TABLA DE CONTENIDO

1. Objetivo

Establecer las directrices y definiciones necesarias para garantizar la protección de los datos personales de los consumidores financieros en el marco del Modelo Operativo de Finanzas Abiertas. Este lineamiento busca asegurar el cumplimiento de las normativas vigentes en materia de protección de datos, promoviendo la transparencia y el ejercicio adecuado de los derechos de los titulares de la información.

2. Alcance

El presente documento abarca todas las etapas del tratamiento de datos personales en el contexto del Modelo Operativo de Finanzas Abiertas. Inicia con la verificación de la autorización previa del consumidor financiero y culmina con el ejercicio de derechos sobre dicha autorización, incluyendo la autorización de tratamiento de datos cuando el banco actúe como Tercero Receptor de Datos (TRD).

3. Protección de datos finanzas abiertas

A continuación, se relacionan los componentes de privacidad y protección de datos que se deben tener en cuenta en el modelo operativo de finanzas abiertas, según lo establecido en la Circular 004 de 2024 de la SFC, modelo en el cual, a través de la arquitectura tecnológica se garantice que con la API contratada se asegura el adecuado consentimiento del titular de los datos, así como los procedimientos de autenticación, para garantizar la seguridad en la operación.

3.1. Verificación de la Autorización Previa del Consumidor Financiero

Objetivo: Se debe asegurar que el tercero receptor de los datos cuente con la autorización previa, expresa e informada del consumidor financiero para el tratamiento de sus datos personales.

Requerimiento:

I. Verificación del consentimiento:

El área de Arquitectura TIC deberá garantizar que con el proceso de apificación1 contratada por el Banco para el marco de finanzas abiertas, antes del suministro de información al Tercero Receptor de Datos, se debe verificar que este tercero acredite la autorización previa, expresa e informada del consumidor financiero para el tratamiento de sus datos.

(1) Apificación es un modelo de negocio que consta en vender datos como un servicio a través de APIs (Application Programming Interface) con el fin de ser utilizados para crear nuevos productos o servicios digitales

II. Registro y Archivo:

El área de Arquitectura TIC deberá garantizar que con el proceso de apificación contratada por el Banco para el marco de finanzas abiertas, se disponga un registro electrónico de la verificación del consentimiento otorgado al tercero receptor de datos, el cual debe alojarse en un log que dé cuenta de la documentación de la autorización de manera segura y accesible para futuras auditorías o PQRS.

3.2. Autenticación del Consumidor Financiero

Objetivo: Se debe garantizar la autenticación del consumidor financiero para otorgar, modificar o revocar su autorización de tratamiento de datos mediante mecanismos fuertes.

Requerimiento:

I. Implementación de Mecanismos de Autenticación:

El área líder de finanzas abiertas en el Banco deberá asegurar que, para otorgar, modificar y/o revocar su autorización de tratamiento de datos se requerirán mecanismos de autenticación conforme a lo dispuesto en el Capítulo I del Título II de la Parte I de la Circular Básica Jurídica y el numeral 3 del artículo 2.17.4.1.3. del Decreto 2555 de 2010.

II. Proceso de Autenticación:

El área líder de finanzas abiertas en el Banco deberá asegurar que la verificación de la identidad del consumidor financiero se realice mediante factores de autenticación según lo establecido el Circular Básica Jurídica, siguiendo los requerimientos de las áreas de seguridad de información y ciberseguridad, así como los procesos actuales con los que cuenta el Banco.

III. Registro de Autenticaciones:

El área líder de finanzas abiertas en el Banco deberá asegurar que se cuente con un registro de cada autenticación realizada en una base de datos segura y auditable, para su consulta posterior.

3.3. Obtención de la Autorización Previa, Expresa e Informada

Objetivo: Contar con la autorización previa, expresa e informada del consumidor financiero para el tratamiento de sus datos personales por parte del Banco en el esquema de finanzas abiertas.

Requerimiento:

I. Disposición de la autorización para el tratamiento de datos:

El área líder de finanzas abiertas en el Banco deberá asegurar que, en el modelo operativo de suministro de información a los TRD, de forma previa a este, el consumidor financiero otorgue la autorización de tratamiento de datos al Banco, la cual debe disponerse de forma previa, clara y precisa, para su acceso, comprensión y emisión del consentimiento.

II. Información que debe contener la autorización:

El área de Arquitectura TIC deberá garantizar que con el proceso de apificación contratada por el Banco para el marco de finanzas abiertas, se disponga que en el proceso de redireccionamiento del TRD al Banco, para cada caso de llamado de API, en la confirmación de la autorización de tratamiento de datos en instancia Banco se incluya la siguiente información:

- Identificación del tercero receptor de datos (razón social y domicilio).
- Datos específicos cuyo tratamiento se autoriza.
- Tratamiento al cual serán sometidos los datos.
- Finalidad específica del tratamiento.
- Por cuánto tiempo se realizará el tratamiento de los datos
- Advertencia sobre la comercialización de los datos, si aplica.
- Información sobre remuneración o costos relacionados.

III. Registro y Almacenamiento de la Autorización:

El área de Arquitectura TIC deberá garantizar que la confirmación de la autorización sea almacenada de electrónica a través de Log, la que dé cuenta de la elección, fecha y hora del otorgamiento.

Almacenar la información relacionada de manera segura y accesible.

3.4. Ejercicio de Derechos sobre la Autorización de Tratamiento de Datos

Objetivo: Permitir al consumidor financiero consultar de manera accesible y permanente, revocar, y actualizar las autorizaciones otorgadas, así como tener la posibilidad de abstenerse de autorizar el tratamiento de la autorización en el marco de finanzas abiertas.

Requerimiento:

I. Desarrollo de la instancia para el ejercicio de los derechos

Implementar una instancia en el modelo operativo de finanzas abiertas para que el consumidor financiero pueda realizar el ejercicio de sus derechos de habeas data, garantizando que el consumidor pueda ingresar, autenticarse, y realizar la actividad que requiera de forma digital, en línea y garantizando su operación inmediata.

II. Acceso Seguro:

Hay que asegurar que el acceso a la instancia dispuesta esté protegido mediante mecanismos de autenticación robustos.

Verificar la identidad del solicitante mediante mecanismos de autenticación.

III. Mantenimiento de la Plataforma:

Actualizar y mantener la plataforma para garantizar su disponibilidad y accesibilidad.

IV. Proceso de ejercicio de derechos

Registrar el ejercicio de derecho (consultar de manera accesible y permanente, revocar, y actualizar las autorizaciones otorgadas, así como tener la posibilidad de abstenerse de autorizar el tratamiento de la autorización), y procesarlo.

Notificar al tercero receptor de datos sobre el ejercicio de derecho (consultar de manera accesible y permanente, revocar, y actualizar las autorizaciones otorgadas, así como tener la posibilidad de abstenerse de autorizar el tratamiento de la autorización), y asegurar la cesación del tratamiento de los datos o la parametrización del tratamiento.

3.5. Autorización de Tratamiento de Datos Cuando el Banco sea TRD

Objetivo: Disponer en el modelo operativo de finanzas abiertas en el escenario en el que el Banco actúa como TRD, la autorización de tratamiento de datos de la entidad para que el consumidor pueda emitir su consentimiento.

Requerimiento:

El área líder de finanzas abiertas en el Banco deberá asegurar que, en el escenario de solicitud de información a otras entidades, se disponga de forma adecuada la autorización de tratamiento de datos del Banco según el modelo que se ha proyectado y que se remite adjunto. * Este se actualizará según la reglamentación de la SFC.

El área de Arquitectura TIC deberá garantizar que la emisión del consentimiento respecto de los datos a tratar, tiempo, finalidades, y entidad que tiene los datos, se realice de forma satisfactoria y conforme con el consentimiento del titular.