**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. aspectos tecnológicos y de seguridad

# 4. tratamiento de LOS datos de LOS CONSUMIDORES FINANCIEROS en ecosistemas de 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**

# 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 SFC determina los estándares tecnológicos, de seguridad y demás necesarios para el desarrollo de los ecosistemas de finanzas abiertas regulados por el título 8 del Libro 35 de la Parte 2 del Decreto 2555 de 2010.**

# terceros receptores de datos

## Las entidades vigiladas que participen en ecosistemas de finanzas abiertas deben adoptar políticas y procedimientos que garanticen que los terceros receptores de datos cumplan los requisitos establecidos en el presente numeral. Dichas políticas deben ser aprobados por la junta directiva u órgano que haga sus veces. Adicionalmente, 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 de los consumidores financieros en el marco de los ecosistemas de finanzas abiertas.**

## Las entidades vigiladas deben verificar que los terceros receptores de datos cumplan con los siguientes requisitos:

#### **Estén inscritos en el Registro Nacional de Bases de Datos cuando se cumplan los presupuestos previstos en la Ley 1581 de 2012 y el Decreto 886 de 2014 compilado por el Decreto 1074 de 2015, y normas que las modifiquen o sustituyan. En el evento en cual los terceros receptores de datos no deban inscribirse en el registro mencionado, las entidades vigiladas deben verificar que los mismos cuenten con políticas y procedimientos que garanticen el tratamiento de los datos atendiendo lo establecido en las normas relacionadas con habeas data y protección de datos de que tratan las Leyes 1266 de 2008 y 1581 de 2012, y normas que las reglamenten, modifiquen, sustituyan o adicionen.**

#### **Cuenten con procedimientos para la atención de consultas y reclamos relacionados con las normas señaladas en el literal anterior.**

#### **Cuenten con mecanismos que les permitan: i) tratar de forma segura los datos, y ii) mitigar los riesgos asociados al tratamiento de la información, en particular, el de ciberseguridad y fallas en la infraestructura, tecnología y sistemas en los que se almacene la información. Para el efecto, los terceros receptores que tengan la calidad de entidad vigilada deberán dar cumplimiento a las instrucciones en materia de seguridad de la información y ciberseguridad previstas en el Capítulo V del Título IV de la Parte I de presente Circular. En caso contrario, las entidades vigiladas deben verificar que los terceros receptores tengan vigente, como mínimo, con la certificación ISO 27001. En adición a lo anterior, podrán tener en cuenta marcos de referencia tales como: NIST *Cybersecurity Framework* u OWASP ASVS última versión, o cualquiera que los modifique, sustituya o adicione.**

#### **Cuenten con procedimientos para la supresión de los datos de los consumidores financieros, de conformidad con las normas aplicables.**

## Las entidades vigiladas deben cumplir las instrucciones del Capítulo IV del Título IV de la Parte I de la Circular Básica Jurídica frente a los terceros receptores de datos. Para el efecto, los terceros receptores de datos se entenderán como proveedores.

## Las entidades vigiladas deben establecer controles para verificar que el tercero receptor de datos cumpla de manera permanente los requisitos antes señalados durante la vigencia de la relación contractual.

## Las entidades vigiladas deben dejar constancia de la verificación de los requisitos establecidos en el presente numeral por cada tercero receptor de datos, la cual debe quedar a disposición de la SFC.

## En ningún caso las entidades vigiladas pueden restringir la vinculación de terceros receptores de datos que cumplan con lo establecido en el numeral 2 del presente Capítulo.

## Las entidades vigiladas no pueden dar un trato discriminatorio a los terceros receptores de datos.

# aspectos tecnológicos y de seguridad

**Las entidades vigiladas deben implementar interfaces de programación de aplicaciones (API, por sus siglas en inglés) para atender las solicitudes de acceso a datos presentadas por los terceros receptores de datos en el desarrollo de ecosistemas de finanzas abiertas. En ningún caso las entidades vigiladas podrán utilizar mecanismos diferentes a las API.**

## Las API que implementen las entidades vigiladas en desarrollo de los ecosistemas de finanzas abiertas deben cumplir, como mínimo, con los siguientes requisitos:

### En materia de arquitectura:

#### **Ejecutar el intercambio de datos bajo el formato JSON.**

#### **Cumplir con el marco de referencia REST y su implementación debe ser RESTful.**

### En materia de administración de datos, cumplir con el estándar ISO 20022 última versión, o cualquiera que lo modifique, sustituya o adicione, en lo relacionado con el diccionario de datos y utilizar el diccionario de campos que establece el referido estándar.

### En materia de seguridad:

#### **Ejecutar la autorización sobre el protocolo OAuth 2.0 última versión, o cualquiera que lo modifique, sustituya o adicione, desarrollado por el IETF OAuth Working Group. 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, últimas versiones o cualquiera que los modifique, sustituya o adicione. El Token de Acceso deberá generarse haciéndose uso del estándar JWT (JSON Web Token) y firmarlo utilizando algoritmos seguros tales como RS256 o superiores.**

#### **Cumplir con el marco FAPI 2.0 última versión, o cualquiera que lo modifique, sustituya o adicione, desarrollado por The OpenID Foundation (OIDF, por sus siglas en inglés) para los perfiles de seguridad.**

#### **Realizar el intercambio de información bajo el protocolo TLS última versión, o cualquiera que lo modifique, sustituya o adicione y garantizando el proceso de autenticación mutua o recíproca (mutual authentication).**

#### **Contar con certificados digitales vigentes, de acuerdo con lo establecido en la Ley 527 de 1999 y normas que la sustituyan, modifiquen o reglamenten.**

## Las entidades vigiladas deben contar con políticas, procedimientos y recursos técnicos y humanos para monitorear que las solicitudes de datos presentadas a través de API se realicen en condiciones de seguridad. Para el efecto, las entidades vigiladas deben dar cumplimiento, como mínimo, a las siguientes instrucciones:

#### **Mantener los sistemas relacionados con los ecosistemas de finanzas abiertas y las API en una red interna independiente de los demás sistemas de información.**

#### **Monitorear la información que circula a través de las API, para lo cual deben verificar y garantizar que las especificaciones de los campos de las solicitudes de datos de la API y sus respuestas se ajusten a las definiciones establecidas entre las entidades vigiladas y los terceros receptores de datos.**

#### **Abstenerse de exponer públicamente los repositorios de información a los que tienen acceso las API.**

#### **Mantener *logs*, por el término de 5 años, por cada solicitud de datos realizada a través de las API, las cuales deben contener la información necesaria para determinar, como mínimo: el origen desde el cual se realizó la solicitud, el momento en que se realizó el consumo, el usuario que lo ejecutó, la información que circula por la API y el estado del proceso. En todo caso, según el nivel de sensibilidad o criticidad de la información esta se deberá enmascarar.**

# tratamiento de LOS datos de LOS CONSUMIDORES FINANCIEROS en ecosistemas de finanzas abiertas

## En el marco de los ecosistemas de finanzas abiertas, las entidades vigiladas deben cumplir, como mínimo, con las siguientes obligaciones para el tratamiento de los datos de los consumidores financieros:

#### **Autenticar al consumidor financiero para realizar cualquier acción que busque otorgar, modificar y revocar su autorización de tratamiento de datos personales en el ecosistema de finanzas abiertas a través de mecanismos fuertes de autenticación, en los términos del Capítulo I del Título II de la Parte I de la Circular Básica Jurídica.**

#### **Contar o verificar que el tercero receptor de datos cuente con la autorización previa, expresa e informada del consumidor financiero para el tratamiento de sus datos dando estricto cumplimiento a las Leyes 1266 de 2008 y 1581 de 2012, y 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. De igual forma, debe contener, como mínimo, la siguiente información:**

##### La identificación del tercero receptor de datos, indicando como mínimo su razón social y su domicilio.

##### Los datos específicos cuyo tratamiento autoriza el consumidor financiero.

##### El tratamiento al cual serán sometidos los datos del consumidor financiero por parte del tercero receptor de datos.

##### La finalidad específica para la cual el consumidor financiero autoriza el tratamiento de sus datos. En el evento en que se vayan a comercializar los datos, la solicitud de autorización debe advertir además de forma expresa dicha situación.

##### El tiempo de la finalidad para la cual el consumidor financiero autoriza el tratamiento de sus datos de conformidad con el artículo 11 del Decreto 1377 de 2013 incorporado en el Decreto 1074 de 2015 y 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 al otorgamiento de la autorización para el tratamiento de datos personales en el marco de los ecosistemas de finanzas abiertas.**

#### **Permitir que los consumidores financieros se abstengan de autorizar el tratamiento de su información en el marco de los ecosistemas de finanzas abiertas.**

#### **Permitir o verificar que el tercero receptor de datos permita al consumidor financiero consultar de manera accesible y permanente las autorizaciones otorgadas para el tratamiento de sus datos personales en el marco de los ecosistemas de finanzas abiertas.**

#### **Contar o verificar que el tercero receptor cuente con un procedimiento de revocatoria de la autorización otorgada por el consumidor financiero para el tratamiento de sus datos en el marco de los ecosistemas de finanzas abiertas y garantizar que dicho procedimiento se pueda realizar en cualquier momento. Este procedimiento debe ser transparente, accesible, y de fácil entendimiento y ejecución.**

# DEBERES DE REVELACIÓN DE información

**Las entidades vigiladas deben publicar en el portal de inicio de su página web la información que le permita a los consumidores financieros conocer las condiciones de implementación de los ecosistemas de 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:**

#### **El contenido de la autorización previa y expresa para el tratamiento de los datos que deben otorgar los consumidores financieros, haciendo especial énfasis en la finalidad del tratamiento, su término y uso de la información.**

#### **El procedimiento para consultar de manera accesible y permanente la autorización otorgada para el tratamiento de los datos del consumidor financiero.**

#### **El procedimiento para revocar la autorización para el tratamiento de los datos del consumidor financiero.**

#### **Los datos de contacto de los terceros receptores de datos, así como los canales dispuestos por estos.**

#### 

#### **Los canales dispuestos por la entidad vigilada para la atención de consultas y reclamos relacionados con el tratamiento de los datos, de conformidad con lo dispuesto en la normativa aplicable.**

#### **Los procedimientos que permitan la supresión de los datos de los consumidores financieros, según aplique, conforme a 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 los ecosistemas de finanzas abiertas.**