósito mejorar, hacer más eficiente, agilizar, o fortalecer la seguridad de las siguientes actividades: i) compensación y liquidación, ii) provisión de servicios de pago por delegación de adquirentes o entidades emisoras, y iii) procesamiento de órdenes de pago o transferencia de fondos y suministro de tecnologías de corresponsales, puntos de recaudo y cajeros electrónicos.

6. ESTÁNDARES OPERATIVOS, TÉCNICOS Y DE SEGURIDAD

Las EASPBV deben definir requerimientos operativos, técnicos y de seguridad proporcionales al rol y a los riesgos inherentes a la actividad que cada uno de sus participantes ejecuta dentro del SPBV. Dichos requerimientos deben estar alineados con estándares internacionales y promover el cumplimiento de los principios definidos en el art. 2.17.1.1.2 del Decreto 2555 de 2010. Las EASPBV deben realizar, de manera previa, un análisis técnico que justifique y soporte los criterios empleados para la definición de tales requerimientos.

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

PARTE III
MERCADO DESINTERMEDIADO

TÍTULO IV
PROVEEDORES DE INFRAESTRUCTURA Y OTROS AGENTES

CAPÍTULO IX: ENTIDADES ADMINISTRADORAS DE SISTEMAS DE PAGO DE BAJO VALOR- EASPBV

CONTENIDO

1. AUTORIZACIÓN PARA EJERCER LA ACTIVIDAD DE COMPENSACIÓN Y LIQUIDACIÓN EN SISTEMAS DE PAGO DE BAJO VALOR

1.1 Autorización de los reglamentos de las EASPBV
1.2 Régimen de inversión en EASPBV

2. REGISTRO DE ADQUIRENTES NO VIGILADOS - RANV

2.1 Objeto y alcance del RANV
2.2 Requisitos y efectos de la Inscripción
2.3 Procedimiento de inscripción
2.3.1 Reglas relativas a la solicitud
2.3.2 Negación de la solicitud de inscripción

2.4 Reglas particulares de operación del registro
2.4.1 Remisión periódica de información
2.4.2 Cancelación de la inscripción
2.4.3 Publicidad del RANV y su contenido

3. OBLIGACIONES DE TRANSPARENCIA DE LOS ADQUIRENTES ENTIDADES RECEPTORAS

4.JUNTAS DIRECTIVAS DE LAS EASPBV

5. ACTIVIDADES CONEXAS DE LAS EASPBV

6. ESTÁNDARES OPERATIVOS, TÉCNICOS Y DE SEGURIDAD