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.

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.