Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Estudio para Elaborar Recomendaciones en Materia de Protección de Datos Personales para Instituciones de Tecnología Financiera

"Informe Final"

Elaborado por Davara Abogados

Diciembre, 2019

Elaborado por Davara Abogados:

Isabel Davara F. de Marcos (Coordinadora)
Gregorio Barco Vega
Alexis Cervantes Padilla
Paulina Islas Huacuja
José de la Luz López Santiago

Contenido

I. Abreviaturas empleadas

Abreviatura	Significado
API	Interfaz de Programación de Aplicaciones (del inglés API: Application Programming Interface)
BANXICO	Banco de México
CLABE	Clave Bancaria Estandarizada
CNBV	Comisión Nacional Bancaria de y de Valores
CONDUSEF	Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros
CPEUM	Constitución Política de los Estados Unidos Mexicanos
CPF	Código Penal Federal
CUITF o Disposiciones	Disposiciones de carácter general aplicables a las Instituciones de Tecnología Financiera
Derechos ARCO	Derechos de Acceso, Rectificación, Cancelación y Oposición
DCGA58	Disposiciones de carácter general a que se refiere el artículo 58 de la Ley para Regular las Instituciones de Tecnología Financiera, emitidas por la Secretaría de Hacienda y Crédito Público
DCGCONDUSEF	Disposiciones de carácter general de la CONDUSEF en materia de transparencia y sanas prácticas aplicables a las instituciones de tecnología financiera
DCGMP	Disposiciones de carácter general en materia de publicidad y promoción de los Sistemas de Ahorro para el Retiro
DLLS	Dólares de los EE. UU. A.
DOF	Diario Oficial de la Federación.
FPE	Fondos de Pago Electrónico
IFC	Institución de Financiamiento Colectivo.
IFPE	Institución de Fondos de Pago Electrónico que se pretenda organizar y operar.
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
ITF	Institución de Tecnología Financiera
LAP	Lineamientos del Aviso de Privacidad
LD/FT	Lavado de dinero y financiamiento al terrorismo
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares
LIC	Ley de Instituciones de Crédito
LTOSF	Ley para la Transparencia y Ordenamiento de los Servicios Financieros
LPDUSF	Ley de Protección y Defensa al Usuario de Servicios Financieros
OBS	Open Banking Standard o Estándar de Banca Abierta en español
OBWG	Open Banking Working Group
ODI	Open Data Institute
PLD/CFT	Prevención de lavado de dinero y combate al financiamiento al terrorismo
LRITF o Ley FinTech	Ley para Regular las Instituciones de Tecnología Financiera
RLFPDPPP	Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares
SHCP	Secretaría de Hacienda y Crédito Público
2FA	Doble factor de autenticación

II. Introducción

Este documento conforma el Informe Final del Estudio para Elaborar Recomendaciones en Materia de Protección de Datos Personales para Instituciones de Tecnología Financiera (en adelante "Estudio") y tiene como propósito presentar una síntesis de los resultados obtenidos a partir del Estudio y que se han concretado en la identificación de procesos, tratamientos y riesgos relacionados en materia de protección de datos personales en las ITF. [1]

El Estudio sintetiza y ordena los dos componentes fundamentales que lo integran a partir de sus elementos esenciales:

- *Entregable 1.* En esta parte del Estudio se realizó una identificación de los distintos procesos y subprocesos relacionados con las operaciones realizadas por las ITF reguladas por la LRITF, es decir, las instituciones identificadas bajo los acrónimos de IFC e IFPE.
- *Entregable 2.* Este componente del Estudio se conformó de dos partes diferenciadas e interrelacionadas:
    - *Identificación de tratamientos de datos personales.* A partir de los distintos procesos y subprocesos identificados en el Entregable 1 se identificaron los distintos tratamientos de datos personales presentes en las ITF (IFC e IFPE) considerando el ciclo de vida de los datos personales tratados en dichas instituciones.
    - *Identificación de riesgos de seguridad y cumplimiento a la normatividad en las ITF.* En este parte del entregable 2 se identificaron los riesgos en materia de seguridad de datos personales en las ITF, así como los riesgos relacionados con el incumplimiento del marco normativo aplicable a las ITF que podrían presentarse en estas últimas.

Finalmente, es importante destacar que, dada la naturaleza y alcance del Estudio también se acompaña una síntesis de los distintos aspectos teóricos presentes en los Entregables 1 y 2.2.

Por último, en la sección final de este documento se señalan las conclusiones derivadas del Estudio.

III. Objetivo

Este documento tiene como propósito presentar un Informe final de los entregables 1 y 2 que conformaron el Estudio relativo a las recomendaciones en materia de protección de datos personales en las ITF.

Como objetivos del Estudio se pueden destacar los siguientes:

- Identificar los tratamientos de datos personales que se realizan a través de los procesos y operaciones que realizan las ITF.
- Evaluar el estado y cumplimiento de las obligaciones establecidas en la LFPDPPP y su Reglamento por parte de las ITF.
- Identificar los riesgos en materia de seguridad de datos personales con relación a los tratamientos que realizan las ITF.
- Desarrollar un Informe Final con conclusiones para identificar áreas de oportunidad en materia de datos personales en las ITF.

[1] Al respecto es importante señalar que la LRITF reconoce a las instituciones de financiamiento colectivo (IFC) y a las instituciones de fondos de pago electrónico como instituciones de tecnología financiera.

IV. Alcance

Este documento se enfoca en el análisis de procesos, tratamientos de datos personales y riesgos relacionados, exclusivamente, **con la operación de las ITF reguladas en la LRITF**. Al respecto, debe tenerse presente que la LRITF reconoce a dos tipos de instituciones de tecnología financiera: IFPE e IFC.

V. Metodología

La elaboración de los entregables 1 y 2 partió de un análisis normativo comprehensivo a partir del cual se consideró como punto de partida la recepción legal del término ITF y su distinción en dos instituciones principales: las IFC y las IFPE. En virtud de lo anterior, se procedió a analizar los distintos procesos que involucran el tratamiento de datos personales en ambas instituciones reguladas por la LRITF y de forma posterior se identificaron los tratamientos y riesgos derivados de su operación.

Para realizar la identificación de los tratamientos de datos personales existentes en las ITF se parte del estudio de los distintos procesos existentes en dichas instituciones.

Para lograr lo anterior, se realizó un análisis integral de la LFPDPPP, el RLFPDPPP, la RITF, la CUITF, las DCGA58, las DCGCONDUSEF, entre otras disposiciones de aplicación para las ITF.

VI. Delimitación conceptual

Como se mencionó en el entregable 1, respecto del significado y alcance del término FinTech se debe señalar que se trata de un concepto dinámico y en un proceso de constante discusión. Por ello, a la fecha no existe una definición unánime sobre cuál es su significado concreto.

No obstante, se suele aceptar que el término FinTech se deriva de los términos, en inglés, *finance* y *technology* haciendo referencia a una multitud de servicios financieros que se apoyan en la tecnología.

Así, se distingue un ecosistema financiero complejo en el que participan diversas organizaciones que proveen servicios financieros apoyados en la tecnología existente y de lo que se derivan distintos servicios, entornos o plataformas.

A partir de la LRITF en México podemos distinguir como instituciones reguladas las ITF que se dividen a su vez en IFPE e IFC. No obstante, pese a ser ejemplar, esta Ley no regula todos los servicios FinTech sino exclusivamente aquellos ofertados por las IFPE y las IFC.

Por lo anterior, se puede señalar que ITF no es sinónimo de FinTech, ya que las ITF son un subconjunto del ecosistema FinTech. Toda ITF es FinTech, pero no todo FinTech es ITF. Las ITF son una ficción jurídica que crea la LRITF que hace referencia a las entidades reguladas (IFC e IFPE) bajo los distintos esquemas previstos en la Ley FinTech, los cuales regulan ciertos servicios ofrecidos en el segmento FinTech; sin embargo, no ofrecen el universo de servicios que FinTech implica.

La Ley Fintech, en consecuencia, regula y reconoce a las siguientes instituciones jurídicas:

- *IFC*: Son las que de conformidad con el artículo 15 de la LRITF pueden realizar actividades destinadas a poner en contacto a personas del público en general, con el fin de que entre ellas se otorguen financiamientos mediante alguna de las operaciones señaladas en el artículo 16 del citado ordenamiento (*financiamiento colectivo de deuda, financiamiento colectivo de capital y financiamiento colectivo de copropiedad o regalías*), realizadas de manera habitual y

profesional, a través de aplicaciones informáticas, interfaces, páginas de internet o cualquier otro medio de comunicación electrónica o digital.

- *IFPE*: Son las personas morales autorizadas por la CNBV, previo acuerdo del Comité Interinstitucional al que hace referencia la LRITF, para prestar de forma habitual y profesional los servicios de emisión, administración, redención y transmisión de fondos de pago electrónico a través de aplicaciones informáticas, interfaces, páginas de internet o cualquier otro medio de comunicación electrónica o digital.

Además, otro de los grandes logros de la LRITF fue consagrar el movimiento a nivel mundial de *"Open Banking"* (que correctamente para el caso de México se le debería llamar *"Open Finance"*). Esta figura se regula en el ordenamiento mexicano a través del artículo 76, el cual impone a las Entidades Financieras[2], a los transmisores de dinero, a las sociedades de información crediticia, a las cámaras de compensación, a las ITF y a las sociedades autorizadas para operar con Modelos Novedosos[3] la obligación de establecer interfaces de programación de aplicaciones informáticas estandarizadas que posibiliten la conectividad y acceso de otras interfaces desarrolladas o administradas por los mismos sujetos a que se refiere este artículo y terceros especializados en tecnologías de la información, con el fin de compartir los datos financieros abiertos[4], datos agregados[5] y datos transaccionales[6].

En consecuencia, es posible señalar que derivado de la regulación existente se pueden distinguir dos instituciones reguladas: las IFPE e IFC, las cuales se toman como referencia para la identificación de procesos y subprocesos que se relacionan con el tratamiento de datos personales para el presente estudio.

---

[2] De acuerdo con la fracción XII del artículo IV de la LRITF se entiende por Entidades Financieras a las sociedades controladoras y subcontroladoras de grupos financieros, instituciones de crédito, casas de bolsa, bolsas de valores, sociedades operadoras de fondos de inversión, sociedades distribuidoras de acciones de fondos de inversión, uniones de crédito, organizaciones auxiliares del crédito, casas de cambio, sociedades financieras de objeto múltiple, sociedades financieras populares, sociedades financieras comunitarias con niveles de operaciones I a IV, organismos de integración financiera rural, sociedades cooperativas de ahorro y préstamo con niveles de operación I a IV, instituciones para el depósito de valores, contrapartes centrales de valores, instituciones calificadoras de valores, sociedades de información crediticia, instituciones de seguros, instituciones de fianzas, sociedades mutualistas de seguros, administradoras de fondos para el retiro, así como otras instituciones y fideicomisos públicos que realicen actividades respecto de las cuales la CNBV, la CNSF o la CONSAR ejerzan facultades de supervisión;

[3] *Vid*, Artículo 76.- Las Entidades Financieras, los transmisores de dinero, las sociedades de información crediticia, las cámaras de compensación a que se refiere la Ley para la Transparencia y Ordenamiento de los Servicios Financieros, las ITF y las sociedades autorizadas para operar con Modelos Novedosos estarán obligadas a establecer interfaces de programación de aplicaciones informáticas estandarizadas que posibiliten la conectividad y acceso de otras interfaces desarrolladas o administradas por los mismos sujetos a que se refiere este artículo y terceros especializados en tecnologías de la información, con el fin de compartir los datos e información siguiente:

I. Datos financieros abiertos: son aquellos generados por las entidades mencionadas en el primer párrafo de este artículo que no contienen información confidencial, tales como información de productos y servicios que ofrecen al público general, la ubicación de sus oficinas y sucursales, cajeros automáticos u otros puntos de acceso a sus productos y servicios, entre otros y según sea aplicable;

II. Datos agregados: son los relativos a cualquier tipo de información estadística relacionada con operaciones realizadas por o a través de las entidades mencionadas en el primer párrafo de este artículo, sin contener un nivel de desagregación tal que puedan identificarse los datos personales o transacciones de una persona.

Solamente tendrán acceso a los datos agregados las personas que cuenten con los mecanismos de autenticación que establezcan las Comisiones Supervisoras, o el Banco de México para el caso de las cámaras de compensación y sociedades de información crediticia a que se refiere el primer párrafo de este artículo, mediante disposiciones de carácter general que para tal efecto emitan, y

III. Datos transaccionales: son aquellos relacionados con el uso de un producto o servicio, incluyendo cuentas de depósito, créditos y medios de disposición contratados a nombre de los clientes de las entidades mencionadas en el primer párrafo de este artículo, entre otra información relacionada con las transacciones que los clientes hayan realizado o intentado realizar en su Infraestructura Tecnológica. Estos datos, en su carácter de datos personales de los clientes, solo podrán compartirse con la previa autorización expresa de éstos.

[…]

[4] "aquellos generados por las entidades a las que se refiere el artículo 76 de la LRITF que no contienen información confidencial, tales como información de productos y servicios que ofrecen al público general, la ubicación de sus oficinas y sucursales, cajeros automáticos u otros puntos de acceso a sus productos y servicios, entre otros."

[5] "aquellos relacionados a cualquier tipo de información estadística relacionada con operaciones realizadas por o a través de las entidades a las que se refiere el artículo 76 de la LRITF, sin contener un nivel de desagregación tal que puedan identificarse los datos personales o transacciones de una persona."

[6] "aquellos relacionados con el uso de un producto o servicio, incluyendo cuentas de depósito, créditos y medios de disposición contratados a nombre de los clientes de las entidades a las que se refiere el artículo 76 de la LRITF, entre otra información relacionada con las transacciones que los clientes hayan realizado o intentado realizar en su Infraestructura Tecnológica."

Parte 1. “Identificación de procesos que involucran el tratamiento de datos personales en las ITF”

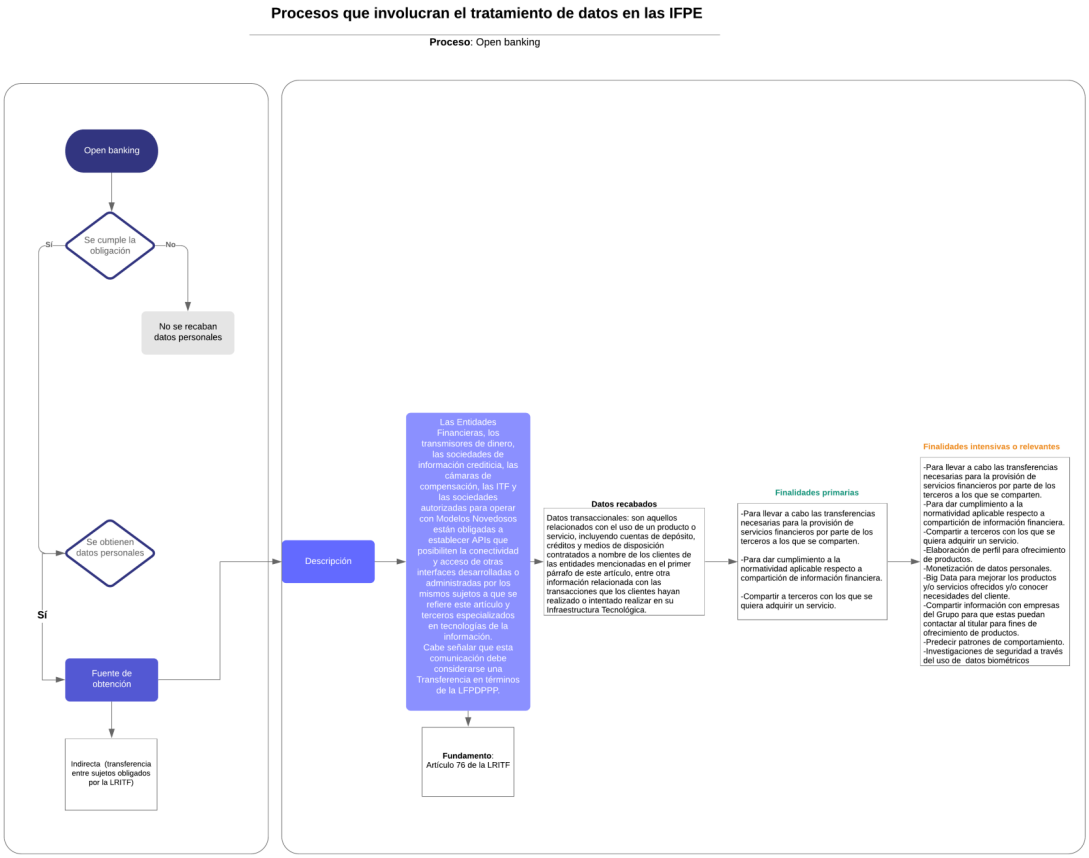
VII. Identificación de procesos en las ITF

La primera parte del Estudio consistió en identificar, desde la normatividad aplicable a datos personales, los distintos procesos y subprocesos que involucran el tratamiento de datos personales en el ejercicio de las operaciones de las ITF de acuerdo con la LRITF y demás normatividad aplicable.

Esta sección del Informe Final presenta un resumen de los procesos y subprocesos que involucran el tratamiento de datos personales en las operaciones de las IFC e IFPE identificando las finalidades del tratamiento a partir de 3 grupos principales: 1) finalidades primarias o genéricas; 2) finalidades secundarias; y 3) finalidades intensivas o relevantes.

Para apoyar la explicación posterior se han diseñado una serie de esquemas prácticos que corresponden a cada uno de los procesos y subprocesos identificados en las ITF en los que, a partir de la obtención de datos se describen los procesos y las distintas finalidades del tratamiento.

A continuación, se presenta un esquema aplicable a las operaciones de las IFPE:



De esta forma, en este apartado los procesos que involucran el tratamiento de datos personales en las ITF se dividen en 2 rubros principales:

1) Procesos que involucran el tratamiento de datos personales en las IFC.
2) Procesos que involucran el tratamiento de datos personales en las IFPE.

1. Procesos que involucran el tratamiento de datos personales en las IFC

A continuación, se presentan los procesos y subprocesos relacionados con el tratamiento de datos en las IFC reguladas por la LRITF. Los procesos generales identificados fueron los siguientes:

1. Alta del cliente;
2. PLD/CFT;
3. Obligación de conservar documentos;
4. Mecanismos de seguimiento y agrupaciones de operaciones;
5. Aspectos generales de las IFC;
6. Operaciones de las IFC;
7. *Open banking.*

Dentro del estudio de cada uno de los procesos identificados, se identificará y analizará cada uno de sus subprocesos.

1.1. Alta de cliente

1.1.1. Proceso general de alta de cliente

El proceso de alta de cliente inicia cuando una persona física o moral busca invertir o solicitar un financiamiento a través de las plataformas o medios que ponen a disposición las IFC. Derivado de lo anterior, los clientes interesados deberán firmar un contrato con las IFC que tenga por objeto celebrar las operaciones autorizadas por parte de las autoridades competentes. Antes de la firma del contrato la persona física o moral deberá entregar directamente la información y documentación necesaria para el expediente que la IFC debe mantener, para que ésta de cumplimiento a la normatividad aplicable y este en posibilidad de brindar los servicios de financiamiento colectivo a las personas físicas o morales que deseen contratar sus servicios.[7] Cabe señalar, que este expediente es requerido por un tema de PLD/CFT; sin embargo, es parte integrante del proceso necesario para dar de alta un cliente. Una vez que el cliente haya entregado la información y documentación necesaria la IFC podrá realizar la firma del contrato para darle el carácter a dicho cliente de solicitante o inversionista, los cuales para este momento podrán realizar las operaciones estipuladas en el contrato que celebren con ellos.

Para integrar el expediente las IFC deberán obtener de sus potenciales clientes el dato personal de geolocalización del dispositivo móvil desde el cual el cliente abra su cuenta o celebre el contrato respectivo. Con independencia de esto, la IFC deberá requerir, en función del tipo de cliente, la información señalada en los diagramas.[8]

1.1.2. Alta de cliente de riesgo de bajo

De conformidad con el artículo 12 de las DCGA58 existen cuentas y contratos que ofrecen las IFC, que podrán ser consideradas como de Riesgo bajo y podrán tener un régimen de identificación simplificado:

- ***Cuentas nivel 1***: celebradas con personas físicas cuya operación se encuentra limitada a 750 UDIS en el trascurso de un mes calendario. En este supuesto la IFC solo estará obligada a recabar el apellido paterno, apellido materno y nombre o nombres sin abreviatura, fecha de nacimiento, género, entidad federativa, ocupación, profesión, actividad o giro del negocio y dirección del correo electrónico. Estas cuentas están sujetas a un saldo máximo de 1,000 UDIS.
- ***Cuenta nivel 2***: celebradas con personas físicas, cuya operación se encuentre limitada a 3,000 UDIS, en el trascurso de mes calendario. En este supuesto la IFC solo estará obligada a recabar

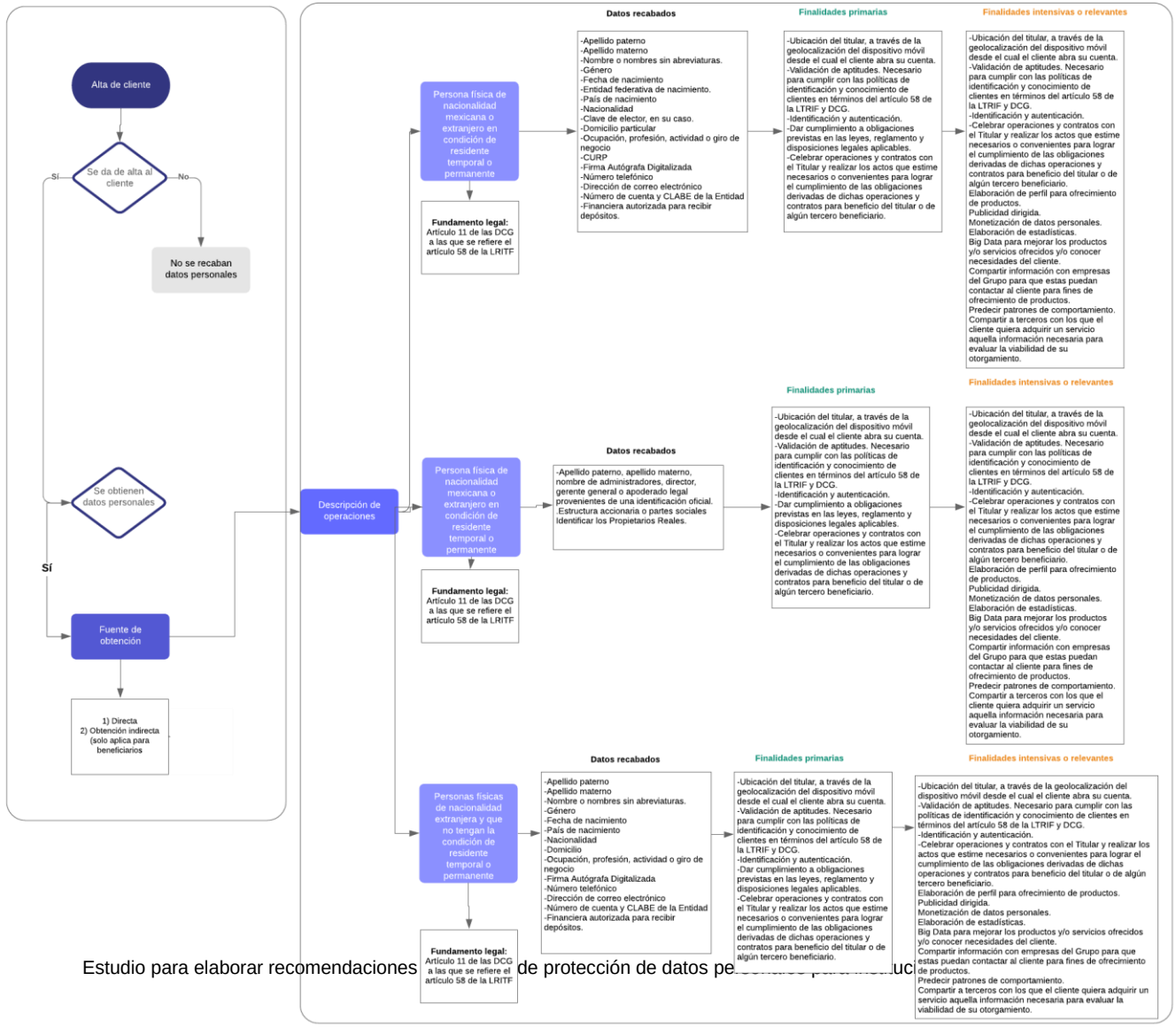
[7] Art. 11 de las DCGA58.
[8] La información se desprende del artículo 11 de las DCGA58.

lo establecido en la fracción I anterior y el domicilio, así como la versión digital del documento donde provengan los datos de identificación.

El proceso anterior se describe en el siguiente gráfico:

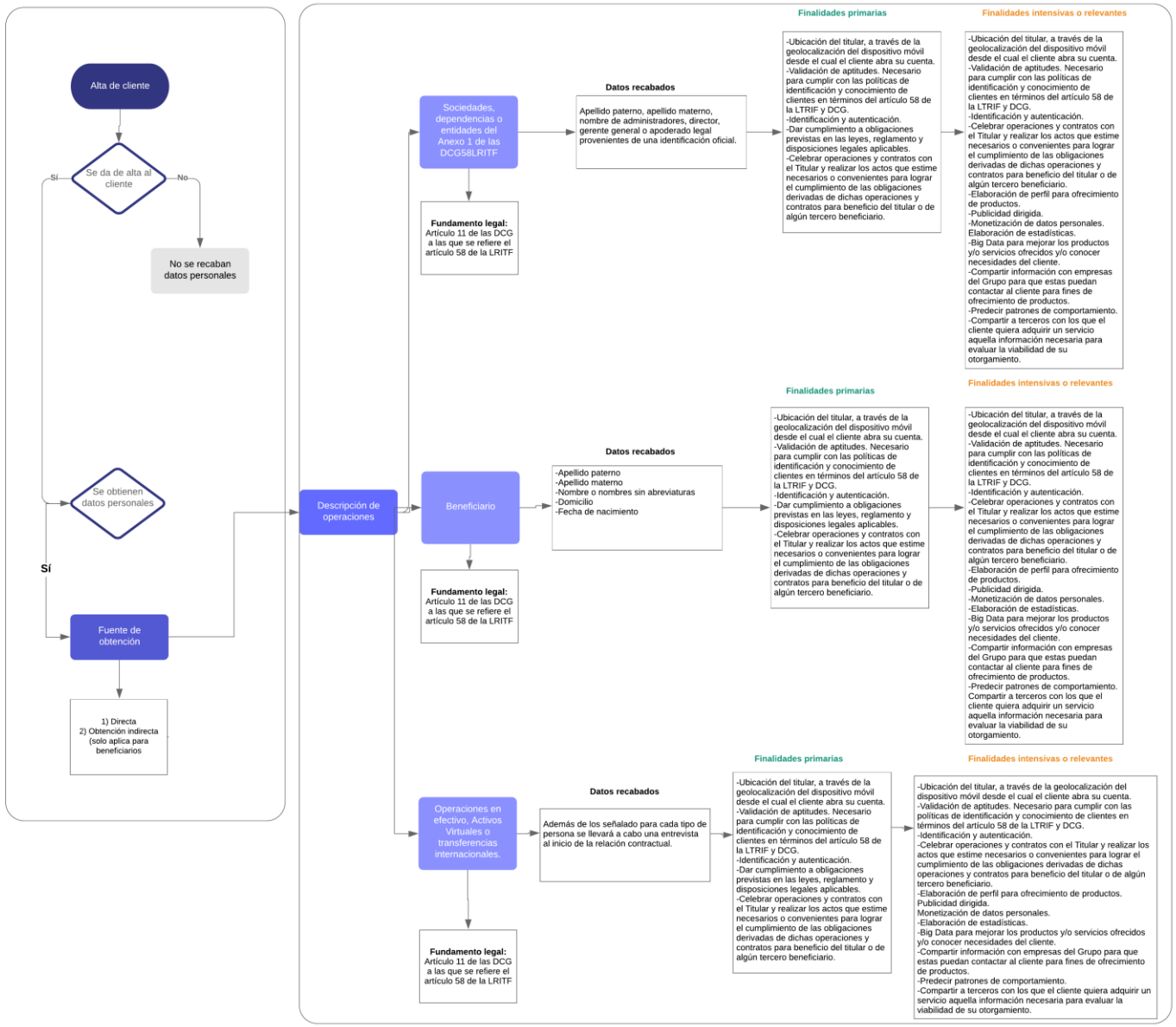
Procesos que involucran el tratamiento de datos en las IFC

Proceso: Alta de Cliente (Primera parte)
Subproceso: Identificación de los datos personales provenientes de documento válido, el cual deberá digitalizarse



Procesos que involucran el tratamiento de datos en las IFC

Proceso: Alta de Cliente (Segunda parte)
Subproceso: Identificación de los datos personales provenientes de documento válido, el cual deberá digitalizarse



1.2. PLD/CFT

Derivado del análisis realizado a la normatividad FinTech se identificó un proceso general relacionado con el tratamiento de datos personales: la prevención de lavado de dinero y combate al financiamiento al terrorismo (PLD/CFT).

El lavado de dinero "es el proceso a través del cual es encubierto el origen de los fondos generado mediante el ejercicio de algunas actividades ilegales […]. El objetivo de la operación, […], consiste en hacer que los fondos o activos obtenidos a través de actividades ilícitas aparezcan como fruto de actividades legítimas y circulen sin problema en el sistema financiero."[9] Asimismo, el financiamiento al terrorismo, "consiste en la aportación, financiación o recaudación de recursos o fondos económicos que tengan como fin provocar alarma, temor o terror en la población, en un grupo o sector de ella, para atentar contra la seguridad nacional o presionar a la autoridad para que tome una determinación."[10] En este sentido, las autoridades del sector financiero deben asegurar que la procedencia de los recursos sea lícita; es decir que las ITF no sean el medio comisivo para la realización de operaciones con recursos de procedencia ilícita y de financiamiento al terrorismo. En este sentido, las autoridades para ayudar a las ITF a evitar ser un medio para la comisión de delitos relacionados al lavado de dinero y financiamiento al terrorismo crea un marco jurídico estricto en el que obliga a las ITF conocer a su cliente, determinar su grado de riesgo, monitorear si este se encuentra en listas de personas bloqueadas, realizar una labor de supervisión mediante los reportes que deben entregar a autoridades; así como, la información que puedan compartirse entre ellas para determinar el riesgo del cliente a nivel del sistema financiero.

Este proceso involucra el tratamiento de datos personales, ya que para que las ITF puedan determinar el grado de riesgo del cliente estas llevan un expediente, el cual se describió en la sección de alta de cliente, para identificarlo; asimismo, llevan un registro de las operaciones incluyendo montos, volumen, divisa, lugar de destino, entre otras características de la Operación.

1.2.1. Subprocesos identificados de PLD/CFT

Como proceso general relacionado con el tratamiento de datos personales en las ITF (IFC e IFPE) se identificó la obtención de datos personales de los clientes para dar cumplimiento a las previsiones del articulo 58 de la LRITF y las correspondientes DCGA58. Derivado del análisis de las operaciones de las IFC en cumplimiento a la normatividad señalada se identificaron los siguientes subprocesos en materia de PLD/CFT: 1) reportes que se deberán remitir a la SHCP; 2) intercambio de información; 3) clasificación de clientes por grado de riesgo: bajo, medio o alto; 4) políticas de conocimiento de clientes; 5) listas de personas bloqueadas; y 6) auditorías para revisar el cumplimiento de las DCGA58.

1.2.1.1. Reportes que se deberán remitir a la SHCP

En el momento en el que se emite un reporte, es importante tener en cuanta que existe una transferencia de datos personales a la SHCP por parte de la IFC, esta transferencia se deberá apegar a lo que se establece en la normatividad para llevar un proceso claro y conforme a la ley.

En concreto, los reportes que se deberán remitir a la SCHP por parte de las IFC son los siguientes:

I. *Reportes de Operaciones Relevantes*, los cuales deberán realizarse dentro de 10 primero días hábiles de los meses de enero, abril, julio y octubre.

[9] https://www.gob.mx/cms/uploads/attachment/file/71151/VSPP_Lavado_de_Dinero___130701.pdf
[10] https://www.cnbv.gob.mx/CNBV/Documents/VSPP_Financiamiento%20al%20Terrorismo.pdf

II. *Reportes de operaciones en efectivo en moneda extranjera,* los cuales deberán realizarse dentro de 10 primero días hábiles de los meses de enero, abril, julio y octubre. Los reportes aplicarán cuando se realice una operación por un monto igual o superior a 500 dlls.
III. *Reporte de transferencias internacionales*, el cual se deberá remitir mensualmente por cada Operación de transferencia internacional que haya recibido o enviado cualquiera de sus Clientes durante dicho mes, por un monto igual o superior a 1,000 dlls o su equivalente en pesos o la moneda extranjera en que se realice con el respectivo cargo o abono a las cuentas.
IV. *Reporte de Operaciones Inusuales,* el cual se deberá remitir dentro de los siguientes tres días hábiles que concluya la sesión del Comité que la dictamine como tal.
V. *Reporte de Operaciones con Activos Virtuales*, los cuales deberán realizarse dentro de 10 primero días hábiles de los meses de enero, abril, julio y octubre. Dicho reporte deberá incluir la compra o venta de Activos Virtuales.
VI. *Reporte de Operaciones Internas Preocupantes*, el cual se deberá remitir dentro de los siguientes tres días hábiles que concluya la sesión del Comité que la dictamine como tal.

Estos reportes que se deberán presentar a la SHCP, por conducto de la CNBV, contienen los siguientes datos personales:

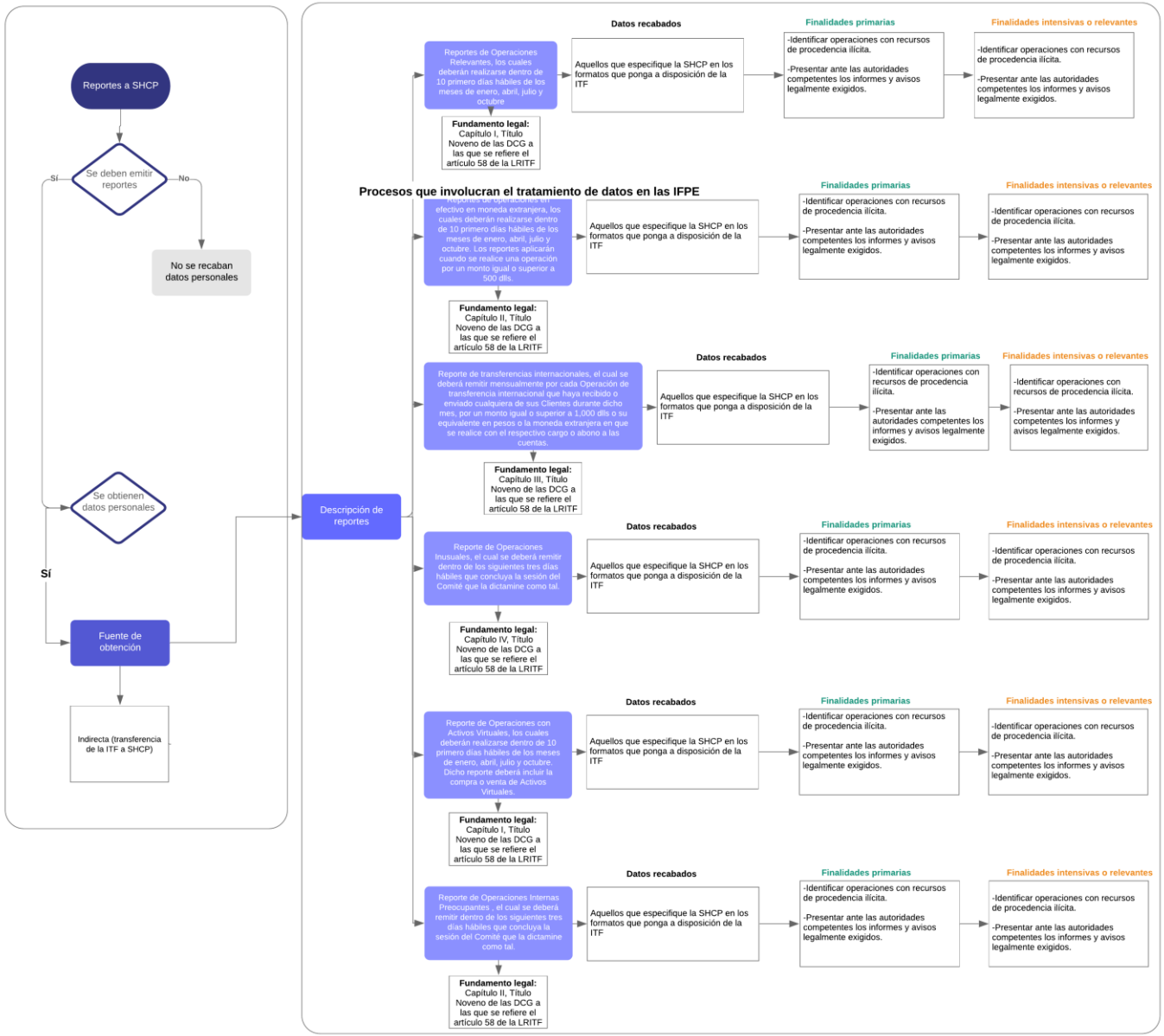
- Actos, operaciones y servicios que realicen con sus clientes y las operaciones entre estos, según corresponda,
- Todo acto, operación o servicio que realicen los miembros del consejo de administración, directivos, funcionarios, empleados, factores y apoderados que pudiesen contravenir o vulnerar la adecuada aplicación de las DCGA58.[11]

El siguiente esquema resume el subproceso de emisión de reportes y sus variantes:

[11] Art. 58 de la LRITF

Procesos que involucran el tratamiento de datos en las IFC

Proceso: PLD/CFT
Subproceso: Reportes que se deberán remitir a la SHCP



1.2.1.2. Intercambio de información[12]

Se identifican tres tipos de tratamientos en el proceso de intercambio de información: el intercambio de información con autoridades, el intercambio de información entre autoridades y el intercambio de información entre entidades financieras. Este tratamiento se identifica como una transferencia de datos personales con el fin de dar cumplimiento a la LRITF para prevenir el lavado de dinero y el financiamiento al terrorismo.

Las ITF están obligadas a proporcionar a la CNBV y BANXICO, en el ámbito de sus respectivas competencias, la información que dichas Autoridades Financieras les requieran sobre sus Operaciones y aquellas realizadas entre sus Clientes, incluso respecto de alguna o algunas de ellas en lo individual, los datos que permitan estimar su situación financiera y, en general, aquella que sea útil a la CNBV o al BANXICO para proveer el adecuado cumplimiento de sus funciones, en la forma y términos que las propias Autoridades determinen.[13]

Con el objeto de preservar la estabilidad financiera, evitar interrupciones o alteraciones en el funcionamiento del sistema financiero o del sistema de pagos, así como para facilitar el adecuado cumplimiento de sus funciones, la SHCP a, las Comisiones Supervisoras y BANXICO, podrán intercambiar entre sí la información que tengan en su poder por haberla obtenido:

a) En el ejercicio de sus facultades;
b) Como resultado de su actuación en coordinación con otras entidades, personas o autoridades, y
c) Directamente de otras autoridades.

Las autoridades financieras deberán celebrar convenios de intercambio de información en los que se especifique la información objeto de intercambio y se determine los términos y condiciones a los que deberán de sujetarse.[14] Asimismo, las autoridades financieras nacionales deberán tener suscrito un acuerdo de intercambio de información con autoridades financieras del exterior de que se trate en el que se contemple el principio de reciprocidad.[15]

Tanto la CNBV como BANXICO pueden abstenerse de proporcionar información cuando el uso que se le pretenda dar sea distinto a aquel para el cual haya sido solicitada, a la seguridad nacional o a los términos convenidos en el acuerdo de intercambio de información.

1.2.1.2.1. Intercambio de información entre las IFC

Las IFC podrán intercambiar información de las Operaciones, actividades y servicios que realicen con sus Clientes o de estos entre sí, con el objeto de fortalecer las medidas y procedimientos para prevenir y detectar actos, omisiones u operaciones que pudiesen actualizar los supuestos previstos en los artículos 139 Quáter o 400 Bis del CPF o favorecer, prestar ayuda, auxilio o cooperación de cualquier especie para la comisión de delitos en contra de sus Clientes o de la propia IFC. [16]

Para el intercambio de información las IFC deberán seguir lo siguiente:

a) Se pueden realizar entre dos o mas ITF

[12] El intercambio de información para temas de PLD/CFT se encuentra en el Título Décimo Primero de las DCGA58.
[13] Art. 70 de la LRITF
[14] Art. 74 de la LRITF
[15] Art. 75 de la LRITF
[16] Art. 77 de las DCGA58.

b) Ser solicitados por los funcionarios de las IFC autorizados para tales efectos mediante escrito en donde se especifique el motivo y clase de información que se requiera. Esta solicitud puede ser remitida de forma electrónica o digital asegurando la confidencialidad de la información.
c) La respuesta a esa solicitud debe remitirse por escrito firmando un funcionario autorizado en un plazo no mayor a 30 días naturales contados a partir de la fecha de la solicitud, misma que puede ser remitida de la misma forma que la solicitud, siempre asegurando la confidencialidad de la información.
d) La información proporcionada solo puede ser utilizada por la ITF solicitante salvo que sea compartida con otras ITF.
e) Las IFC podrán compartir con otras ITF la información que consideren relevante para fines del art 77 de las disposiciones, a través de mecanismos que para tales efectos establezca que cumpla con la normatividad aplicable.[17]

La IFC que comparta con otras ITF información, deberá conservar la misma información y documentación, misma que deberá estar a disposición de la secretaría y CNBV, dentro del plazo que la propia CNBV establezca.

Por otra parte, la IFC podrá intercambiar información con otras Entidades Financieras, así como con centros cambiarios, transmisores de dinero y asesores en inversiones.

Las IFC que formen parte de grupos financieros en términos de la Ley para Regular las Agrupaciones Financieras, podrán intercambiar cualquier tipo de información sobre las Operaciones, actividades y servicios que realicen con sus Clientes, con las otras Entidades Financieras que formen parte del mismo grupo que estén facultadas para ello conforme a las disposiciones aplicables en materia de prevención de operaciones con recursos de procedencia ilícita y financiamiento al terrorismo, siempre que celebren entre ellas un convenio en el que estipulen lo siguiente:

a) El tratamiento confidencial que se le dará a la información intercambiada.
b) Los cargos de los funcionarios autorizados para realizar el mencionado intercambio.

La IFC deberá conservar toda la información y documentación soporte que acredite tanto el procedimiento realizado para tal fin como la información intercambiada.[18]

Tratándose del Intercambio de Información con Entidades Financieras extranjeras es importante mencionar que:

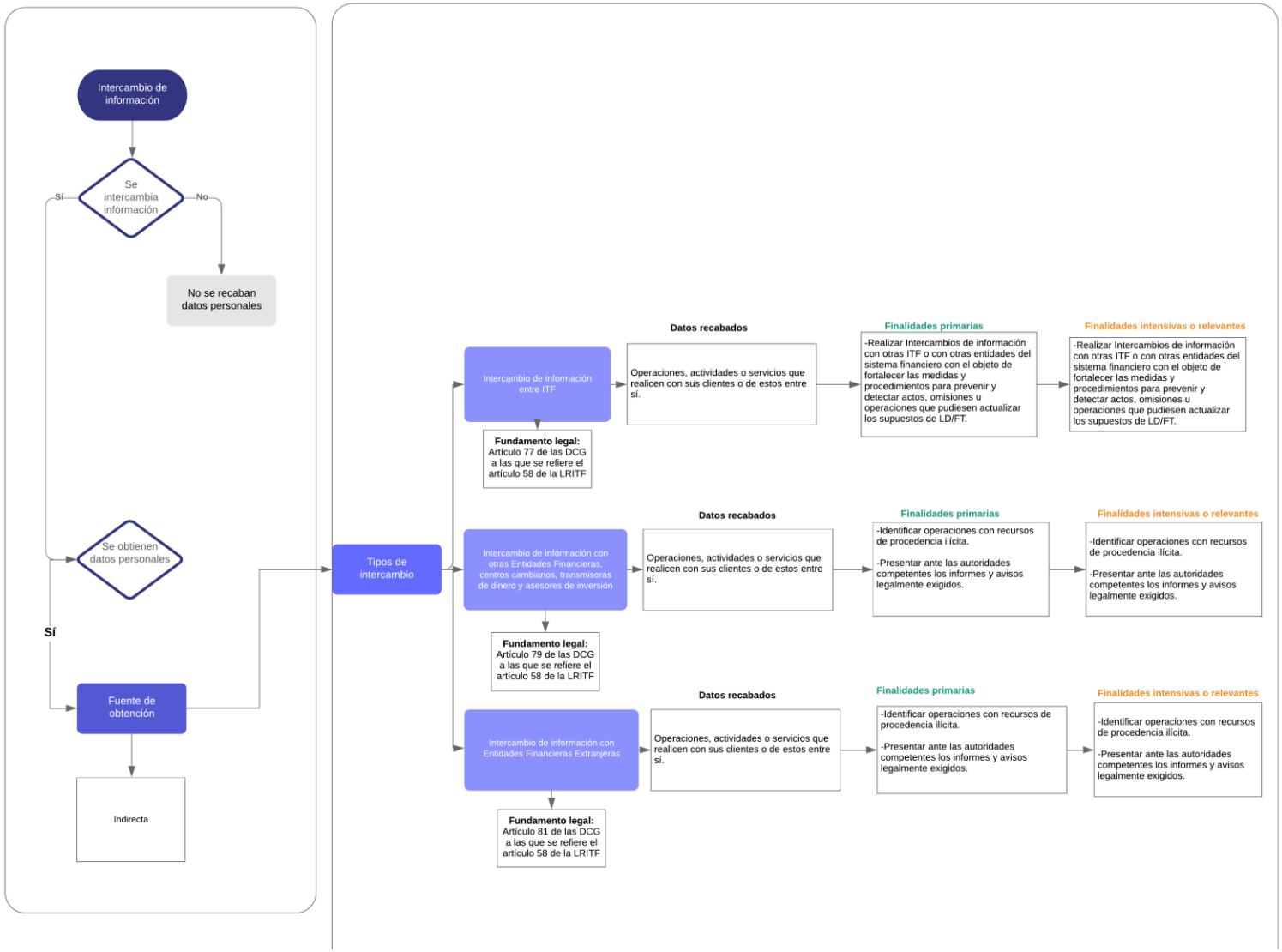
a) Únicamente se puede intercambiar información con las Entidades Financieras extranjeras que sean determinadas por la Secretaría,
b) Las IFC deberán convenir con las mismas entidades el tratamiento confidencial de la información intercambiada y los cargos de los funcionarios autorizados por ambas partes para realizar dicho intercambio.
c) Las IFC deberán enviar a la SHCP a través de la CNBV mediante los medios que la misma designe, copia de formato que contenga la información intercambiada. [19]

El proceso anterior se resume en el siguiente diagrama:

[17] Art. 78 de las DCGA58.
[18] Art. 80 de las DCGA58.
[19] Art. 81 de las DCGA58.

Procesos que involucran el tratamiento de datos en las IFC

Proceso: PLD/CFT
Subproceso:Intercambio de información



1.2.1.3. Clasificación de Clientes por Grado de Riesgo: bajo, medio o alto

Para establecer el Grado de Riesgo, las IFC deben diseñar e implementar una metodología para evaluar el grado del riesgo a las que se encuentran expuestas derivado de productos, servicios, clientes, áreas geográficas, etc.

La metodología deberá establecer y describir todos los procesos que se llevarán a cabo para identificar el Grado de Riesgo así como la información que resulte aplicable. [20]

Para diseñar la metodología deberán cumplir con lo siguiente:

a) Identificar el elemento a evaluar, en este caso Tipo de Clientes
b) Utilizar un método para medir el Riesgo
c) Identificar los Mitigantes que la IFC tiene implementados al momento de diseñar la metodología, considerando políticas, criterios medidas y procedimientos internos contenidos en su Manual de Cumplimiento, con la finalidad de establecer el efecto que estos tendrán sobre los indicadores y elementos de Riesgo.[21]

Las IFC deberán asegurarse de:

a) Que no existan inconsistencias entre la información que incorporen y la que obre en sistemas autorizados
b) Utilizar la información correspondiente en un periodo mínimo de doce meses

En el supuesto de que se detecte existencia de mayores o nuevos riesgos para las IFC, deberán modificar las políticas, criterios, medidas y procedimientos correspondientes. Las modificaciones serán revisadas por las IFC en un plazo no mayor a 12 meses contados a partir de que la propia IFC cuente con los resultados de su implementación.[22]

De la clasificación del Grado de Riesgo del Cliente

El modelo de evaluación de Riesgo con el que deberán contar las IFC, deberá apegarse en todo momento a la metodología a la que se hace referencia en los párrafos anteriores, para clasificar a sus Clientes por Grado de Riesgo, el cual deberá estar establecido en su Manual de Cumplimiento. Las clasificaciones deberán de establecer tres Grados de Riesgo, siendo estos bajo, medio y alto, y pueden establecer los grados intermedios que consideren necesarios, apegándose siempre a la metodología implementada para la misma clasificación.[23]

Las IFC deben considerar mínimo los primeros seis meses la información proporcionada por cada uno de sus clientes para determinar el Grado de Riesgo. Las evaluaciones de grado de riesgo se deberán llevar a cabo cada seis meses con la finalidad de determinar si el grado de riesgos diferente al establecido en un inicio. Entre mas alto sea el grado del riesgo, la frecuencia de evaluación incrementa.[24]

Algunos puntos importantes a considerar para determinar el grado del riesgo del Cliente a través de la metodología ya mencionada anteriormente son:

[20] Art. 3 de las DCGA58.
[21] Art. 4 de las DCGA58.
[22] Art. 5 de las DCGA58.
[23] Art. 29 de las DCGA58.
[24] Art. 30 de las DCGA58.

I. Características inherentes de la persona:

a. Antecedentes del cliente
b. Tipo de persona
c. Fecha de nacimiento o constitución
d. Giro o actividad
e. Nacionalidad
f. Lugar de residencia
g. Fuentes de ingreso
h. Naturaleza o propósito de la relación que tenga con la IFC

II. Características transaccionales:

a. Tipo y numero de productos y servicios contratados
b. Volumen en número y monto de Operaciones
c. Frecuencia de Operaciones
d. Número de contrapartes
e. Origen y destino de los recursos
f. Instrumento monetario
g. Tipo de moneda.[25]

Clientes de grado de riesgo alto son:

a. Los no residentes en el país
b. Cuando las operaciones que los clientes realicen estén vinculadas o tengan efectos en los países o jurisdicciones siguientes:
   i. Que la legislación mexicana considera que aplican regímenes fiscales preferentes. [SEP]
   ii. Que las autoridades mexicanas, organismos internacionales o agrupaciones intergubernamentales en materia de prevención de operaciones con recursos de procedencia ilícita o financiamiento al terrorismo de los que México sea miembro determinen que no cuenten con medidas para prevenir, detectar y combatir dichas operaciones, o bien, cuando la aplicación de dichas medidas sea deficiente. [SEP] (art 70)
c. Personas políticamente expuestas extranjeras [26]

Las IFC, en las Operaciones que realicen con Clientes clasificados con Grado de Riesgo alto, deberán:

Para el caso de personas físicas

a) Adoptar medidas reforzadas para conocer el origen y destino de los recursos.
b) Obtener, en su caso, los datos señalados en el Título Tercero, Capítulo I de las DCGA58, en los términos que al efecto prevean en su Manual de Cumplimiento elaborado por las propias IFC, respecto del cónyuge y dependientes económicos del Cliente, así como de las sociedades y asociaciones con las que mantenga vínculos patrimoniales.

Para el caso de personas morales,

Obtener mayor información de sus principales accionistas o socios, según corresponda, debiendo consultar para confirmar los datos, los registros electrónicos de la Secretaría de Economía para verificar la información proporcionada por el Cliente. [SEP]

Personas Políticamente Expuestas extranjeras

[25] Art. 31 de las DCGA58.
[26] Art. 33 de las DCGA58.

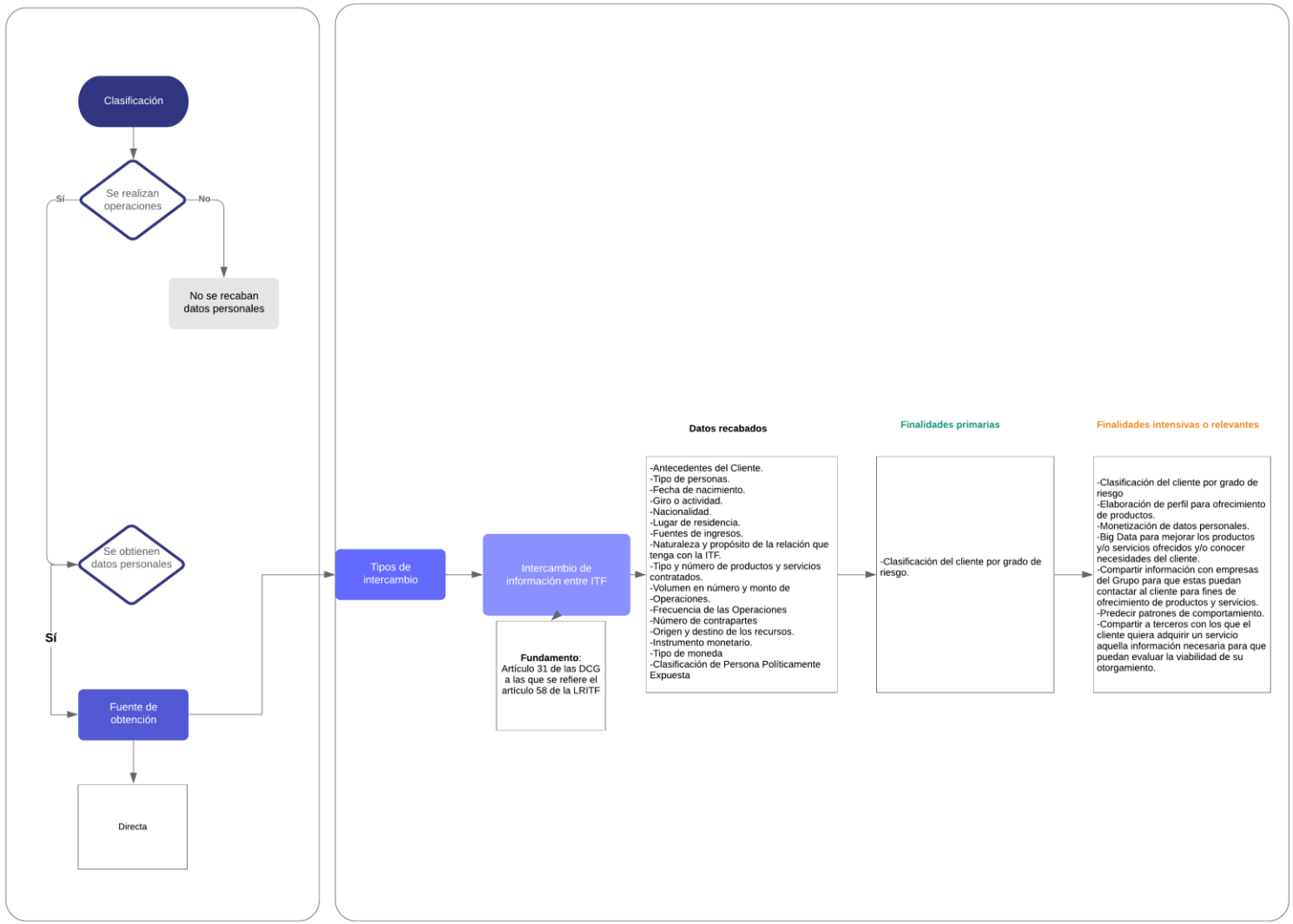
Obtener, además de los datos a que se refiere el presente artículo, la documentación señalada en el Título Tercero, Capítulo I de las DCGA58, respecto de las personas físicas y morales antes señaladas en este párrafo. [27]

El proceso anterior se resume en el siguiente diagrama:

[27] Art. 38 de las DCG

Procesos que involucran el tratamiento de datos en las IFC

Proceso: PLD/CFT
Subproceso: Clasificación por grado de riesgo



1.2.1.4. Políticas de conocimiento de clientes

Las IFC están obligadas a elaborar una política de conocimiento de sus Clientes, que deberá incluir:

a) Las políticas, criterios, medidas, procedimientos y controles para mitigar los Riesgos,
b) procedimientos para dar seguimiento y monitorear las Operaciones, actividades o servicios realizados por sus Clientes.
c) procedimientos para el debido conocimiento del perfil transaccional de cada uno de sus Clientes.
d) supuestos en que las Operaciones se aparten del perfil transaccional de cada uno de sus Clientes y, en caso de cambios significativos en dicho perfil, los casos en que procede la revisión y actualización del expediente de identificación del Cliente que sobre este mantenga la IFC.
e) Medidas para la identificación de posibles Operaciones Inusuales.
f) Criterios para establecer y, en su caso, modificar el grado de Riesgo previamente determinado a un Cliente. [28]

Esta política se basa en el grado de Riesgo que representa el Cliente.

Las IFC, para determinar el perfil transaccional de sus Clientes deberán considerar, al menos, lo siguiente:

a) La información proporcionada por el Cliente, por los empleados o funcionarios de la IFC con base en su cartera de Clientes, o bien, la que obre en los archivos de la IFC.
b) El monto, número, tipo, naturaleza y frecuencia de las Operaciones que, de forma habitual o recurrente, realice el Cliente.
c) El origen y destino de los recursos o bienes objeto de la Operación.
d) La información de geolocalización del dispositivo móvil desde el cual el Cliente, en su caso, realice la Operación, actividad o servicio con la respectiva IFC.
e) Los demás elementos y criterios que determinen las propias IFC para tales efectos.

Las IFC, deben de considerar los seis primeros meses iniciando la relación comercial, la información que proporcione cada uno de sus Clientes para determinar su perfil transaccional inicial y deberán realizar una evaluación a fin de determinar si es necesario o no modificarlo.[29]

Los directivos de una IFC con facultades para autorizar que se celebren contratos o realización de Operaciones, deberán otorgar aprobación de forma escrita, digital o electrónica. [30]

Para los casos en que las IFC detecten que un Cliente reúne los requisitos para ser considerado Persona Políticamente Expuesta y, además, como de Grado de Riesgo alto, dichas IFC deberán, de acuerdo con lo que al efecto establezcan en su Manual de Cumplimiento, obtener la aprobación de una de las personas a que se refiere el artículo 39, a efecto de llevar a cabo la Operación de que se trate. [31]

En caso de que se presuma que alguno de los clientes actúa en nombre y representación de un tercero, la IFC deberá solicitar al Cliente información necesaria para identificar al Propietario Real de los recursos o bienes objeto de la Operación.[32]

[28] Art. 34 de las DCGA58.
[29] Art. 35 de las DCGA58.
[30] Art. 39 de las DCGA58.
[31] Art. 40 de las DCGA58.
[32] Art. 42 de las DCGA58.

Se deberán establecer mecanismos de seguimiento y agrupación de operaciones que realicen sus clientes. Los mecanismos deberán ser mas estrictos respecto a:

a) Instituciones de Financiamiento Colectivo: cuando sus Clientes realicen Operaciones durante un mes calendario, en efectivo por un monto igual o superior al equivalente en moneda nacional o extranjera, o Activos Virtuales a doce mil quinientas unidades de inversión.

b) Instituciones de Fondos de Pago Electrónico: cuando sus Clientes realicen Operaciones durante un mes calendario, en efectivo o en fondos de pago electrónico, en moneda nacional o extranjera, o Activos Virtuales, por un monto igual o superior a siete mil quinientas unidades de inversión.

Asimismo, las IFC deberán de llevar un registro de clientes respecto de las operaciones mencionadas anteriormente que contendrá:

a) Los datos de la política de identificación del cliente a que se refieren el artículo 11 de las Disposiciones Generales, según se trate de personas físicas o morales.

b) Fecha y monto de cada una de las Operaciones que haya realizado el Cliente.

Las IFC deberán conservar la información contemplada en este artículo para proporcionarla[33], en caso de ser requerida a:

- A la SHCP;

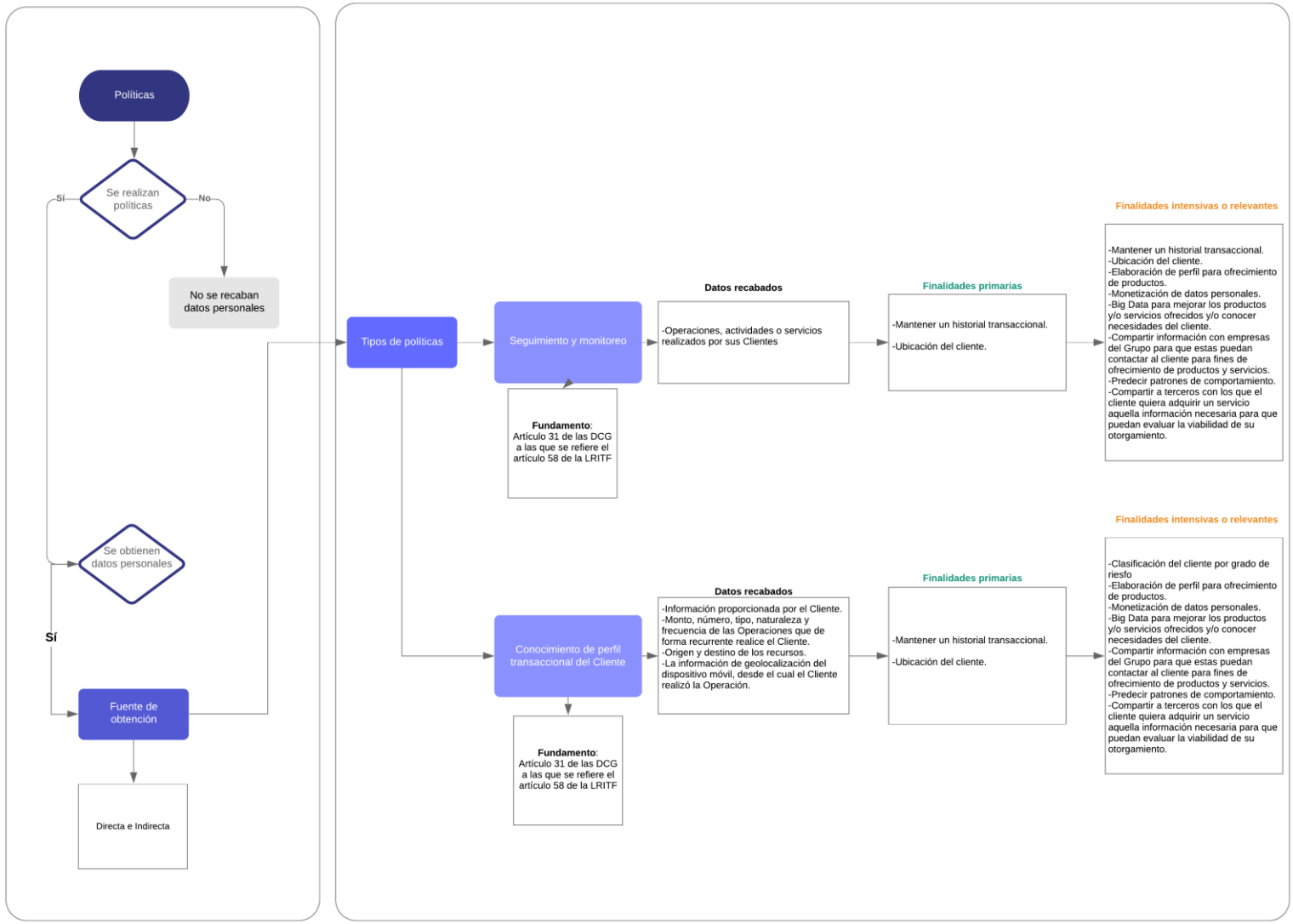
- CNBV.

El proceso anterior se resume en el siguiente diagrama:

[33] Art. 43 de las DCGA58.

Procesos que involucran el tratamiento de datos en las IFC

Proceso: PLD/CFT
Subproceso: Política de conocimiento de clientes



1.2.1.5. Listas de personas bloqueadas

México es un estado miembro de la ONU, lo que le obliga a dar cumplimiento a las resoluciones del Consejo de Seguridad de la Organización de las Naciones Unidas (CSONU). Asimismo, es miembro del Grupo de Acción Financiera Internacional (GAFI), el cual es "el organismo intergubernamental que fija los estándares internacionales en materia de prevención y combate al lavado de dinero y financiamiento al terrorismo."[34] "Las Resoluciones 1267 (1999), 1373 (2001) y demás relacionadas, emitidas por el CSONU, exigen a los Estados que congelen sin dilación los fondos y demás activos financieros o recursos económicos de las personas que cometan, o intenten cometer, actos de terrorismo, participen en ellos o faciliten su comisión. Por su parte, GAFI en su recomendación 6, establece que los países miembros deben implementar regímenes de sanciones financieras para cumplir con las Resoluciones del CSONU mencionadas, relativas a la prevención y represión del terrorismo y el financiamiento del terrorismo. Derivado de lo anterior, […] se previó la obligación de los sujetos obligados de suspender de forma inmediata la realización de todos los actos, operaciones o servicios que celebren con los clientes o usuarios mediante una lista de personas bloqueadas."[35]

De conformidad con el artículo 58 de la LRITF las IFC deberán suspender de forma inmediata la realización de actos, Operaciones o servicios con los Clientes que la SHCP les informe mediante una lista de personas bloqueadas que tendrá el carácter de confidencial. La lista de personas bloqueadas tendrá la finalidad de prevenir y detectar actos, omisiones u Operaciones que pudieran ubicarse en los supuestos previstos en la fracción I del párrafo primero de este artículo. Esta lista se pondrá a disposición de la IFC, a través de la CNBV para que esta adopte los mecanismos que permita identificar a los clientes que se encuentren dentro de estas listas.[36]

El artículo 61 de las DCGA58 establece los parámetros que utiliza la SHCP para introducir personas a la lista de personas bloqueadas, estos son los siguiente:

- Aquellas que se encuentren en las listas derivadas de las resoluciones 1267 (1999) y sucesivas, y 1373 (2001) y las demás que sean emitidas por el Consejo de Seguridad de las Naciones Unidas o las organizaciones internacionales.
- Aquellas que den a conocer autoridades extranjeras, organismos internacionales o agrupaciones intergubernamentales y que sean determinadas por la SHCP en términos de los instrumentos internacionales celebrados por el Estado Mexicano con dichas autoridades, organismos o agrupaciones, o en términos de los convenios celebrados por la propia Secretaría.
- Aquellas que den a conocer las autoridades nacionales competentes por tener indicios suficientes de que se encuentran relacionadas con los delitos de financiamiento al terrorismo, operaciones con recursos de procedencia ilícita o los relacionados con los delitos señalados, previstos en el CPF.
- Aquellas que estén compurgando sentencia por los delitos de financiamiento al terrorismo u operaciones con recursos de procedencia ilícita, previstos en el CPF.
- Aquellas que las autoridades nacionales competentes determinen que hayan realizado o realicen actividades que formen parte, auxilien, o estén relacionadas con los delitos de financiamiento al terrorismo u operaciones con recursos de procedencia ilícita, previstos en el CPF.
- Aquellas que omitan proporcionar información o datos, la oculten, encubran o impidan conocer el origen, localización, destino o propiedad de recursos, derechos o bienes que provengan de delitos de financiamiento al terrorismo u operaciones con recursos de procedencia ilícita, previstos en el CPF o los relacionados con estos.

[34] https://www.cnbv.gob.mx/PrevencionDeLavadoDeDinero/Documents/VSPP_Listas%20%20%2013042016.pdf
[35] *Ídem*
[36] Art. 60 de las DCGA58

Cuando la IFC identifique que dentro de las listas de personas bloqueadas se encuentra alguno de sus clientes, deberá tomar las medidas siguientes[37]:

- Suspender de manera inmediata la realización de cualquier acto, actividad, Operación o servicio relacionado con el Cliente identificado en la Lista de Personas Bloqueadas.
- Remitir a la SHCP, por conducto de la CNBV, dentro de las veinticuatro horas contadas a partir de que conozca dicha información, un reporte de Operación Inusual

Asimismo, cuando la IFC haya suspendido los actos, Operaciones, actividades o servicios con sus clientes, de manera inmediata deberán hacer del conocimiento dicha situación, esta notificación podrá realizarse a través de medios electrónicos.[38]

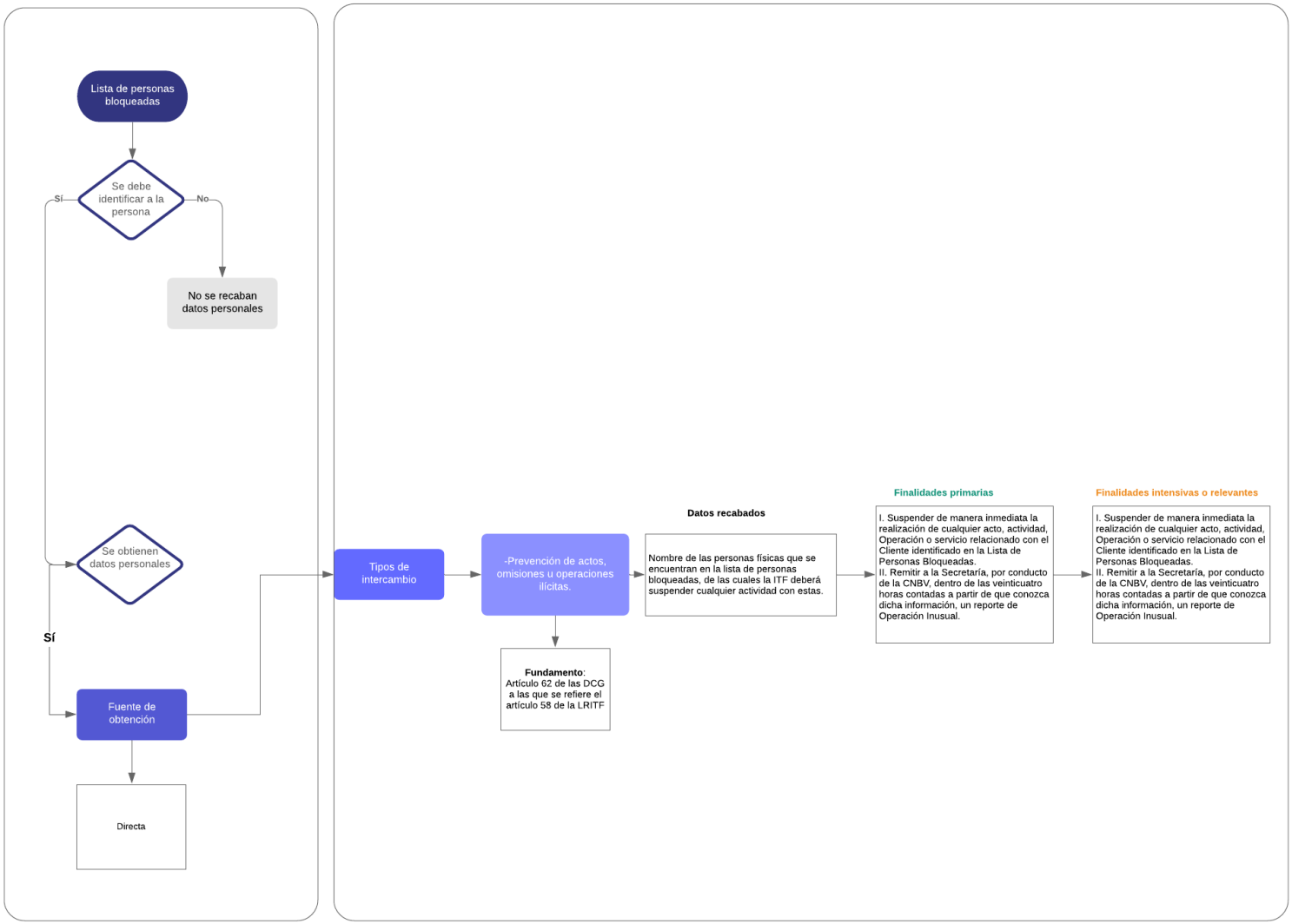
Por último, las IFC deberán asegurarse que en sus sistemas automatizados contengan las listas de personas bloqueadas para dar cumplimiento al artículo 58 de la LRITF.[39]

El proceso anterior se resume en el siguiente diagrama:

[37] Art. 62 de las DCGA58
[38] Ídem
[39] Art. 45, fracción VI, de las DCGA58.

Procesos que involucran el tratamiento de datos en las IFC

Proceso: PLD/CFT
Subproceso: Obligaciones de las ITF respecto a la lista de personas bloqueadas



1.2.1.6. Auditoría para revisar el cumplimiento de las DCGA58

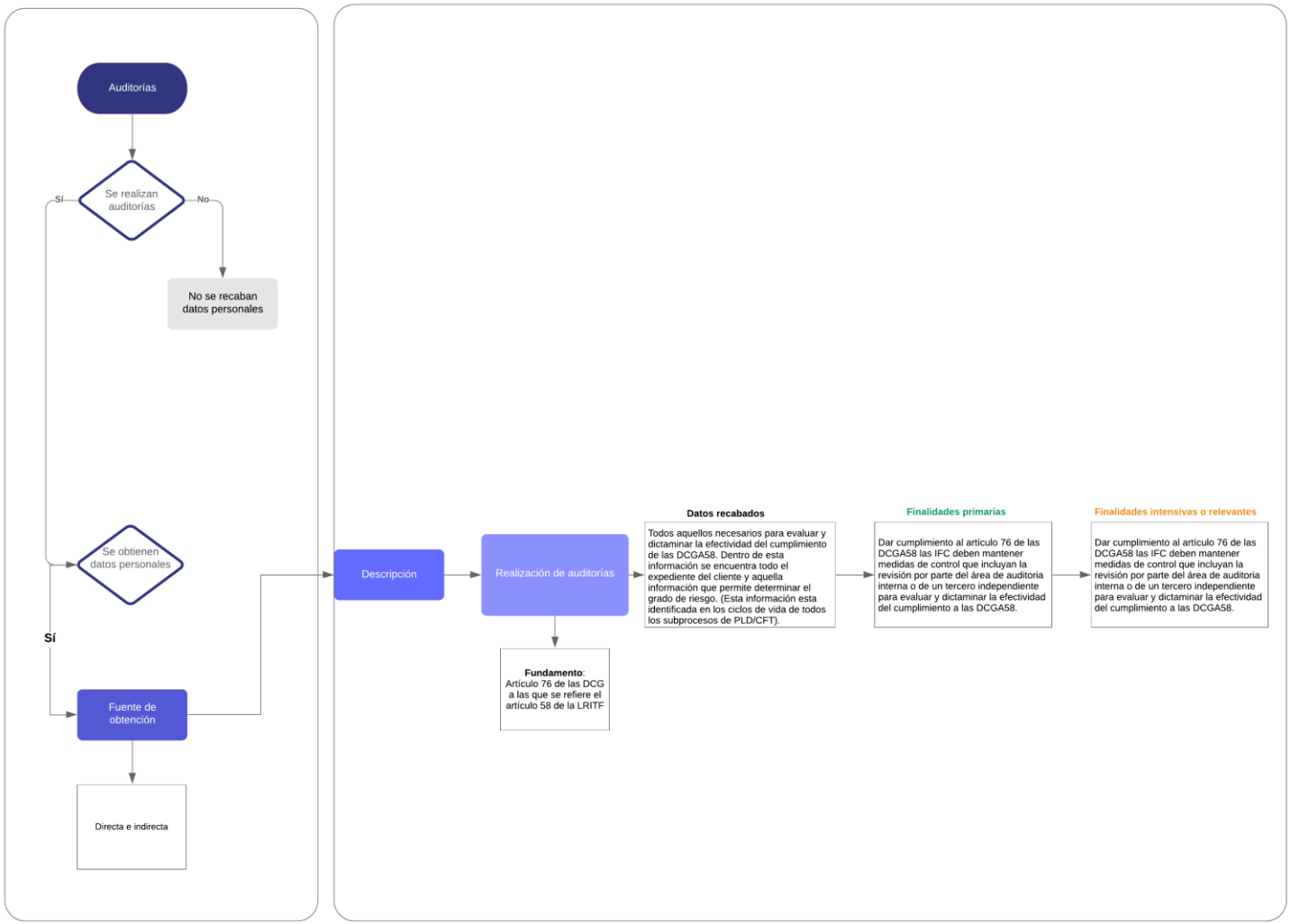
De conformidad con el artículo 76 de las DCGA58 las IFC deben mantener medidas de control que incluyan la revisión por parte del área de auditoria interna o de un tercero independiente para evaluar y dictaminar la efectividad del cumplimiento a las DCGA58. En este sentido, se pude identificar una comunicación de datos personales entre la IFC y el tercero independiente que realice la evaluación del cumplimiento a las DCGA58.

Los resultados de la revisión deberán presentarse al administrador único o a la dirección general y, en su caso, al comité de la IFC a manera de informe, a fin de avaluar la eficacia operativa de las medidas implementadas y dar seguimientos a programas de acciones correctivas. El responsable de suscribir la revisión deberá haber obtenido la certificación prevista en el artículo 4, fracción X de la Ley de la CNBV. Es importante señalar, que la información deberá ser conservada por un plazo no menor a 5 años y remitirse a la CNBV dentro de los 60 días naturales siguientes al cierre del ejercicio que corresponda la revisión.

El proceso anterior se resume en el siguiente diagrama:

Procesos que involucran el tratamiento de datos en las IFC

Proceso: PLD/CFT
Subproceso: Auditoría para revisar el cumplimiento de las DCGA58



1.3. Obligación de conservar documentos

Se identifico un subproceso en el artículo 48 de la LRITF, el cual obliga a las IFC a conservar por un plazo de mínimo de 10 años los comprobantes originales de sus Operaciones, debidamente archivados y, en formato impreso, o en medios electrónicos, ópticos o de cualquier otra tecnología, siempre y cuando, en estos últimos medios, se observe lo establecido en la norma oficial mexicana sobre digitalización y conservación de mensajes de datos aplicable, de tal manera que puedan relacionarse con dichas Operaciones y con el registro que de ellas se haga. Asimismo, deberán resguardar y garantizar la seguridad de la información y documentación relativas a la identificación de sus clientes o que lo hayan sido, así como la de aquellos actos, Operaciones y servicios reportados, esta información y documentación deberá conservarse por lo menos 10 años.[40]

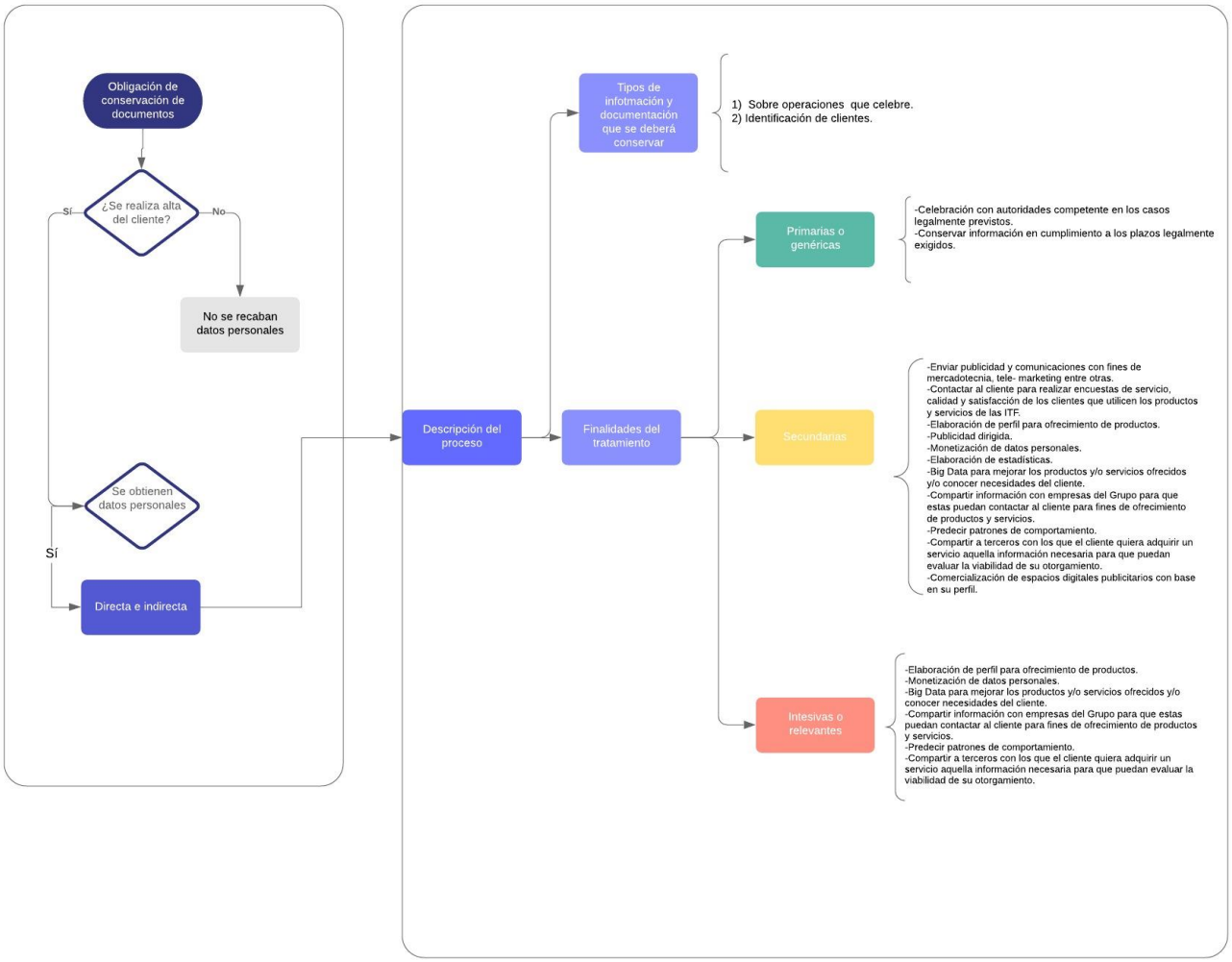
Derivado de lo anterior, a pesar de que no existe una lista exhaustiva de los datos personales que se pudieran llegar a conservar. Se Identifican los siguientes: datos personales de identificación y autenticación, contacto, demográficos, ubicación geográfica, características de dispositivo electrónico, patrimoniales y/o financieros, crediticios, laborales y biométricos para fines de colaboración con autoridades competentes en los casos legalmente previstos y conservar información en cumplimiento a los plazos legalmente exigidos. Es importante determinar el plazo de conservación de los documentos ya que permite determinar el momento exacto en el que la IFC deberá cancelar los datos personales.

El proceso anterior se resume en el siguiente diagrama:

[40] Art. 58 de la LRITF

Procesos que involucran el tratamiento de datos en las IFC

Proceso: Obligación de conservación de documentos



1.4. Mecanismos de seguimiento y agrupaciones de operaciones

Los mecanismos de seguimiento y agrupación de operaciones es una obligación que deberán cumplir las IFC mediante mecanismos que permitan identificar a los clientes y a las operaciones que estos realizan, independientemente del monto mediante el cual están operando. Este seguimiento y agrupación de las operaciones del cliente obliga a la IFC a llevar a cabo un registro del cliente respecto a las operaciones, el cual contendrá lo siguiente:

I. Los datos de identificación necesarios para dar de alta a un cliente. (obtenidos de forma directa)
II. Fecha y monto de cada una de las operaciones que haya realizado un cliente. (obtenidos de forma indirecta)

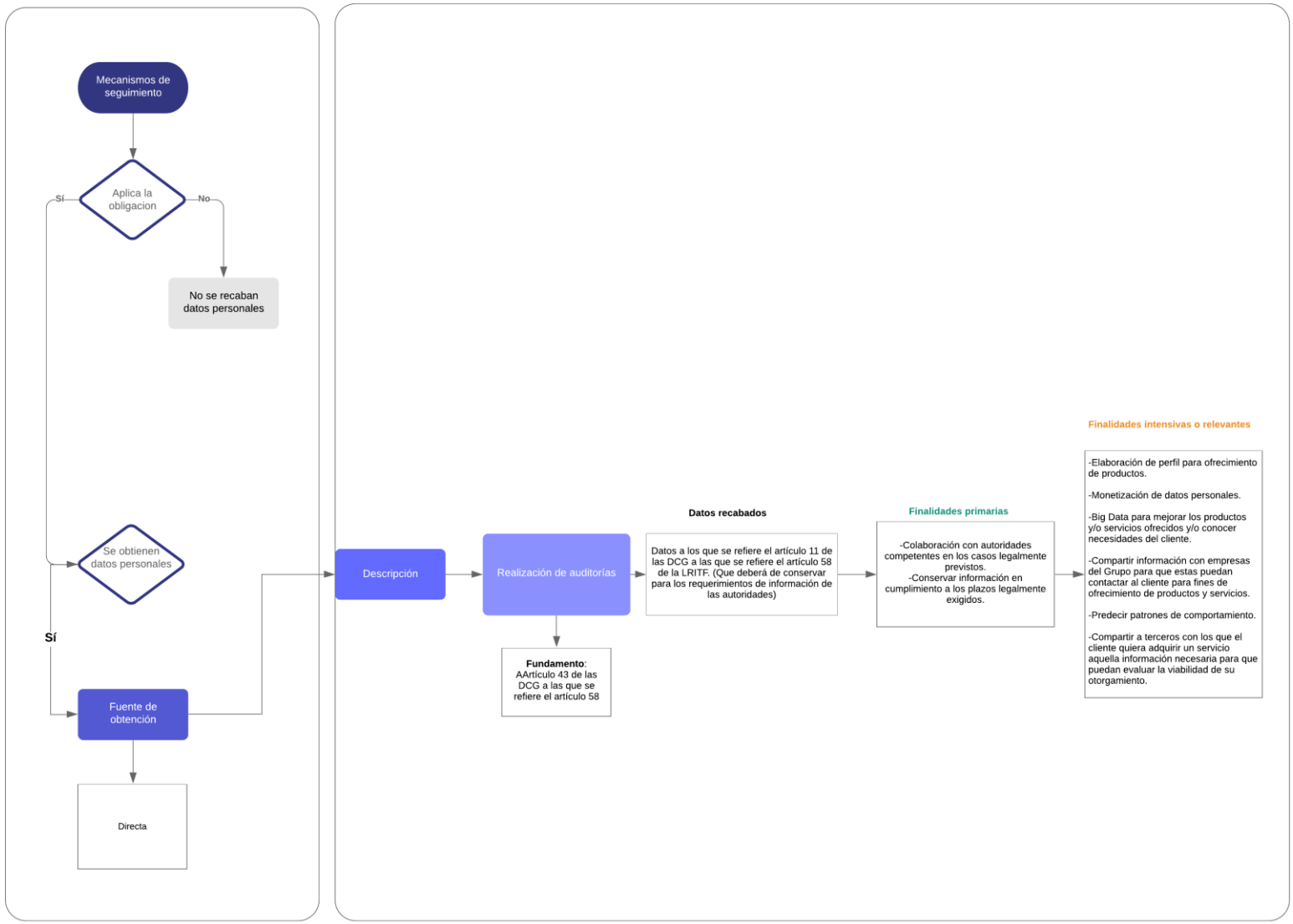
Esta información deberá ser conservada para proporcionarla a las SHCP y la CNBV, a requerimiento de esta última

En este sentido, se identifica el tratamiento de datos ya que por una parte existe la conservación de este expediente, independiente de aquél que fue resultado del alta del cliente, por parte de la IFC y obliga a esta institución a comunicar dichos datos a las autoridades competentes.

El proceso anterior se resume en el siguiente diagrama:

Procesos que involucran el tratamiento de datos en las IFC

Proceso:Mecanismos de seguimiento y agrupación de las operaciones



1.5. Características de las Operaciones que realizan las IFC

Conforme a lo dispuesto por el artículo 15 de la LRITF, las IFC pueden realizar actividades destinadas a poner en contacto a personas del público en general, con el fin de que entre ellas se otorguen financiamientos mediante alguna de las operaciones señaladas en el artículo 16 del citado ordenamiento (*financiamiento colectivo de deuda, financiamiento colectivo de capital y financiamiento colectivo de copropiedad o regalías*), realizadas de manera habitual y profesional, a través de aplicaciones informáticas, interfaces, páginas de internet o cualquier otro medio de comunicación electrónica o digital.

En sintonía con lo anterior, las Disposiciones en materia de PLD/FT definen a las IFC en la fracción XIII de su artículo segundo al señalar que una IFC es: "*aquella persona moral autorizada por la CNBV que, de manera habitual y profesional, lleve a cabo actividades destinadas a poner en contacto a personas del público en general, con el fin de que entre ellas se otorguen financiamientos mediante alguna de las Operaciones a que se refiere el artículo 16 de la Ley, a través de aplicaciones informáticas, interfaces, páginas de Internet o cualquier otro medio de comunicación electrónica o digital*."

De acuerdo con la LRITF, las IFC se encuentran habilitadas para realizar las actividades que les son inherentes a su objeto, así como las siguientes actividades previstas en el artículo 19 de la LRITF:

- Recibir y publicar las solicitudes de operaciones de financiamiento colectivo de los solicitantes y sus proyectos a través de la interfaz, página de internet o medio de comunicación electrónica o digital que utilice para realizar sus actividades.
- Facilitar que los potenciales inversionistas conozcan las características de las solicitudes de operaciones de financiamiento colectivo de los solicitantes y sus proyectos a través de la interfaz, página de internet o medio de comunicación electrónica o digital que utilice para realizar sus actividades.
- Habilitar y permitir el uso de canales de comunicación electrónicos mediante los cuales los inversionistas y solicitantes puedan relacionarse a través de la interfaz, página de internet o medio de comunicación electrónica o digital que utilice para realizar sus actividades.
- Obtener préstamos y créditos de cualquier persona, nacional o extranjera, destinados al cumplimiento de su objeto social.
- Emitir valores por cuenta propia.
- Adquirir o arrendar los bienes muebles e inmuebles necesarios para la realización de su objeto y enajenarlos cuando corresponda.
- Constituir depósitos en entidades financieras autorizadas para ello.
- Constituir los fideicomisos que resulten necesarios para cumplir su objeto social.
- Realizar inversiones permanentes en otras sociedades, siempre y cuando les presten servicios auxiliares, complementarios o de tipo inmobiliario.
- Realizar la cobranza extrajudicial o judicial de los créditos otorgados a los solicitantes por cuenta de los inversionistas
- Renegociar los términos y condiciones los créditos otorgados a los solicitantes.
- Realizar los actos necesarios para la consecución de su objeto social.

Además de los anteriores, las IFC pueden realizar actividades para facilitar la venta o adquisición de los derechos o títulos intercambiados que documenten las operaciones de financiamiento colectivo de deuda, financiamiento colectivo de capital y financiamiento colectivo de regalías, así como actuar como mandatarias o comisionistas de sus clientes para la realización de las actividades relacionadas con las operaciones que lleven a cabo.

Cabe señalar, que los Clientes de una IFC que intervengan en las operaciones de la IFC serán denominadas inversionistas y solicitantes. Inversionistas son aquellas persona físicas y morales que aporten recursos a los solicitantes. Solicitantes, son aquellas físicas y morales que hubieren requeridos tales recursos a través de la IFC. Los cuales podrán realizar entre ellos: financiamiento colectivo de deuda, financiamiento colectivo de capital y financiamiento colectivo de copropiedad o regalías

Los procesos generales identificados en las IFC fueron los siguientes: Aspectos generales de las IFC y Operaciones de las IFC.

1.5.1. Constancia electrónica sobre riesgos

En términos la LRITF[41] las IFC deberán obtener de los inversionistas constancia electrónica sobre los riesgos a que está sujeta su inversión en la institución. Dicha constancia electrónica deberá recabarse a través de la Plataforma, por única ocasión, previo a la celebración del contrato que les permita realizar Operaciones.

En este subproceso se ha identificado que las IFC en primer lugar deberán dar a conocer, a través de su Plataforma, a sus inversionistas previamente a la celebración del contrato que les permita realizar Operaciones en la Plataforma de que se trate, advertencias respecto de los riesgos a los que estará sujeta su Inversión.

Las advertencias respecto de los riesgos a los que estará sujeta la inversión del inversionista deben ser, por lo menos, las siguientes:

- La imposibilidad de disponer los recursos invertidos en el momento en el que el Inversionista así lo requiera.
- La posibilidad de que no existan las condiciones para que, a través de la institución de financiamiento colectivo, se lleve a cabo la venta de los derechos o títulos que documenten las Operaciones.
- La posibilidad de perder la totalidad de los recursos que se hayan invertido a través de la institución de financiamiento colectivo, en caso de que el Solicitante no pague el financiamiento o este no se pueda recuperar.
- La posibilidad de invertir, a través de la institución de financiamiento colectivo, en sociedades o proyectos en etapa de formación que no tengan historial de operación probado, pudiendo perderse hasta el cien por ciento de la inversión. Además, la posibilidad de no recibir dividendos, ingresos, utilidades o regalías, y que, como resultado de la participación de más Inversionistas en la sociedad o proyecto de que se trate, los derechos corporativos puedan verse disminuidos.
- La posibilidad de que los estados financieros de las sociedades o proyectos en los que se invierta, no estén dictaminados por un auditor externo independiente, por lo que la información financiera podría no reflejar razonablemente la situación financiera de la sociedad o proyecto de que se trate.
- La posibilidad de recibir información inicial y subsecuente limitada en comparación a lo observado en el mercado de valores por lo que, eventualmente, el Inversionista podría no contar con suficiente información para tomar decisiones de inversión.
- La prohibición establecida para las instituciones de financiamiento colectivo de conformidad con lo previsto en el artículo 20 de la LRITF y la imposibilidad para estas a que se refiere el artículo 11, tercer párrafo de dicho ordenamiento. [42]

Las IFC deberán añadir las advertencias acerca de cualquier otro riesgo de inversión que identifiquen y que no esté contemplado en las advertencias señaladas anteriormente.

[41] Artículo 18, Fracción III de la LRITF

[42] Anexo 8 de las Disposiciones de Carácter General Aplicables a las Instituciones de Tecnología Financiera Publicadas en el Diario Oficial de la Federación el 10 de septiembre de 2018, modificadas mediante resolución publicada en el citado Diario el 25 de marzo de 2019.

En segundo lugar, una vez que los Inversionistas confirmen que han leído las advertencias señaladas anteriormente, las IFC recabarán, en un formulario que la propia institución proporcione, las respuestas sobre el conocimiento de los riesgos a que dichos Inversionistas se exponen por su inversión. Dichas respuestas no podrán ser contestadas por los Inversionistas en su totalidad en sentido negativo o positivo.

Cuando de cualquiera de las respuestas se desprenda que lo inversionistas no conocen los riesgos, las IFC deberán interrumpir automáticamente el proceso de contratación y re-direccionar al inversionista a la pantalla donde se describen las advertencias de los riesgos generales de invertir en los solicitantes o proyectos que la IFC de que se trate publique a través de su Plataforma.

Al remitir las respuestas con su firma electrónica avanzada o cualquier otra forma de autenticación de conformidad con lo previsto en el artículo 56, primer párrafo de la LRITF, los inversionistas harán constar electrónicamente que conocen los riesgos asociados a su inversión en los solicitantes o proyectos que la IFC publique a través de su Plataforma.

Las IFC deberán conservar por un plazo mínimo de diez años el comprobante original de la constancia electrónica de riesgos, debidamente archivado, ya sea en formato impreso, o a través de medios electrónicos, ópticos o de cualquier otra tecnología. [43]

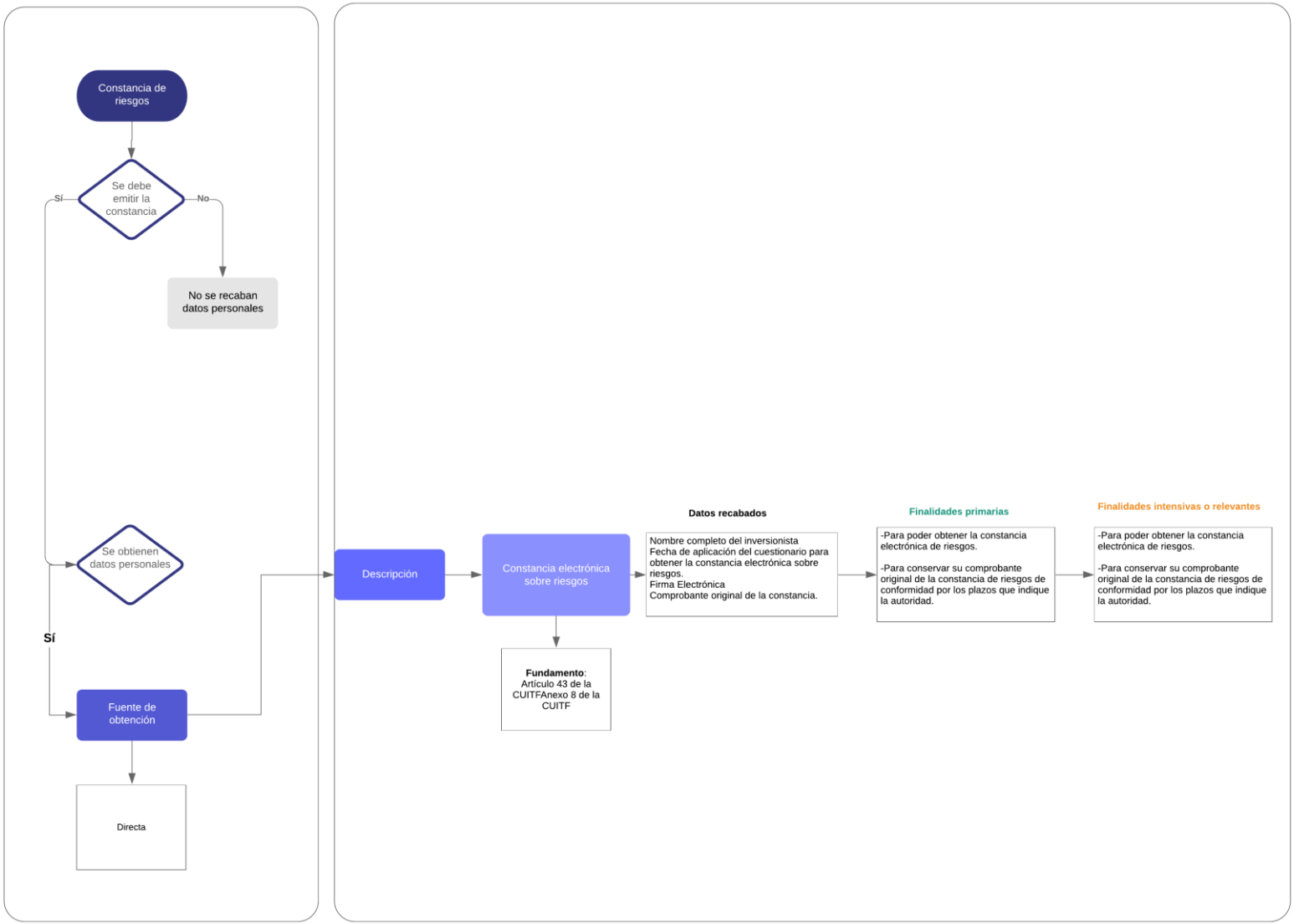
En este subproceso se identificó que de forma directa se obtienen datos personales patrimoniales y/o financieros para obtener la constancia electrónica de riesgos y conservar su comprobante original de la constancia de riesgos por un plazo mínimo de diez años a través de soportes físicos o electrónicos. Estos procesos y sus finalidades se consideran de alto riesgo ya que asignan un nivel de riesgo al titular a partir de una gran cantidad de información que permite la construcción de un perfil detallado del cliente.

El subproceso anterior se resume en el siguiente diagrama:

[43] Artículo 43 de las Disposiciones de Carácter General Aplicables a las Intituciones de Tecnología Financiera Publicadas en el Diario Oficial de la Federación el 10 de septiembre de 2018, modificadas mediante resolución publicada en el citado Diario el 25 de marzo de 2019.

Procesos que involucran el tratamiento de datos en las IFC

Proceso: Características de las operaciones
Subproceso: Constancia electrónica sobre riesgos



1.5.2. Límites de recursos que las IFC podrán mantener a nombre de sus clientes

Dado que la LRITF[44] establece que límites de recursos que las IFC podrán mantener a nombre de sus Clientes o de los que un Cliente podrá disponer a través de dichas IFC, se entiende que las IFC deben mantener un control sobre estos recursos, por lo que se da lugar al tratamiento de datos personales de identificación, autenticación, patrimoniales y/o financieros y transaccionales. Dichos datos serán tratados por las IFC para evitar que superen los límites establecidos por la CNBV, mismos que se enlistan a continuación:

- Tratándose de Financiamiento Colectivo de Deuda de Préstamos Personales entre Personas, el equivalente en moneda nacional a 50,000 UDI's.
- En el caso de Financiamiento Colectivo de Deuda de Préstamos Empresariales entre Personas, de Deuda para el Desarrollo Inmobiliario, de Capital y de Copropiedad o Regalías, el equivalente en moneda nacional a 1'670,000 UDI's.

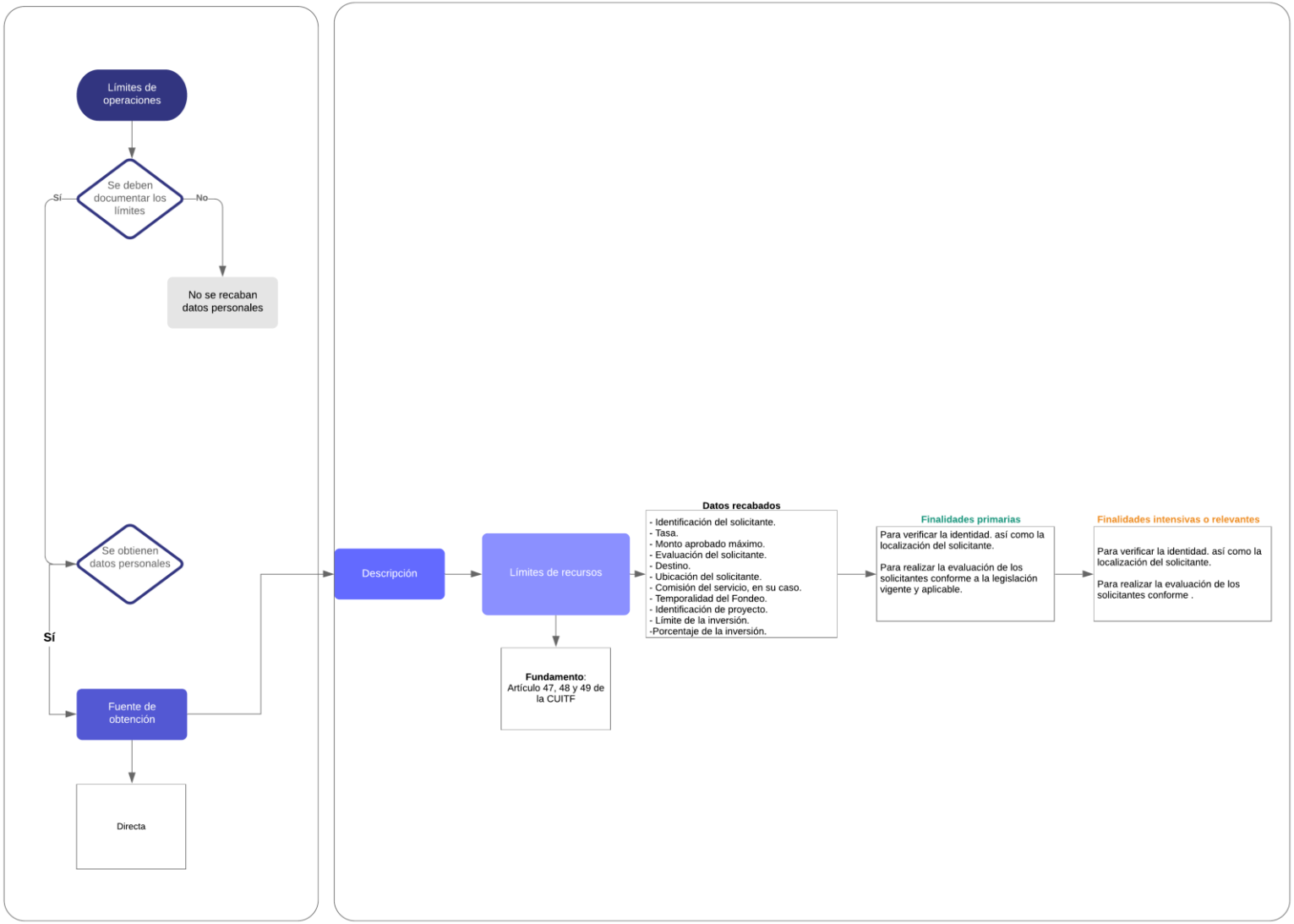
Derivado de este subproceso se identificó que de forma directa se obtienen datos personales de identificación y autenticación, patrimoniales y/o financieros, y transaccionales para verificar la identidad; así como de la localización del solicitante, la evaluación de los solicitantes conforme a la legislación vigente y aplicable y realizar la gestión y administración de los recursos de los clientes de conformidad con los límites establecidos en la legislación vigente y aplicable.

El subproceso anterior se resume en el siguiente diagrama:

[44] Artículo 44 de la LRITF

Procesos que involucran el tratamiento de datos en las IFC

Proceso: Características de las operaciones
Subproceso: Límites de recursos que las IFC podrán mantener a nombre de sus Clientes



1.5.3. Mandatos y comisiones

En términos de la LRITF[45] las IFC pueden celebrar mandatos o comisiones con sus Clientes para la realización de las actividades relacionadas con las Operaciones para temas operativos y demás actividades que tengan por objeto facilitar el ejercicio de los derechos de sus Clientes derivados de las Operaciones, así como la celebración de nuevas Operaciones.

Respecto a dichos mandatos y comisiones se pueden identificar los siguientes:

1. Mandatos y comisiones para Efectuar Operaciones.

En caso de que las IFC pacten mandatos o comisiones con el objeto de que sus clientes efectúen operaciones, la CNBV ha establecido que deberán apegarse a los siguientes términos:

- Tratándose de solicitantes, el plazo de solicitud de financiamiento colectivo, cuya duración deberá ser revelada en todo momento y durante dicho plazo a los inversionistas en la plataforma.
- El plazo en el que se efectuará la entrega, o bien, la ejecución de las gestiones necesarias para que se entreguen los recursos a los que tengan derecho los inversionistas cuando:
    - No se hubiere obtenido el monto requerido para celebrar la operación al término del plazo de solicitud de financiamiento colectivo.
    - En caso de así pactarse, cuando el Solicitante no hubiere confirmado la celebración de la operación al término del plazo de solicitud de financiamiento colectivo.
    - El solicitante realice los pagos correspondientes por las operaciones efectuadas.
- La entrega, o bien, la realización de las gestiones necesarias para que se entreguen los recursos aportados por los Inversionistas a los Solicitantes al término del Plazo de Solicitud de Financiamiento Colectivo o, en caso de así pactarse, cuando se cuente con la confirmación del Solicitante para la celebración de la Operación.
- Para el caso de los mandatos o comisiones a que se refiere el artículo 54 de estas disposiciones, que serán revocables en el momento en que lo decida el Inversionista.[46]

En virtud de lo anterior, se identificó que de forma directa se obtienen datos personales de identificación y autenticación y patrimoniales y/o financieros, para realizar las operaciones a nombre del cliente y verificar la identidad y el tipo de operación del cliente.

2. Mandatos y comisiones para invertir, por cuenta de los Inversionistas, sus recursos o activos virtuales.

En caso de que las IFC, en la ejecución de mandatos o comisiones que tengan por objeto invertir de manera automática, por cuenta de los Inversionistas, sus recursos o activos virtuales que provengan de los pagos efectuados por los financiamientos otorgados a los Solicitantes o de Operaciones no perfeccionadas, deberán:

- Contar con el previo consentimiento expreso para realizar las inversiones automáticas de recursos en su representación y por cuenta de ellos, el cual deberá solicitarse de manera

[45] Artículo 52 de las Disposiciones de Carácter General Aplicables a las Instituciones de Tecnología Publicadas en el Diario Oficial de la Federación el 10 de septiembre de 2018. modificadas mediante resolución publicada en el citado Diario el 25 de marzo de 2019.

[46] Artículo 53 de las Disposiciones de Carácter General Aplicables a las Instituciones de Tecnología Publicadas en el Diario Oficial de la Federación el 10 de septiembre de 2018. modificadas mediante resolución publicada en el citado Diario el 25 de marzo de 2019.

independiente al contrato inicial que se celebre entre los Inversionistas y las instituciones de financiamiento colectivo para la prestación de los servicios que ofrezcan.

- Informar previamente la forma y términos en que se llevarían a cabo las inversiones, los criterios a utilizar para seleccionar a los Solicitantes o proyectos sobre los que se invertirán los recursos, el nivel de riesgo al cual estarán expuestas las inversiones según su metodología de riesgos, así como el monto o porcentaje de recursos que podrán ser invertidos.
- Mantener visible y disponible en la página inicial del Inversionista, una vez iniciada su sesión en la Plataforma, la solicitud de revocación de este tipo de mandatos o comisiones, bastando para que surta efectos la revocación, la simple solicitud. [47]

Se identificó que de forma directa se obtienen datos personales de identificación y autenticación y patrimoniales y/o financieros, para realizar las operaciones de inversión a nombre del cliente y verificar la identidad del solicitante.

Asimismo, las IFC tienen la obligación de obtener el consentimiento expreso del inversionista para realizar inversiones automáticas de recursos en su representación y por cuenta de ellos, mismo que deberá ser obtenido mediante un mecanismo independiente al contrato inicial para la prestación de los servicios que ofrece la IFC al inversionista.

3. Mandatos y comisiones para cobranza extrajudicial.

En caso de que las IFC celebren mandatos o comisiones con sus inversionistas para la ejecución de mandatos o comisiones que tengan por objeto la realización de la cobranza extrajudicial de los derechos de cobro que tengan a su favor los Inversionistas, así como para renegociar los términos y condiciones de los financiamientos, deberán informar a los propios inversionistas la siguiente información previo a la celebración del mandato o comisión:

- Las acciones que llevará a cabo, por sí o a través de terceros, para realizar la cobranza extrajudicial, así como los alcances y objetivos que se pretenden con dicha gestión, incluyendo la resolución de controversias por la vía conciliatoria o de arbitraje.
- Los términos y condiciones en los que podrá pactar con los Solicitantes modificaciones a las condiciones originales para reestructurar o renovar los créditos, hacer quitas o recibir en pago bienes, realizar operaciones de factoraje, venta o cesión de derechos de cobro que tengan los Inversionistas, durante la recuperación extrajudicial, así como informar aquellos para considerar un crédito como incobrable. [48]

En virtud de lo anterior, se identificó que de forma directa se obtienen datos personales de identificación y autenticación y patrimoniales y/o financieros, para realizar a nombre del cliente cobranza extrajudicial de los derechos de cobro que tengan a su favor los inversionistas.

4. Mandatos y comisiones para representar a los Inversionistas en asambleas de accionistas, socios o cualquier órgano de decisión colegiada.

Tratándose de mandatos o comisiones que tengan por objeto representar a los Inversionistas en asambleas de accionistas, socios o cualquier otro órgano de decisión colegiada de los solicitantes, las IFC deberán informar a los inversionistas sobre los asuntos listados en el orden del día que se discutirán en las sesiones correspondientes.[49]

[47] Artículo 54 de las Disposiciones de Carácter General Aplicables a las Instituciones de Tecnología Publicadas en el Diario Oficial de la Federación el 10 de septiembre de 2018. modificadas mediante resolución publicada en el citado Diario el 25 de marzo de 2019.
[48] Artículo 55 de las Disposiciones de Carácter General Aplicables a las Instituciones de Tecnología Publicadas en el Diario Oficial de la Federación el 10 de septiembre de 2018. modificadas mediante resolución publicada en el citado Diario el 25 de marzo de 2019.
[49] Artículo 56 de las Disposiciones de Carácter General Aplicables a las Instituciones de Tecnología Publicadas en el Diario Oficial de la Federación el 10 de septiembre de 2018. modificadas mediante resolución publicada en el citado Diario el 25 de marzo de 2019.

En virtud de lo anterior, se identificó que de forma directa se obtienen datos personales de identificación y autenticación y patrimoniales y/o financieros, para actuar en calidad de representantes de los inversionistas en asambleas de accionistas, socios o de cualquier órgano de decisión colegiada.

5. Informar en sus plataformas las actividades llevadas a cabo en la ejecución de mandatos y comisiones.

Las IFC deben informar, a través de sus Plataformas, las actividades llevadas a cabo en la ejecución de los mandatos o comisiones celebrados, detallando, según corresponda, lo siguiente:

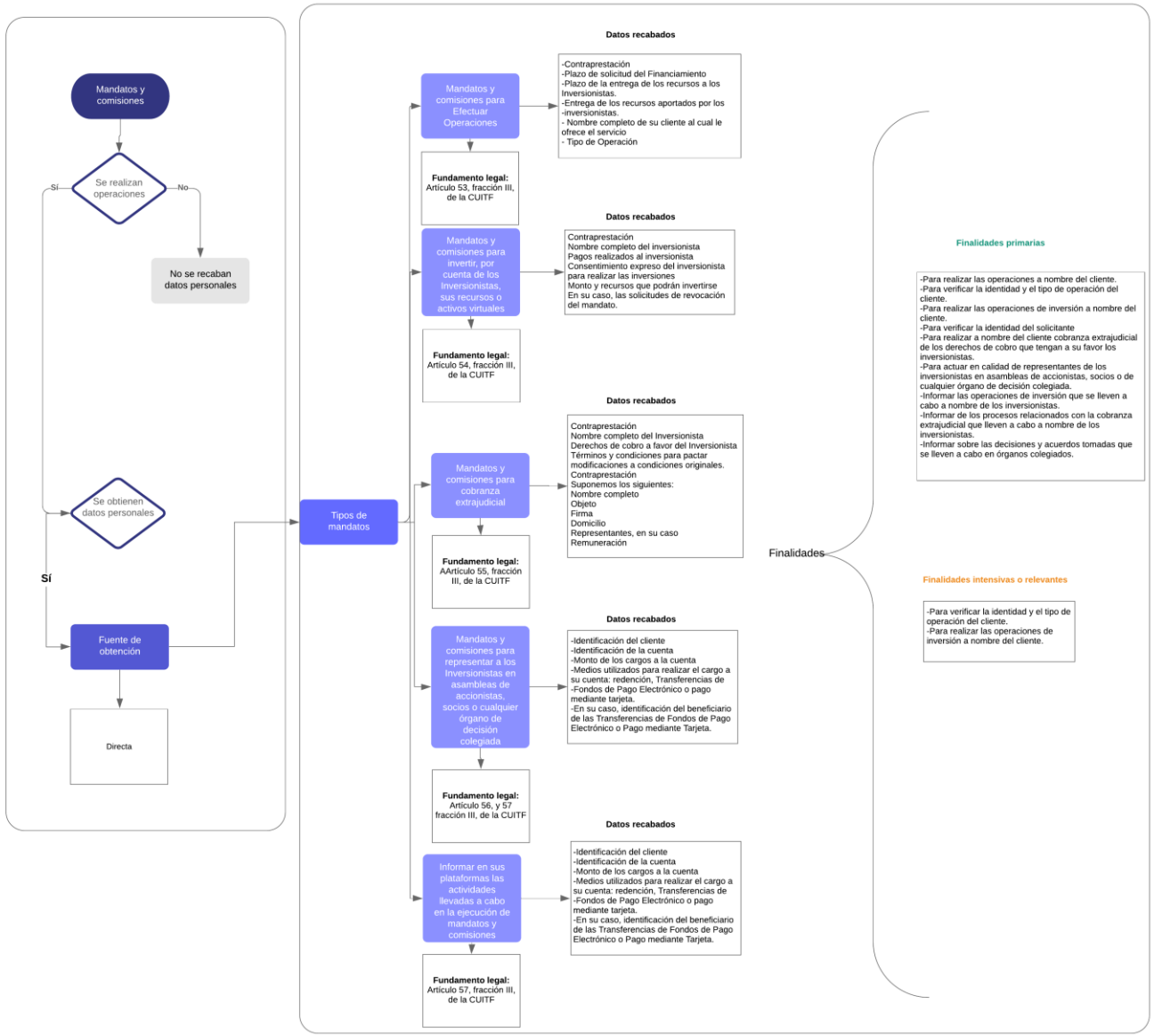
- Tratándose de la inversión de recursos a que se refiere el artículo 54 de estas disposiciones, el o los proyectos o solicitantes en los cuales se realizó dicha inversión, incluyendo los nuevos compromisos de inversión y las inversiones que hayan quedado firmes, los montos, el plazo de solicitud de financiamiento colectivo y demás información relacionada.
- Para el caso de la cobranza extrajudicial, el estado en que se encuentre cualquier proceso que se esté llevando a cabo y los actos que se estén realizando para la cobranza de los financiamientos otorgados, por sí o a través de terceros.
- Respecto de la representación a que se refiere el artículo 56 anterior, los acuerdos y las decisiones tomadas en asambleas de accionistas, socios o cualquier otro órgano de decisión colegiada.

En virtud de lo anterior, se identificó que de forma directa se obtienen datos personales de identificación y autenticación y patrimoniales y/o financieros, para informar las operaciones de inversión que se lleven a cabo a nombre de los inversionistas, informar de los procesos relacionados con la cobranza extrajudicial que lleven a cabo a nombre de los inversionistas e informar sobre las decisiones y acuerdos tomadas que se lleven a cabo en órganos colegiados.

El proceso anterior se resume en el siguiente diagrama:

Procesos que involucran el tratamiento de datos en las IFC

Proceso: Aspectos generales de las IFC
Subproceso: Mandatos y Comisiones



1.6. Operaciones de las IFC

1.6.1. Tipos de financiamiento

Como se vio anteriormente, los clientes de una IFC pueden ser inversionistas o solicitantes, estos Clientes pueden efectuar entre ellos y a través de las IFC las operaciones siguientes:

- *Financiamiento Colectivo de Deuda*, con el fin de que los inversionistas otorguen préstamos, créditos, mutuos o cualquier otro financiamiento causante de un pasivo directo o contingente a los solicitantes;
- *Financiamiento Colectivo de Capital*, con el fin de que los inversionistas compren o adquieran títulos representativos del capital social de personas morales que actúen como solicitantes, y
- *Financiamiento colectivo de copropiedad o regalías,* con el fin de que los inversionistas y solicitantes celebren entre ellos asociaciones en participación o cualquier otro tipo de convenio por el cual el inversionista adquiera una parte alícuota o participación en un bien presente o futuro o en los ingresos, utilidades, regalías o pérdidas que se obtengan de la realización de una o más actividades o de los proyectos de un solicitante.

Las Operaciones se deberán determinar en moneda nacional; asimismo, podrán realizar las referidas Operaciones en moneda extranjera o con activos virtuales, en los casos y sujetos a los términos y condiciones que BANXICO establezca.

1.6.2. Identificación de tratamientos de datos en la operación de las IFC

Además del tratamiento que la IFC realiza de datos personales al momento del alta del cliente. Estas instituciones de financiamiento deben dar tratamiento a datos personales adicionales para que las operaciones puedan llevarse a cabo entre los solicitantes y los inversionistas y así, dar cumplimiento a las obligaciones que establece la LRITF y disposiciones aplicables. Por ejemplo[50]:

I. Dar a conocer a los inversionistas los criterios de selección de los solicitantes y proyectos objeto de financiamiento, la información y documentación que se analiza para esos efectos y las actividades que realiza para verificar la veracidad de dicha información y documentación, incluyendo si los solicitantes cuentan con otro financiamiento colectivo. Las IFC tienen prohibido ofertar proyectos que estén siendo ofertados en otra IFC. Para dar cumplimiento a lo anterior la Ley permite realizar comunicaciones de información con otras IFC, previa la obtención del consentimiento del solicitante.
II. Se debe dar a conocer a los inversionistas los riesgos de los solicitantes y los proyectos, incluyendo como datos personales: indicadores sobre su comportamiento de pago y desempeño y calificación de proyectos y solicitantes.
III. Deberán obtener de forma directa de los inversionistas una constancia de que conocen los riesgos a que esta sujeta su inversión.
IV. Poner a disposición de los inversionistas la siguiente información personal del solicitante: comportamiento de pago del solicitante y su desempeño como cliente de la IFC.
V. Entregar los recursos de los inversionistas a los solicitantes que hubieren seleccionado los propios inversionistas.

Como se mencionó en las obligaciones anteriores, las IFC deberán realizar una comunicación de datos personales en cumplimiento de la obligación de dar a conocer a los inversionistas, a través de su

[50] Art. 18 de la LRIF

plataforma, los siguientes datos personales para la selección y calificación de solicitantes y proyectos. Esto con el objetivo de que los inversionistas puedan tomar una decisión informada:

I. Criterios utilizados para seleccionar a los solicitantes y los proyectos.
II. La forma para verificar la identidad y localización de los posibles solicitantes.
III. El tipo de información y documentación que será recabada para llevar a cabo el análisis y la valoración respectiva de los posibles Solicitantes y, en su caso, las actividades para verificar la veracidad de dicha documentación e información.
IV. El plazo y la forma para que la institución de financiamiento colectivo notifique al posible Solicitante sobre la aceptación o el rechazo de su solicitud.
V. La descripción general de la metodología que utilizará para analizar y determinar el grado de riesgo de los posibles Solicitantes y, en su caso, de los proyectos.

En este sentido, se identificó un tratamiento de datos personales en la selección y calificación de los solicitantes para determinar el grado de riesgo para cada tipo de financiamiento: financiamiento colectivo de deuda, financiamientos colectivos de deuda de préstamos empresariales entre personas que se efectúen con el fin de celebrar una operación de factoraje financiero, financiamiento colectivo de deuda para el desarrollo inmobiliario, financiamiento colectivo de capital, financiamiento colectivo de copropiedad o regalías.

Para determinar el grado de riesgo se realiza el tratamiento de los siguientes datos personales[51]:

I. Financiamiento Colectivo de Deuda:

    a. Evaluación cuantitativa y cualitativa respecto a la solvencia.
    b. Historial crediticio.
    c. Capacidad de pago.
    d. Ingresos estimados.
    e. Relación con otros créditos y pasivos; así como su plazo.
    f. Si el financiamiento esta destinado al desarrollo de un proyecto: historial de negocios o conocimientos técnicos de los administradores o ejecutores del proyecto.
    g. Reporte de información crediticia.
    h. En caso de que existan garantes u obligados solidarios se debe verificar su identidad.
    i. Cuando se trate de garantías reales se deberá cerciorar de la debida titularidad del bien que se otorga y su libertad de gravamen.

II. Financiamiento Colectivo de Deuda de Préstamos Empresariales entre personas que se efectúen con el fin de celebrar una operación de factoraje financiero:

    a. La información requerida para la fracción I.
    b. Evaluación crediticia del deudor de los derechos de crédito que adquirirá el inversionista.
    c. En caso de que los derechos a transmitir deriven de una factura, autenticidad y vigencia de dicha factura.
    d. Verificar que los derechos de crédito no hayan sido transmitidos, cedidos o afectados en garantía.

III. Financiamiento Colectivo de Deuda para el Desarrollo Inmobiliario:

    a. La información requerida para la fracción I.
    b. Monto máximo del financiamiento.
    c. Proporción que deben representar las garantías.

[51] Art. 45 de las CUITF

d. En el supuesto de garantía hipotecaría, el certificado de libertad de gravamen ante el Registro Público, documentación que acredite la titularidad del inmueble y el certificado de que no existe un procedimiento de extinción de dominio o expropiación.
e. Etapa de desarrollo del proyecto.
f. Estudios de mercado.
g. Permisos, licencias, uso de suelo, suministro de agua, drenaje que sustenten la viabilidad del proyecto.

IV. Financiamiento Colectivo de Capital y de Copropiedad y Regalías:

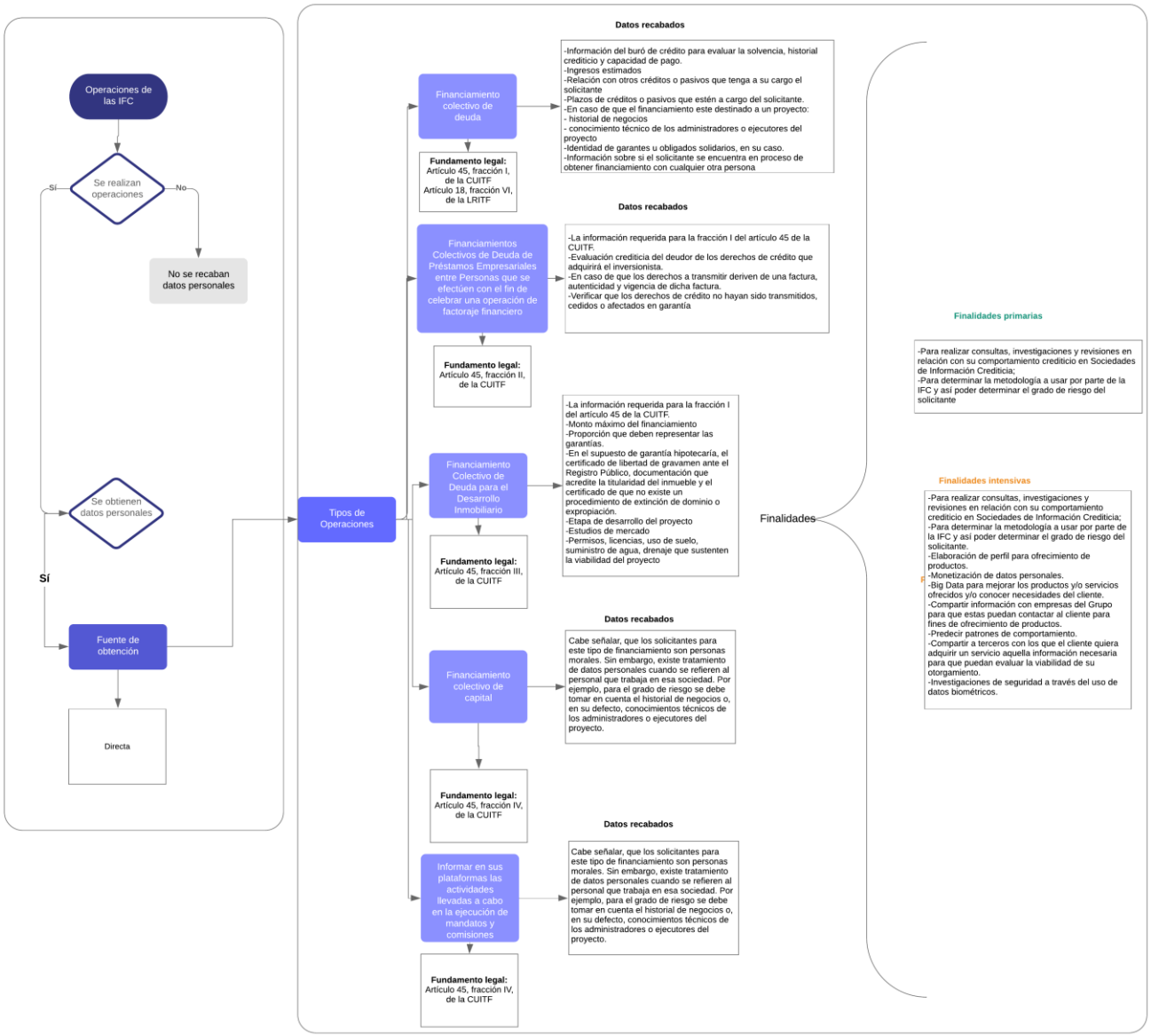
a. Cabe señalar, que los solicitantes para este tipo de financiamiento son personas morales. Sin embargo, existe tratamiento de datos personales cuando se refieren al personal que trabaja en esa sociedad. Por ejemplo, para el grado de riesgo se debe tomar en cuenta el historial de negocios o, en su defecto, conocimientos técnicos de los administradores o ejecutores del proyecto.

V. Mecanismos para verificar que la cuenta de depósito destinada a recibir los recursos de la Operación que se requiera al posible solicitante, este abierta a su nombre en una entidad financiera autorizada para recibir depósitos en territorio nacional o extranjero

El proceso anterior se resume en el siguiente diagrama:

Procesos que involucran el tratamiento de datos en las IFC

Proceso: Operaciones de las IFC
Subproceso: Determinar grado de riesgo del solicitante



1.7. Open banking

El reporte ¿Cuál es el potencial para la banca abierta en México? define al Open Banking o banca abierta como: "un sistema que permite a instituciones financieras compartir cierta información a través de APIs abiertas y seguras. Dentro de estos datos se incluye la información de consumidores que puede ser compartida, con el consentimiento de éstos, con tercero autorizados con el objetivo de recibir servicios más efectivos y eficientes".[52] En el ordenamiento jurídico mexicano este movimiento es consagrado en el artículo 76 de la LRITF el cuál establece la obligación a Entidades Financieras, los transmisores de dinero, las sociedades de información crediticia, las cámaras de compensación a que se refiere la Ley para la Transparencia y Ordenamiento de los Servicios Financieros, las ITF y las sociedades autorizadas para operar con Modelos Novedosos a establecer APIs que posibiliten la conectividad y acceso a los mismos sujetos y terceros especializados en tecnologías de la información. La información que podrán compartirse es la siguiente:

I. *Datos financieros abiertos*: son aquellos generados por las entidades mencionadas en el primer párrafo de este artículo que no contienen información confidencial, tales como información de productos y servicios que ofrecen al público general, la ubicación de sus oficinas y sucursales, cajeros automáticos u otros puntos de acceso a sus productos y servicios, entre otros y según sea aplicable;

II. *Datos agregados*: son los relativos a cualquier tipo de información estadística relacionada con operaciones realizadas por o a través de las entidades mencionadas en el primer párrafo de este artículo, sin contener un nivel de desagregación tal que puedan identificarse los datos personales o transacciones de una persona.

III. *Datos transaccionales*: son aquellos relacionados con el uso de un producto o servicio, incluyendo cuentas de depósito, créditos y medios de disposición contratados a nombre de los clientes de las entidades mencionadas en el primer párrafo de este artículo, entre otra información relacionada con las transacciones que los clientes hayan realizado o intentado realizar en su Infraestructura Tecnológica. Estos datos, en su carácter de datos personales de los clientes, solo podrán compartirse con la previa autorización expresa de éstos.

Es importante señalar, que dentro de la categoría de información que las entidades financieras del artículo 76 pueden compartirse solamente los datos transaccionales son considerados dato personal, ya que es la única información concerniente a una persona física identificada o identificable. Asimismo, el artículo 76 establece que la información de los datos transaccionales solo podrá ser utilizada para los fines estrictamente autorizados por el cliente. Actualmente, las disposiciones de carácter general a las que se refiere el artículo 76, no han sido emitidas. Estas disposiciones deberán establecer:

1. Los estándares necesarios para la interoperabilidad de interfaces de programación de aplicaciones, incluyendo el diseño, desarrollo y mantenimiento.
2. Los mecanismos de seguridad de las interfaces para el acceso, envío u obtención de datos e información.
3. Definir la información crítica para el buen funcionamiento de las aplicaciones que requieran el uso de estas interfaces.
4. Mecanismos por medio de los cuales se obtendrá el consentimiento del cliente.

[52] David Beardmore, et. Al. "*¿Cuál es el potencial de la banca abierta en México?: Recomendaciones y plan de trabajo para adoptar el estándar de banca abierta*", Louise Bolotin, México, abril, 2018, p.10

Esta falta de regulación no permite conocer con certeza jurídica el proceso de Open Banking; sin embargo, describiremos aquél del Reino Unido, el cual ha sido el mayor promotor de la banca abierta a nivel mundial. El proceso de Open Banking en el Reino Unido es el siguiente:

El ecosistema inicia cuando un cliente ve la opción de compartir sus datos con un tercero para obtener un servicio financiero personalizado. Si el cliente desea continuar será direccionado a su proveedor de datos (ej. su banco) para iniciar sesión y brindar su consentimiento expreso (sin compartir sus credenciales de log-in con el tercero). Posteriormente, el cliente será direccionado automáticamente con el tercero quien en este punto tendrá acceso, a través de APIs abiertas, a la información determinada del cliente, la cual solo podrá tratar en función de la finalidad del permiso y por el tiempo establecido de dicho cliente.[53]

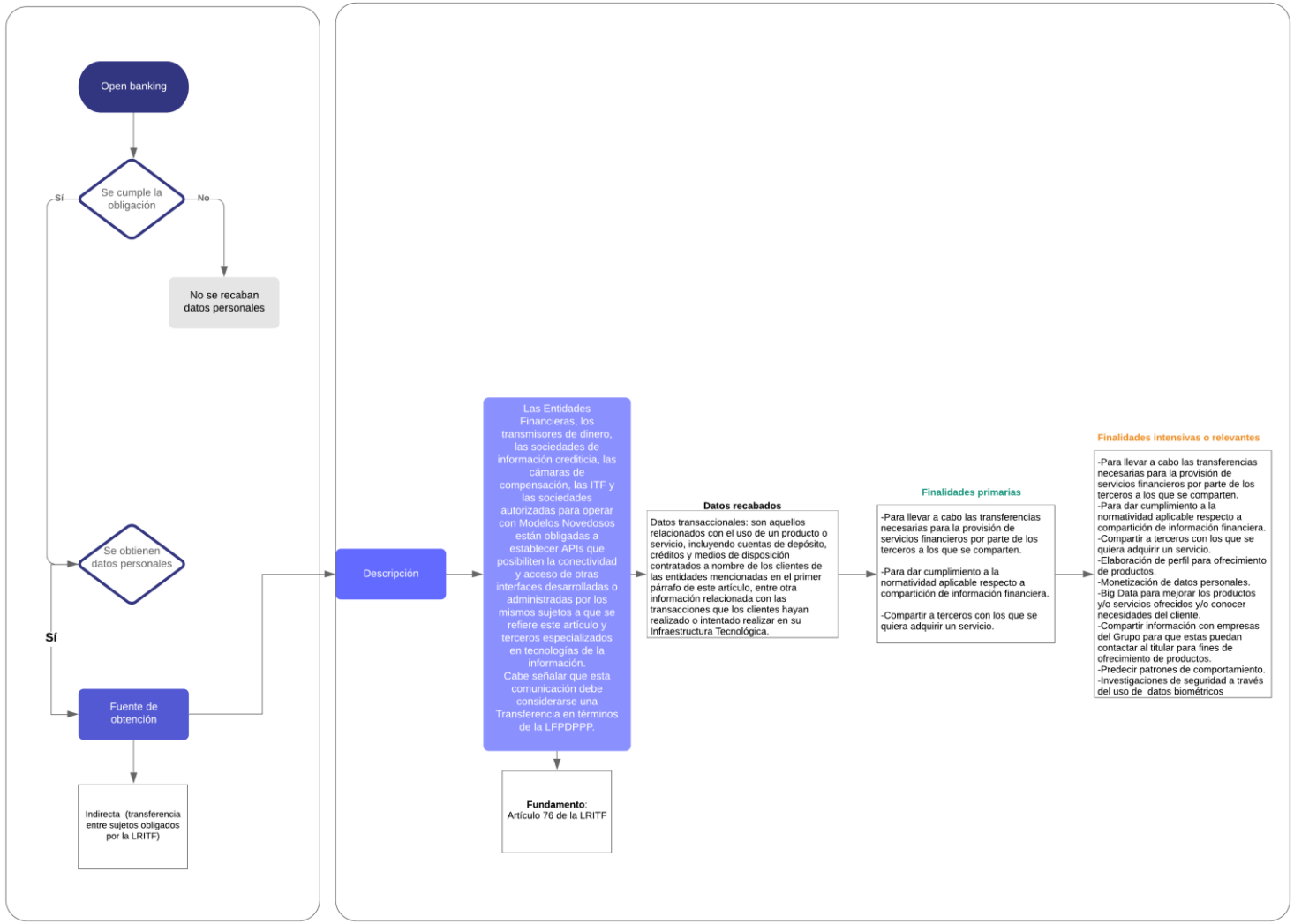
En este proceso se ha identificado que de forma directa se obtienen datos personales de identificación y autenticación, contacto, demográficos, ubicación geográfica para llevar a cabo las transferencias necesarias para la provisión de servicios financieros por parte de los terceros a los que se comparten, dar cumplimiento a la normatividad aplicable respecto a compartición de información financiera y compartir a terceros con los que se quiera adquirir un servicio.

El proceso anterior se resume en el siguiente diagrama:

[53] Open Banking Working Group, *The Open Banking Standard (OBS): unlocking the potential of open banking to improve competition, efficiency and stimulate innovation,* Louise Bolotin, Reino Unido, Londres, 2016, p. 20
Disponible en:
https://www.paymentsforum.uk/sites/default/files/documents/Background%20Document%20No.%202%20-%20The%20Open%20Banking%20Standard%20-%20Full%20Report.pdf

Procesos que involucran el tratamiento de datos en las IFC

Proceso: Open banking



2. Procesos que involucran el tratamiento de datos personales en las IFPE

A continuación, se presentan los procesos y subprocesos relacionados con el tratamiento de datos en las IFPE reguladas por la LRITF. Los procesos generales identificados fueron los siguientes:

1. Alta del cliente;
2. PLD/CFT;
3. Obligación de conservar documentos;
4. Mecanismos de seguimiento y agrupaciones de operaciones;
5. Operaciones que realizan las IFPE;
6. Características de las operaciones;
7. Cierre de cuentas;
8. Requerimientos de información de BANXICO;
9. *Open banking*.

2.1. Alta de cliente

El proceso de alta de cliente inicia cuando una persona física o moral busca obtener una cuenta de fondos de pago electrónico, la cual deberá ser registrada por la IFPE, previo a la firma del contrato que celebre con la persona física o moral. Derivado de lo anterior, los clientes interesados deberán firmar un contrato con las IFPE que tenga por objeto celebrar las operaciones autorizadas por parte de las autoridades competentes. Antes de la firma del contrato la persona física o moral deberá entregar directamente la información y documentación necesaria para el expediente que la IFPE debe mantener, para que ésta de cumplimiento a la normatividad aplicable y este en posibilidad de brindar los servicios de financiamiento colectivo a las personas físicas o morales que deseen contratar sus servicios.[54] Cabe señalar, que este expediente es requerido por un tema de PLD/CFT; sin embargo, es parte integrante del proceso necesario para dar de alta a un cliente. Una vez que el cliente haya entregado la información y documentación necesaria a la IFPE, esta realizará un registro de la cuenta y el cliente podrá abonar, disponer, transferir los FPE emitidos a su nombre en las cuentas que la IFPE administre. Estas operaciones se definen más adelante en las características de las operaciones de la circular 12/2018 de BANXICO.

Para integrar el expediente las IFPE deberán obtener de sus potenciales Clientes la geolocalización del dispositivo móvil desde el cual el cliente abra su cuenta o celebre el contrato respectivo. Con independencia de esto, la IFPE deberá requerir, en función del tipo de cliente, la información que se señala en los diagramas[55]

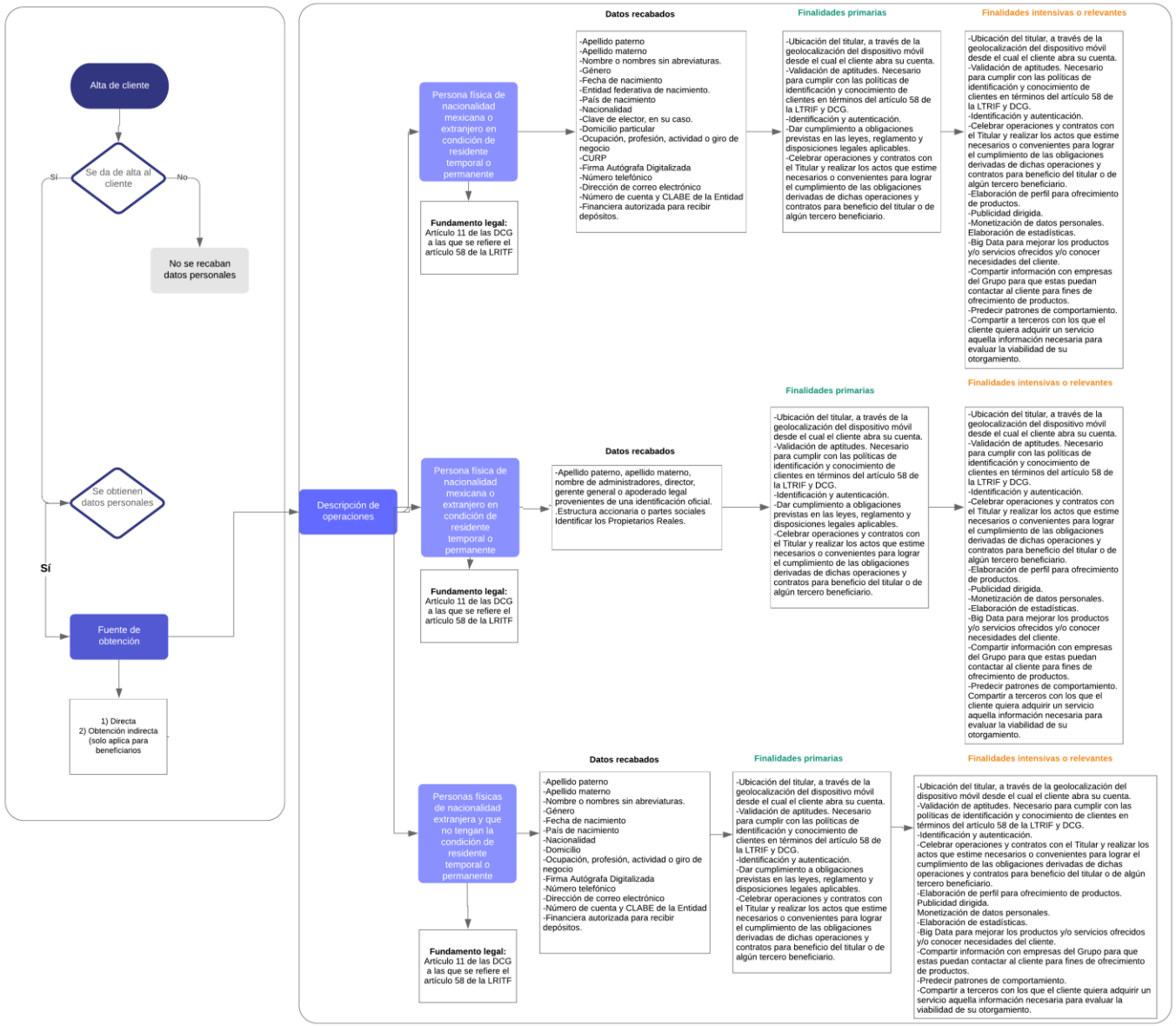
Cuando las cuentas o contratos amparen operaciones con efectivo, con Activos Virtuales o transferencias internacionales, adicionalmente a los datos personales referidos anteriormente se deberá realizar una entrevista con el cliente potencial o su representante legal, esta entrevista podría realizarse vía remota. Estas entrevistas deberán de conservarse en archivos o registros.[56]

El proceso anterior se resume en el siguiente diagrama:

[54] Art. 11 de las DCGA58.
[55] La información se desprende del artículo 11 de las DCGA58.
[56] Obligaciones establecidas en el art. 11 de las DCGA58.

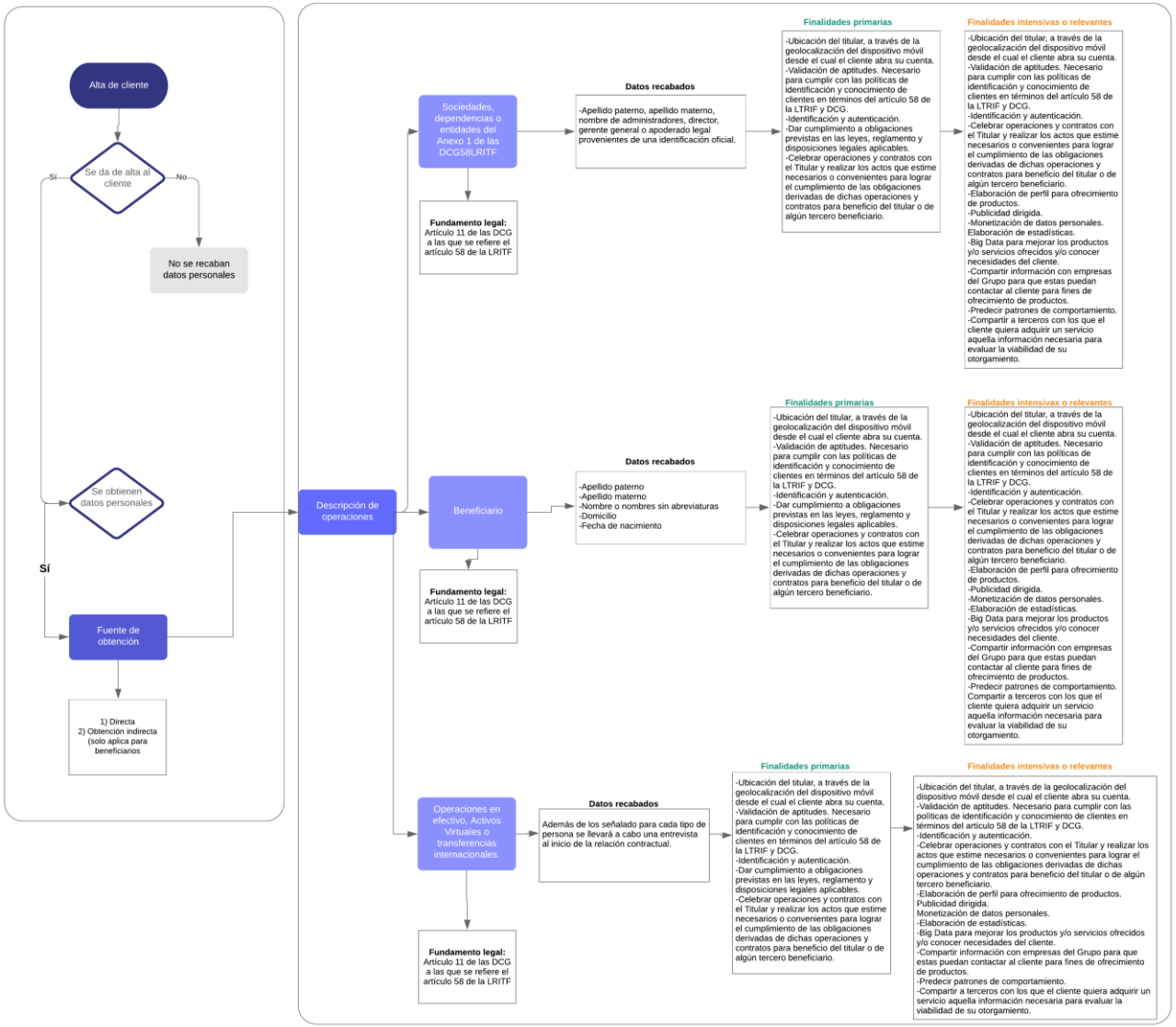
Procesos que involucran el tratamiento de datos en las IFPE

Proceso: Alta de Cliente (Primera parte)
Subproceso: Identificación de los datos personales provenientes de documento válido, el cual deberá digitalizarse



Procesos que involucran el tratamiento de datos en las IFPE

Proceso: Alta de Cliente (Segunda parte)
Subproceso: Identificación de los datos personales provenientes de documento válido, el cual deberá digitalizarse



2.2. PLD/CFT

Como proceso general relacionado con el tratamiento de datos personales en las ITF (IFC e IFPE) se identificó la obtención de datos personales de los clientes para dar cumplimiento a las previsiones del articulo 58 de la LRITF y las correspondientes DCGA58. Derivado del análisis de las operaciones de las IFC en cumplimiento a la normatividad señalada se identificaron los siguientes subprocesos en materia de PLD/CFT: 1) reportes que se deberán remitir a la SHCP; 2) intercambio de información; 3) clasificación de clientes por grado de riesgo: bajo, medio o alto; 4) políticas de conocimiento de clientes; 5) listas de personas bloqueadas; y 6) auditorías para revisar el cumplimiento de las DCGA58.

2.2.1. Reportes que se deben remitir a la SHCP

En el momento en el que se emite un reporte, es importante tener en cuanta que existe una transferencia de datos personales, esta transferencia se deberá apegar a lo que se establece en la normatividad para llevar un proceso claro y apegado a le ley.

En concreto, los reportes que se deberán remitir a la SCHP son los siguientes:

I. Reportes de Operaciones Relevantes, los cuales deberán realizarse dentro de 10 primero días hábiles de los meses de enero, abril, julio y octubre.
II. Reportes de operaciones en efectivo en moneda extranjera, los cuales deberán realizarse dentro de 10 primero días hábiles de los meses de enero, abril, julio y octubre. Los reportes aplicarán cuando se realice una operación por un monto igual o superior a 500 dlls.
III. Reporte de transferencias internacionales, el cual se deberá remitir mensualmente por cada Operación de transferencia internacional que haya recibido o enviado cualquiera de sus Clientes durante dicho mes, por un monto igual o superior a 1,000 dlls o su equivalente en pesos o la moneda extranjera en que se realice con el respectivo cargo o abono a las cuentas.
IV. Reporte de Operaciones Inusuales, el cual se deberá remitir dentro de los siguientes tres días hábiles que concluya la sesión del Comité que la dictamine como tal.
V. Reporte de Operaciones con Activos Virtuales, los cuales deberán realizarse dentro de 10 primero días hábiles de los meses de enero, abril, julio y octubre. Dicho reporte deberá incluir la compra o venta de Activos Virtuales.
VI. Reporte de Operaciones Internas Preocupantes, el cual se deberá remitir dentro de los siguientes tres días hábiles que concluya la sesión del Comité que la dictamine como tal.

Estos reportes que se deberán presentar a la SHCP, por conducto de la CNBV, contienen los siguientes datos personales:

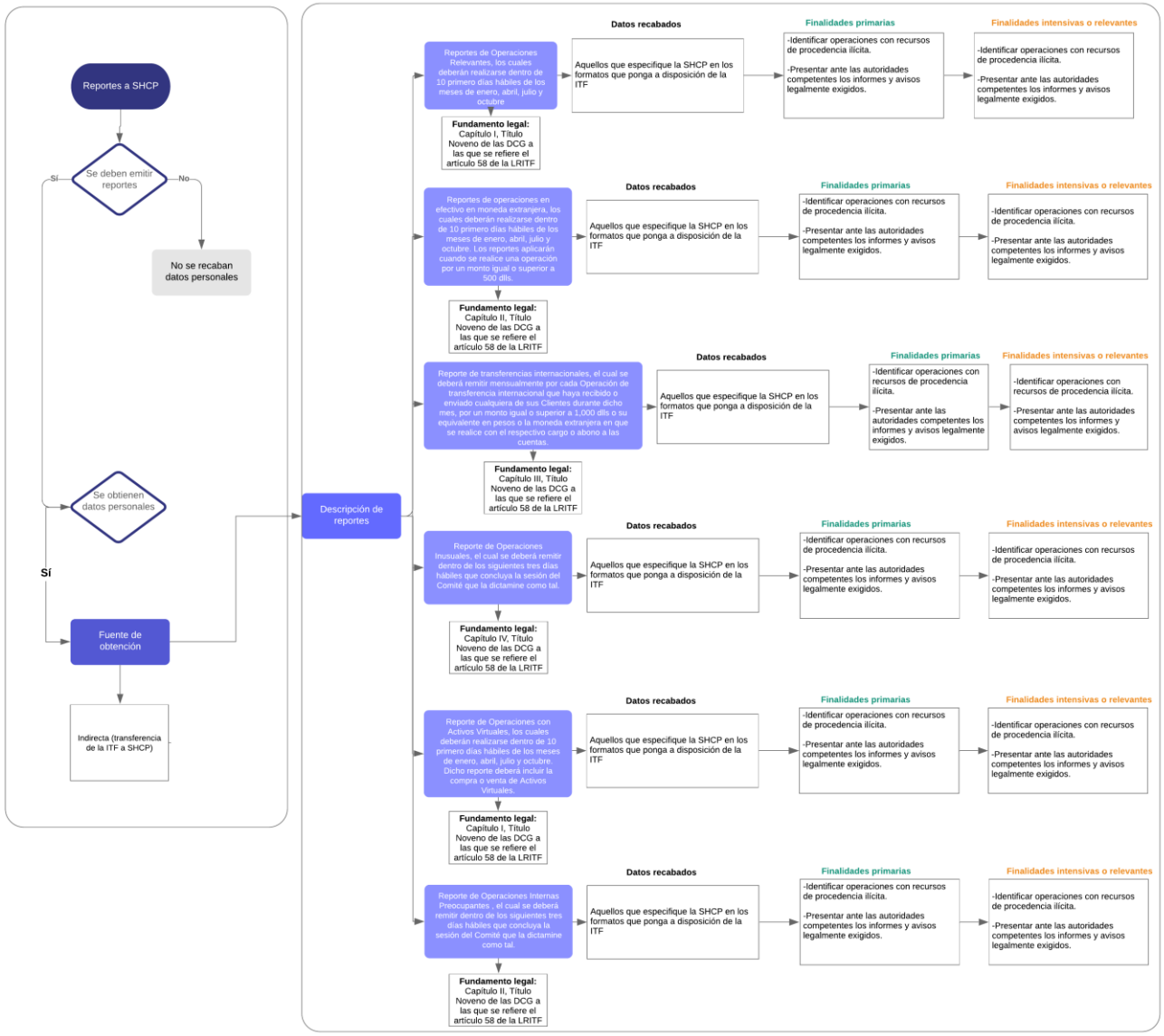
a) Actos, operaciones y servicios que realicen con sus clientes y las operaciones entre estos, según corresponda,
b) Todo acto, operación o servicio que realicen los miembros del consejo de administración, directivos, funcionarios, empleados, factores y apoderados que pudiesen contravenir o vulnerar la adecuada aplicación de las DCG158.[57]

El subproceso anterior se resume en el siguiente diagrama:

[57] Art. 58 de la LRITF

Procesos que involucran el tratamiento de datos en las IFPE

Proceso: PLD/CFT
Subproceso: Reportes que se deberán remitir a la SHCP



2.2.2. Intercambio de información

Se identifican tres tipos de tratamientos en el proceso de intercambio de información: el intercambio de información con autoridades, el intercambio entre autoridades y el intercambio de información entre entidades financiera. Este tratamiento se identifica como una transferencia de datos personales con el fin de dar cumplimiento a la LRITF para prevenir el lavado de dinero y el financiamiento al terrorismo.

2.2.2.1.1. Intercambio de información con autoridades

Las IFPE estarán obligadas a proporcionar a la CNBV y a BANXICO, en el ámbito de sus respectivas competencias, la información que dichas Autoridades Financieras les requieran sobre sus Operaciones y aquellas realizadas entre sus Clientes, incluso respecto de alguna o algunas de ellas en lo individual, los datos que permitan estimar su situación financiera y, en general, aquella que sea útil a la CNBV o a BANXICO para proveer el adecuado cumplimiento de sus funciones, en la forma y términos que las propias Autoridades determinen. [58]

Con el objeto de preservar la estabilidad financiera, evitar interrupciones o alteraciones en el funcionamiento del sistema financiero o del sistema de pagos, así como para facilitar el adecuado cumplimiento de sus funciones, la SHCP, las Comisiones Supervisoras y BANXICO, podrán intercambiar entre sí la información que tengan en su poder por haberla obtenido:

d) En el ejercicio de sus facultades;
e) Como resultado de su actuación en coordinación con otras entidades, personas o autoridades, y
f) Directamente de otras autoridades.

Las Autoridades financieras deberán celebrar convenios de intercambio de información en los que se especifique la información objeto de intercambio y se determine los términos y condiciones a los que deberán de sujetarse.[59]

Las Autoridades Financieras deberán tener suscrito un acuerdo de intercambio de información con autoridades financieras del exterior de que se trate en el que se contemple el principio de reciprocidad.[60]

Tanto la CNBV como BANXICO pueden abstenerse de proporcionar información cuando el uso que se le pretenda dar sea distinto a aquel para el cual haya sido solicitada, a la seguridad nacional o a los términos convenidos en el acuerdo de intercambio de información.

2.2.2.1.2. Intercambio de información entre IFPE

Las ITF podrán intercambiar información de las Operaciones, actividades y servicios que realicen con sus Clientes o de estos entre sí, con el objeto de fortalecer las medidas y procedimientos para prevenir y detectar actos, omisiones u operaciones que pudiesen actualizar los supuestos previstos en los artículos 139 Quáter o 400 Bis del CPF o favorecer, prestar ayuda, auxilio o cooperación de cualquier especie para la comisión de delitos en contra de sus Clientes o de la propia IFPE. [61]

[58] Art. 70 de la LRITF
[59] Art. 74 de la LRITF
[60] Art. 75 de la LRITF
[61] Art. 77 de las DCGA58.

Para el intercambio de información las IFPE deberán seguir lo siguiente:

a) Se pueden realizar entre dos o mas ITF
b) Ser solicitados por los funcionarios de las IFPE autorizados para tales efectos mediante escrito en donde se especifique el motivo y clase de información que se requiera. Esta solicitud puede ser remitida de forma electrónica o digital asegurando la confidencialidad de la información.
c) La respuesta a esa solicitud debe remitirse por escrito firmando un funcionario autorizado en un plazo no mayor a 30 días naturales contados a partir de la fecha de la solicitud, misma que puede ser remitida de la misma forma que la solicitud, siempre asegurando la confidencialidad de la información.
d) La información proporcionada solo puede ser utilizada por la ITF solicitante salvo que sea compartida con otras ITF.
e) Las IFPE podrán compartir con otras ITF la información que consideren relevante para fines del art 77 de las disposiciones, a través de mecanismos que para tales efectos establezca siempre y cuando se cumpla con lo dispuesto en el presente capitulo. [62]

La IFPE que comparta con otras ITF información, deberá conservar la misma información y documentación, misma que deberá estar a disposición de la SHCP y CNBV, dentro del plazo que la propia CNBV establezca.

Cuando se trate del Intercambio de Información con otras Entidades Financieras, así como con centros cambiarios, transmisores de dinero y asesores en inversiones.

Las IFPE que formen parte de grupos financieros en términos de la Ley para Regular las Agrupaciones Financieras, podrán intercambiar cualquier tipo de información sobre las Operaciones, actividades y servicios que realicen con sus Clientes, con las otras Entidades Financieras que formen parte del mismo grupo que estén facultadas para ello conforme a las disposiciones aplicables en materia de prevención de operaciones con recursos de procedencia ilícita y financiamiento al terrorismo, siempre que celebren entre ellas un convenio en el que estipulen lo siguiente:

a) El tratamiento confidencial que se le dará a la información intercambiada.

b) Los cargos de los funcionarios autorizados para realizar el mencionado intercambio.

La IFPE deberá conservar toda la información y documentación soporte que acredite tanto el procedimiento realizado para tal fin como la información intercambiada. [63]

Tratándose del Intercambio de Información con Entidades Financieras Extranjeras es importante mencionar que:

a) Únicamente se puede intercambiar información con las Entidades Financieras extranjeras que sean determinadas por la SHCP.
b) Las IFPE deberán convenir con las mismas entidades el tratamiento confidencial de la información intercambiada y los cargos de los funcionarios autorizados por ambas partes para realizar dicho intercambio.

c) Las IFPE deberán enviar a la SHCP a través de la CNBV mediante los medios que la misma designe,

[62] Art. 78 de las DCGA58.
[63] Art. 80 de las DCGA58.

copia de formato que contenga la información intercambiada [64]

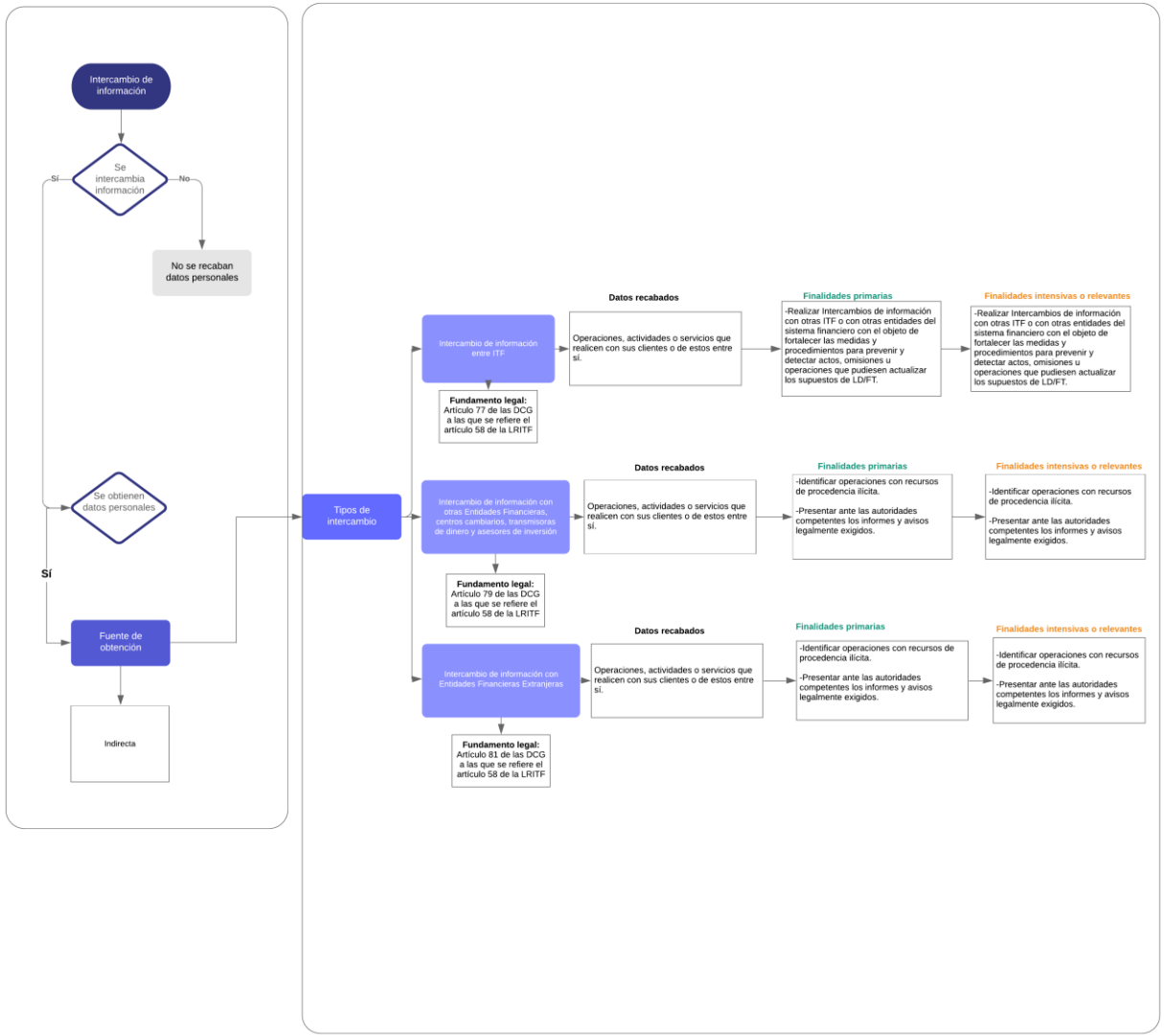
En este subproceso se identificó que de forma directa se obtienen datos personales de identificación, contacto, demográficos, ubicación geográfica, características de dispositivos electrónicos, patrimoniales y/o financieros, laborales y biométricos para realizar Intercambios de información con otras IFPE o con otras entidades del sistema financiero con el objeto de fortalecer las medidas y procedimientos para prevenir y detectar actos, omisiones u operaciones que pudiesen actualizar los supuestos de LD/FT.

El subproceso anterior se resume en el siguiente diagrama:

[64] Art. 81 de las DCGA58.

Procesos que involucran el tratamiento de datos en las IFPE

Proceso: PLD/CFT
Subproceso:Intercambio de información



2.2.3. Clasificación de clientes por grado de riesgo

Para establecer el Grado de Riesgo, las IFPE deben diseñar e implementar una metodología para evaluar el grado del riesgo a las que se encuentran expuestas derivado de productos, servicios, clientes, áreas geográficas, etc.

La metodología deberá establecer y describir todos los procesos que se llevarán a cabo para identificar el Grado de Riesgo así como la información que resulte aplicable. [65]

Para diseñar la metodología deberán cumplir con lo siguiente:

a) Identificar el elemento a evaluar, en este caso Tipo de Clientes
b) Utilizar un método para medir el Riesgo
c) Identificar los Mitigantes que la IFPE tiene implementados al momento de diseñar la metodología, considerando políticas, criterios medidas y procedimientos internos contenidos en su Manual de Cumplimiento, con la finalidad de establecer el efecto que estos tendrán sobre los indicadores y elementos de Riesgo.[66]

Las IFPE deberán asegurarse de:

a) Que no existan inconsistencias entre la información que incorporen y la que obre en sistemas autorizados
b) Utilizar la información correspondiente en un periodo mínimo de doce meses

En el supuesto de que se detecte existencia de mayores o nuevos riesgos para las IFPE, deberán modificar las políticas, criterios, medidas y procedimientos correspondientes. Las modificaciones serán revisadas por las IFPE en un plazo no mayor a 12 meses contados a partir de que la propia IFPE cuente con los resultados de su implementación.[67]

De la clasificación del Grado de Riesgo del Cliente

El modelo de evaluación de Riesgo con el que deberán contar las IFPE, deberá apegarse en todo momento a la metodología a la que se hace referencia en los párrafos anteriores, para clasificar a sus Clientes por Grado de Riesgo, el cual deberá estar establecido en su Manual de Cumplimiento. Las clasificaciones deberán de establecer tres Grados de Riesgo, siendo estos bajo, medio y alto, y pueden establecer los grados intermedios que consideren necesarios, apegándose siempre a la metodología implementada para la misma clasificación. [68]

Las IFPE deben considerar mínimo los primeros seis meses la información proporcionada por cada uno de sus clientes para determinar el Grado de riesgo. Las evaluaciones de grado de riesgo se deberán llevar a cabo cada seis meses con la finalidad de determinar si el grado de riesgos diferente al establecido en un inicio. Entre mas alto sea el grado del riesgo, la frecuencia de evaluación incrementa. [69]

Algunos puntos importantes a considerar para determinar el grado del riesgo del Cliente a través de la metodología ya mencionada anteriormente son:

I. Características inherentes de la persona:
    a. Antecedentes del cliente

[65] Art. 3 de las DCGA58.
[66] Art. 4 de las DCGA58.
[67] Art. 5 de las DCGA58.
[68] Art. 29 de las DCGA58.
[69] Art. 30 de las DCGA58.

b. Tipo de persona
c. Fecha de nacimiento o constitución
d. Giro o actividad
e. Nacionalidad
f. Lugar de residencia
g. Fuentes de ingreso
h. Naturaleza o propósito de la relación que tenga con la IFC

II. Características transaccionales:
a. Tipo y numero de productos y servicios contratados
b. Volumen en número y monto de Operaciones
c. Frecuencia de Operaciones
d. Número de contrapartes
e. Origen y destino de los recursos
f. Instrumento monetario
g. Tipo de moneda. [70]

Clientes de grado de riesgo alto son:

a) Los no residentes en el país
b) Cuando las operaciones que los clientes realicen estén vinculadas o tengan efectos en los países o jurisdicciones siguientes:
iii. Que la legislación mexicana considera que aplican regímenes fiscales preferentes.
iv. Que las autoridades mexicanas, organismos internacionales o agrupaciones intergubernamentales en materia de prevención de operaciones con recursos de procedencia ilícita o financiamiento al terrorismo de los que México sea miembro determinen que no cuenten con medidas para prevenir, detectar y combatir dichas operaciones, o bien, cuando la aplicación de dichas medidas sea deficiente. (art 70)
c) Personas políticamente expuestas extranjeras [71]

Las IFPE, en las Operaciones que realicen con Clientes clasificados con Grado de Riesgo alto, deberán:

Para el caso de personas físicas
a) Adoptar medidas reforzadas para conocer el origen y destino de los recursos.
b) Obtener, en su caso, los datos señalados en el Título Tercero, Capítulo I de las DCGA58, en los términos que al efecto prevean en su Manual de Cumplimiento elaborado por las propias IFPE, respecto del cónyuge y dependientes económicos del Cliente, así como de las sociedades y asociaciones con las que mantenga vínculos patrimoniales.

Para el caso de personas morales,
Obtener mayor información de sus principales accionistas o socios, según corresponda, debiendo consultar para confirmar los datos, los registros electrónicos de la Secretaría de Economía para verificar la información proporcionada por el Cliente.

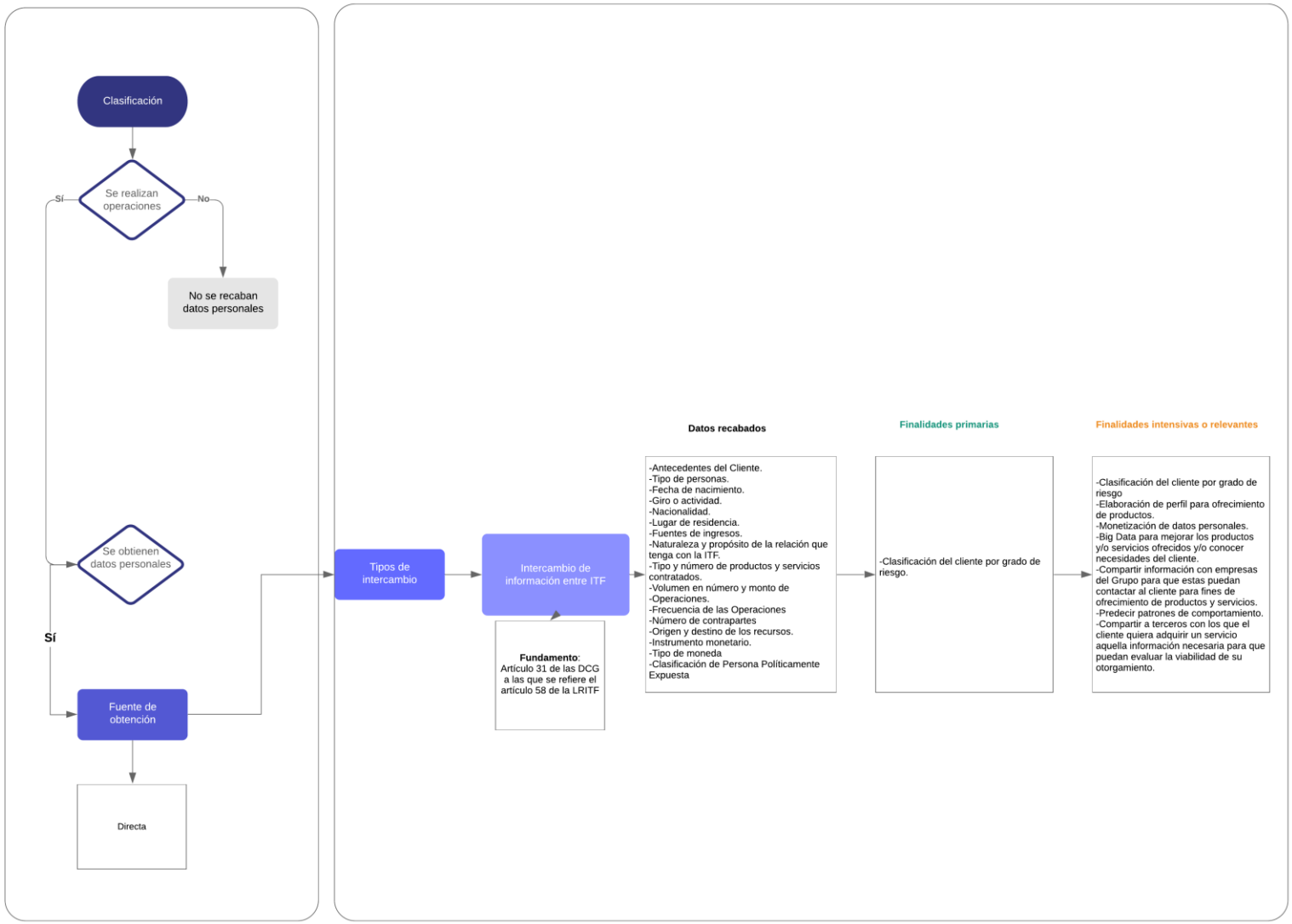
Personas Políticamente Expuestas extranjeras
Obtener, además de los datos a que se refiere el presente artículo, la documentación señalada en el Título Tercero, Capítulo I de las DCGA58, respecto de las personas físicas y morales antes señaladas en este párrafo.[72]

El subproceso anterior se resume en el siguiente diagrama:

[70] Art. 31 de las DCGA58.
[71] Art. 33 de las DCGA58.
[72] Art. 38 de las DCGA58.

Procesos que involucran el tratamiento de datos en las IFPE

Proceso: PLD/CFT
Subproceso: Clasificación por grado de riesgo



2.2.4. Políticas de conocimiento de clientes

Las IFPE están obligadas a elaborar una política de conocimiento de sus Clientes, que deberá incluir:

a) Las políticas, criterios, medidas, procedimientos y controles para mitigar los Riesgos,
b) Procedimientos para dar seguimiento y monitorear las Operaciones, actividades o servicios realizados por sus Clientes.
c) Procedimientos para el debido conocimiento del perfil transaccional de cada uno de sus Clientes.
d) Supuestos en que las Operaciones se aparten del perfil transaccional de cada uno de sus Clientes y, en caso de cambios significativos en dicho perfil, los casos en que procede la revisión y actualización del expediente de identificación del Cliente que sobre este mantenga la IFPE.
g) Medidas para la identificación de posibles Operaciones Inusuales.
h) Criterios para establecer y, en su caso, modificar el grado de Riesgo previamente determinado a un Cliente.[73]

Esta política se basa en el grado de Riesgo que representa el Cliente.

Las IFPE, para determinar el perfil transaccional de sus Clientes deberán considerar, al menos, lo siguiente:

a) La información proporcionada por el Cliente, por los empleados o funcionarios de la IFPE con base en su cartera de Clientes, o bien, la que obre en los archivos de la IFPE.
b) El monto, número, tipo, naturaleza y frecuencia de las Operaciones que, de forma habitual o recurrente, realice el Cliente.
c) El origen y destino de los recursos o bienes objeto de la Operación.
d) La información de geolocalización del dispositivo móvil desde el cual el Cliente, en su caso, realice la Operación, actividad o servicio con la respectiva IFPE.
e) Los demás elementos y criterios que determinen las propias IFPE para tales efectos.

Las IFPE, deben de considerar los seis primeros meses iniciando la relación comercial, la información que proporcione cada uno de sus Clientes para determinar su perfil transaccional inicial y deberán realizar una evaluación a fin de determinar si es necesario o no modificarlo.[74]

Los directivos de una IFPE con facultades para autorizar que se celebren contratos o realización de Operaciones, deberán otorgar aprobación de forma escrita, digital o electrónica.[75]

Para los casos en que las IFPE detecten que un Cliente reúne los requisitos para ser considerado Persona Políticamente Expuesta y, además, como de Grado de Riesgo alto, dichas IFPE deberán, de acuerdo con lo que al efecto establezcan en su Manual de Cumplimiento, obtener la aprobación de una de las personas a que se refiere el artículo 39, a efecto de llevar a cabo la Operación de que se trate. [76]

En caso de que se presuma que alguno de los clientes actúa en nombre y representación e un tercero, la IFPE deberá solicitar al Cliente información necesaria para identificar al Propietario Real de los recursos o bienes objeto de la Operación.[77]

[73] Art. 34 de las DCGA58.
[74] Art. 35 de las DCGA58.
[75] Art. 39 de las DCGA58.
[76] Art. 40 de las DCGA58.
[77] Art. 42 de las DCGA58.

Se deberán establecer mecanismos de seguimiento y agrupación de operaciones que realicen sus clientes. Los mecanismos deberán ser mas estrictos respecto a:

a) Instituciones de Financiamiento Colectivo: cuando sus Clientes realicen Operaciones durante un mes calendario, en efectivo por un monto igual o superior al equivalente en moneda nacional o extranjera, o Activos Virtuales a doce mil quinientas unidades de inversión.
b) Instituciones de Fondos de Pago Electrónico: cuando sus Clientes realicen Operaciones durante un mes calendario, en efectivo o en fondos de pago electrónico, en moneda nacional o extranjera, o Activos Virtuales, por un monto igual o superior a siete mil quinientas unidades de inversión.

Asimismo, las IFPE deberán de llevar un registro de clientes respecto de las operaciones mencionadas anteriormente que contendrá:

a) Los datos de la política de identificación del cliente a que se refieren el artículo 11 de las Disposiciones Generales, según se trate de personas físicas o morales.
b) Fecha y monto de cada una de las Operaciones que haya realizado el Cliente.

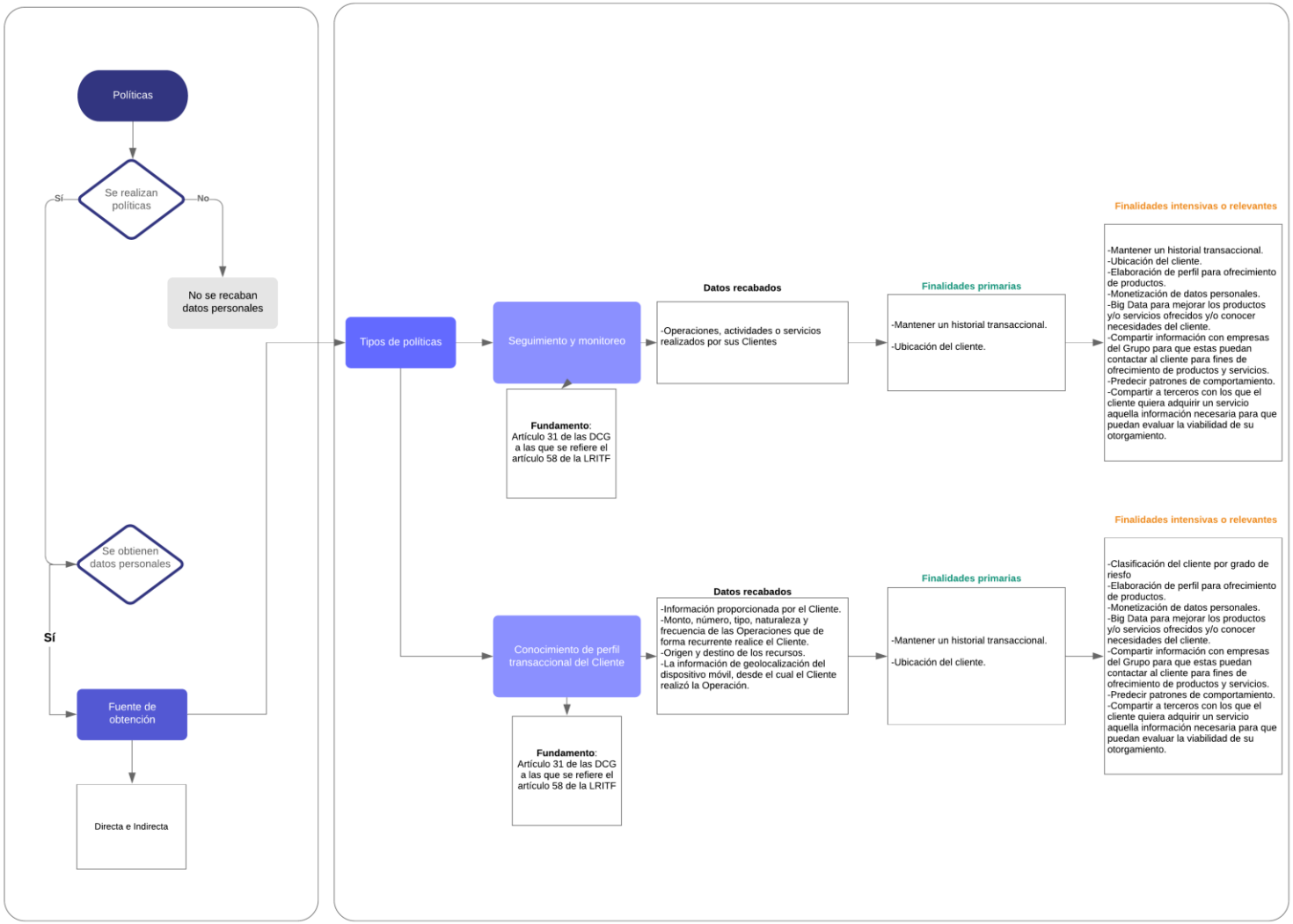
Las IFE deberán conservar la información contemplada en este artículo para proporcionarla a la SHCP y a la CNBV, a requerimiento de esta última. [78]

El subproceso anterior se resume en el siguiente diagrama:

[78] Art. 43 de las DCGA58.

Procesos que involucran el tratamiento de datos en las IFPE

Proceso: PLD/CFT
Subproceso: Política de conocimiento de clientes



2.2.4.1. Listas de personas bloqueadas

De conformidad con el artículo 58 de la LRITF las IFPE deberán suspender de forma inmediata la realización de actos, Operaciones o servicios con los Clientes que la SHCP les informe mediante una lista de personas bloqueadas que tendrá el carácter de confidencial. La lista de personas bloqueadas tendrá la finalidad de prevenir y detectar actos, omisiones u Operaciones que pudieran ubicarse en los supuestos previstos en la fracción I del párrafo primero de este artículo. Esta lista se pondrá a disposición de la IFPE, a través de la CNBV para que esta adopte los mecanismos que permita identificar a los clientes que se encuentren dentro de estas listas.[79]

El artículo 61 de las DCGA58 establece los parámetros que utiliza la SHCP para introducir personas a la lista de personas bloqueadas, estos son los siguiente:

I. Aquellas que se encuentren en las listas derivadas de las resoluciones 1267 (1999) y sucesivas, y 1373 (2001) y las demás que sean emitidas por el Consejo de Seguridad de las Naciones Unidas o las organizaciones internacionales.
II. Aquellas que den a conocer autoridades extranjeras, organismos internacionales o agrupaciones intergubernamentales y que sean determinadas por la SHCP en términos de los instrumentos internacionales celebrados por el Estado Mexicano con dichas autoridades, organismos o agrupaciones, o en términos de los convenios celebrados por la propia SHCP.
III. Aquellas que den a conocer las autoridades nacionales competentes por tener indicios suficientes de que se encuentran relacionadas con los delitos de financiamiento al terrorismo, operaciones con recursos de procedencia ilícita o los relacionados con los delitos señalados, previstos en el CPF.
IV. Aquellas que estén compurgando sentencia por los delitos de financiamiento al terrorismo u operaciones con recursos de procedencia ilícita, previstos en el CPF.
V. Aquellas que las autoridades nacionales competentes determinen que hayan realizado o realicen actividades que formen parte, auxilien, o estén relacionadas con los delitos de financiamiento al terrorismo u operaciones con recursos de procedencia ilícita, previstos en el CPF.
VI. Aquellas que omitan proporcionar información o datos, la oculten, encubran o impidan conocer el origen, localización, destino o propiedad de recursos, derechos o bienes que provengan de delitos de financiamiento al terrorismo u operaciones con recursos de procedencia ilícita, previstos en el CPF o los relacionados con estos.

Cuando la IFPE identifique que dentro de las listas de personas bloqueadas se encuentra alguno de sus clientes, deberá tomar las medidas siguientes[80]:

I. Suspender de manera inmediata la realización de cualquier acto, actividad, Operación o servicio relacionado con el Cliente identificado en la Lista de Personas Bloqueadas.
II. Remitir a la SHCP, por conducto de la CNBV, dentro de las veinticuatro horas contadas a partir de que conozca dicha información, un reporte de Operación Inusual

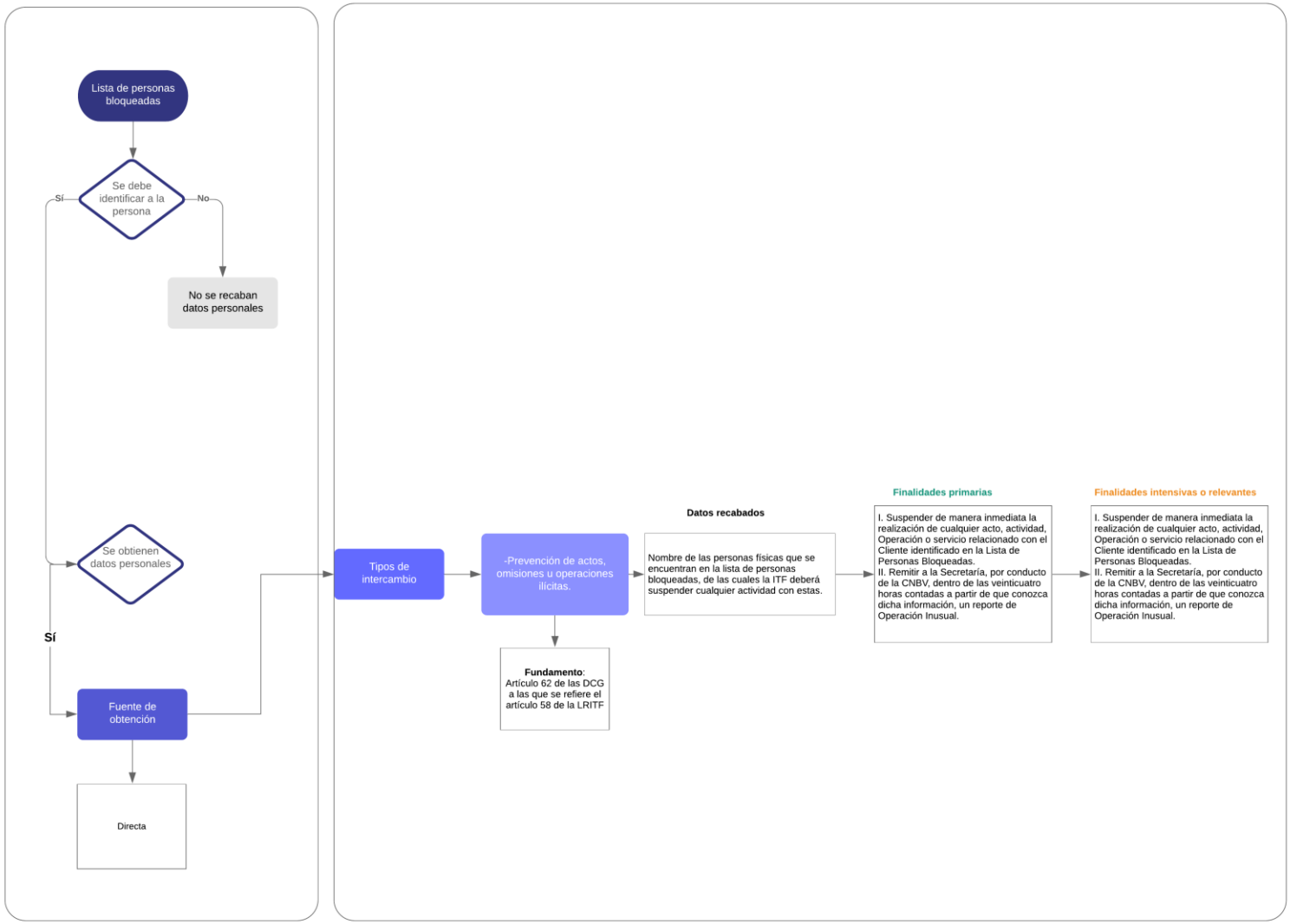
Asimismo, cuando la IFPE haya suspendido los actos, Operaciones, actividades o servicios con sus clientes, de manera inmediata deberán hacer del conocimiento dicha situación, esta notificación podrá realizarse a través de medios electrónicos.[81]

El subproceso anterior se resume en el siguiente diagrama:

[79] Art. 60 de las DCGA58.
[80] Art. 62 de las DCGA58.
[81] Ídem

Procesos que involucran el tratamiento de datos en las IFPE

Proceso: PLD/CFT
Subproceso: Obligaciones de las ITF respecto a la lista de personas bloqueadas



2.2.4.2. Auditoría para revisar el cumplimiento de las DCGA58

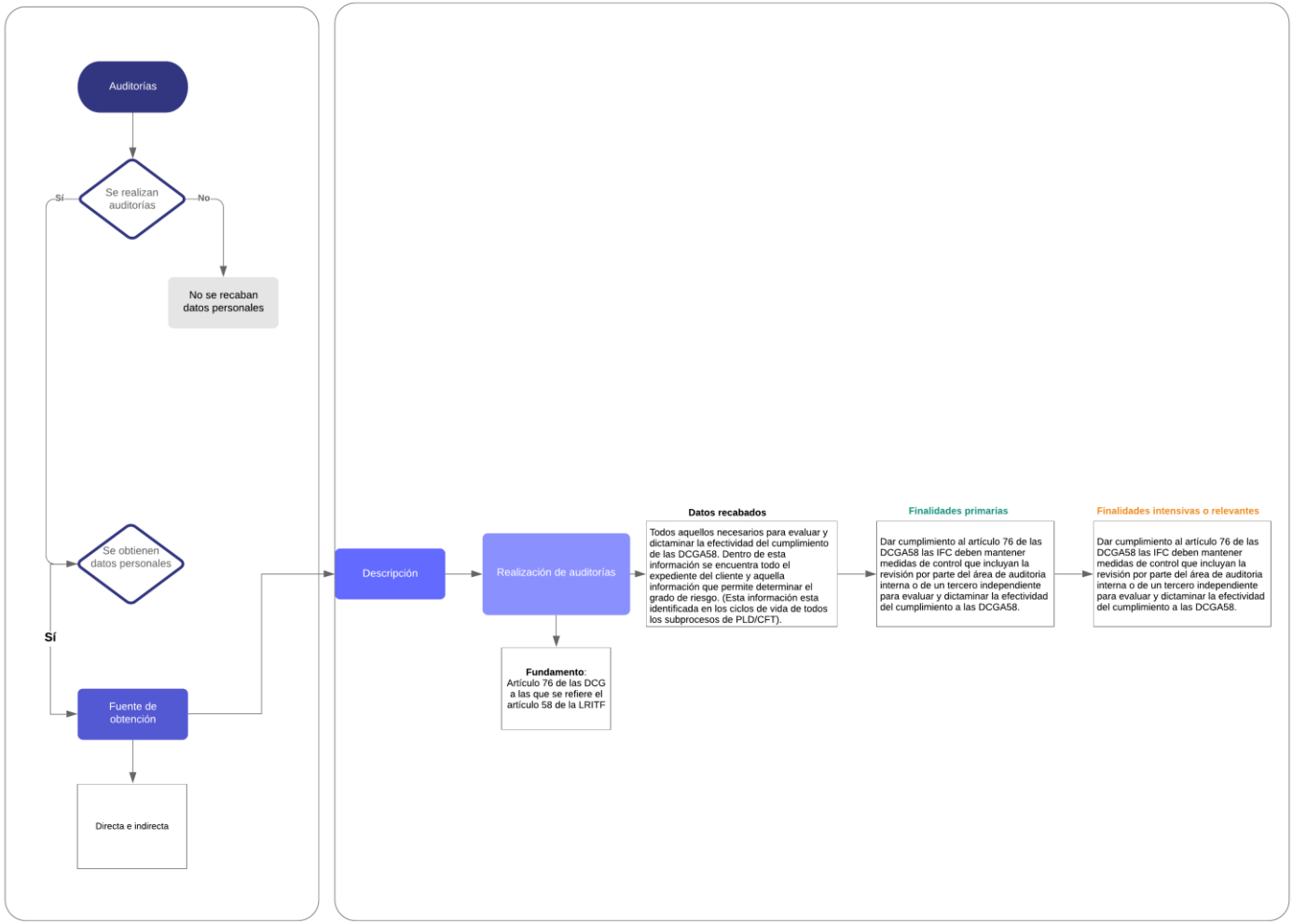
De conformidad con el artículo 76 de las DCGA58 las IFPE deben mantener medidas de control que incluyan la revisión por parte del área de auditoria interna o de un tercero independiente para evaluar y dictaminar la efectividad del cumplimiento a las DCGA58. En este sentido, se pude identificar una comunicación de datos personales entre la IFPE y el tercero independiente que realice la evaluación del cumplimiento a las DCGA58.

Los resultados de la revisión deberán presentarse al administrador único o a la dirección general y, en su caso, al comité de la IFC a manera de informe, a fin de avaluar la eficacia operativa de las medidas implementadas y dar seguimientos a programas de acciones correctivas. El responsable de suscribir la revisión deberá haber obtenido la certificación prevista en el artículo 4, fracción X de la Ley de la CNBV. Es importante señalar, que la información deberá ser conservada por un plazo no menor a 5 años y remitirse a la CNBV dentro de los 60 días naturales siguientes al cierre del ejercicio que corresponda la revisión.

El subproceso anterior se resume en el siguiente diagrama:

Procesos que involucran el tratamiento de datos en las IFPE

Proceso: PLD/CFT
Subproceso: Auditoría para revisar el cumplimiento de las DCGA58



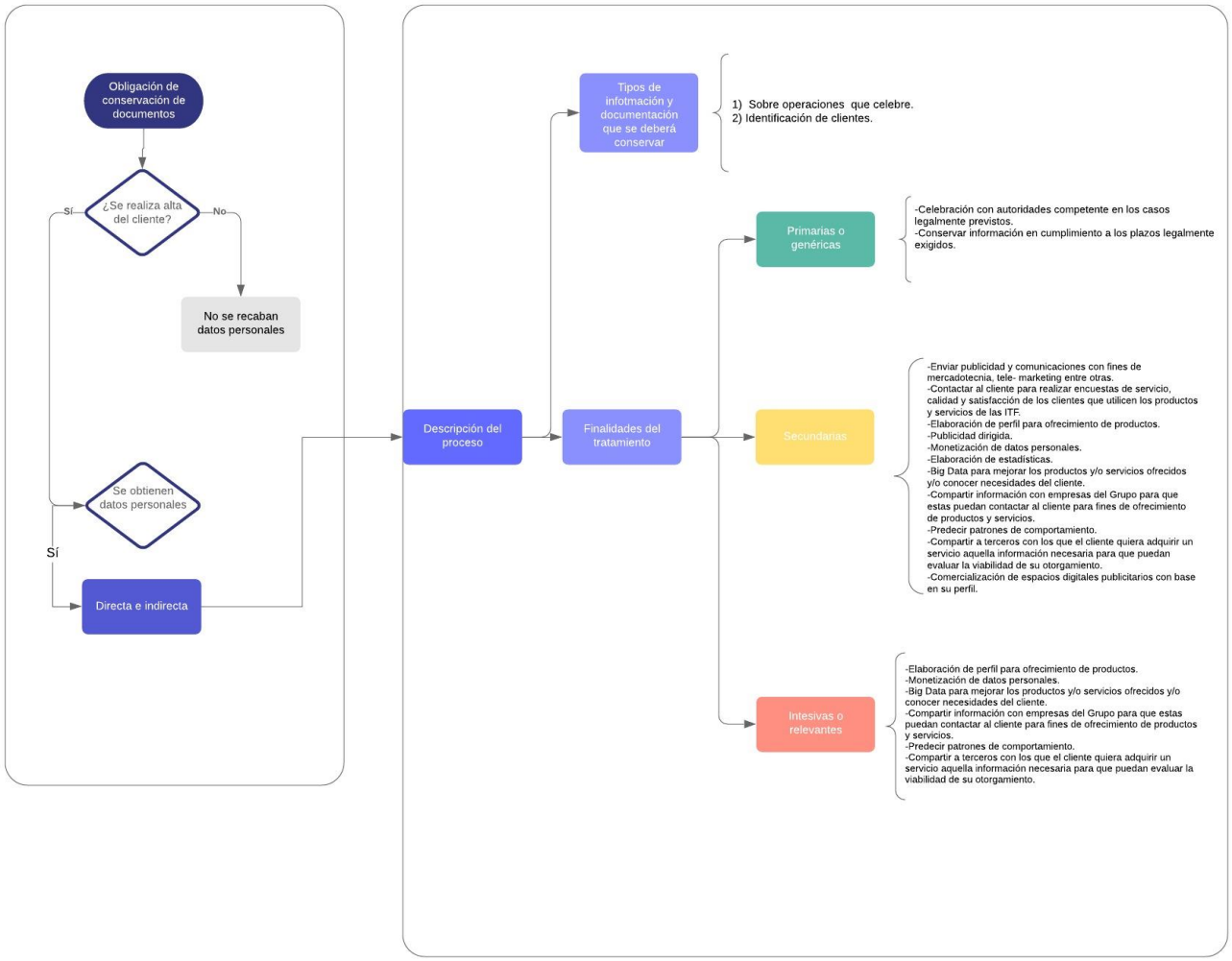
2.3. Conservación de documentos

En este subproceso se identificó que dentro de los procesos las IFPE tienen la obligación de conservar la información y documentación sobre las operaciones que celebre; así como, la información y documentación de la identificación de sus clientes. Derivado de lo anterior, se constató que de forma directa se obtienen datos personales de identificación y autenticación, contacto, demográficos, ubicación geográfica, características de dispositivo electrónico, patrimoniales y/o financieros, crediticios, laborales y biométricos para fines de colaboración con autoridades competentes en los casos legalmente previstos y conservar información en cumplimiento a los plazos legalmente exigidos.

El subproceso anterior se resume en el siguiente diagrama:

Procesos que involucran el tratamiento de datos en las IFPE

Proceso: Obligación de conservación de documentos



2.4. Mecanismos de seguimiento y agrupación de operaciones

Los mecanismos de seguimiento y agrupación de operaciones es una obligación que deberán cumplir las IFPE mediante mecanismos que permitan identificar a los clientes y a las operaciones que estos realizan, independientemente del monto mediante el cual están operando. Este seguimiento y agrupación de las operaciones del cliente obliga a la IFPE a llevar a cabo un registro del cliente respecto a las operaciones, el cual contendrá lo siguiente:

I. Los datos de identificación necesarios para dar de alta a un cliente. (obtenidos de forma directa)
II. Fecha y monto de cada una de las operaciones que haya realizado un cliente. (obtenidos de forma indirecta)

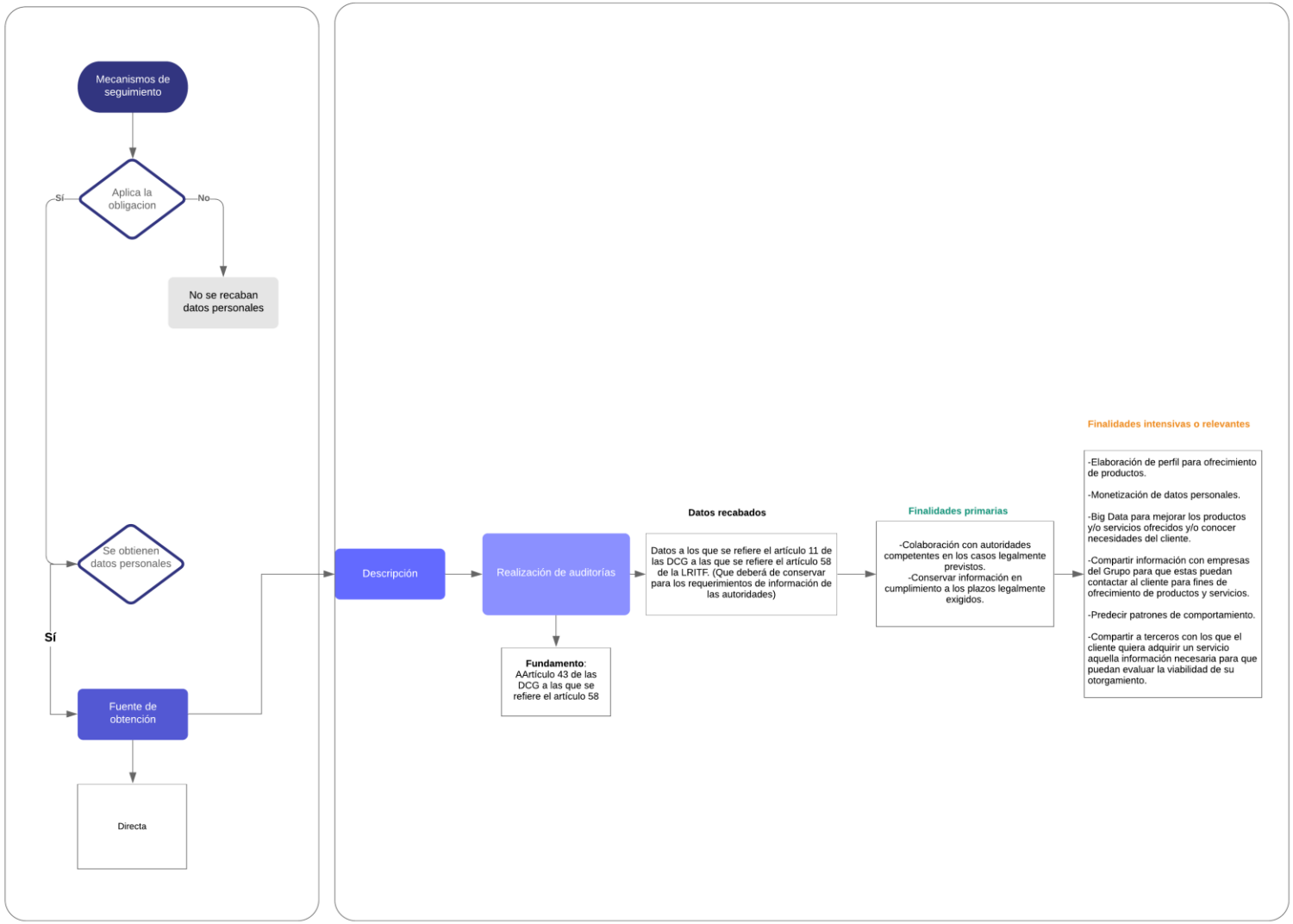
Esta información deberá ser conservada para proporcionarla a las SHCP y la CNBV, a requerimiento de esta última

En este sentido, se identifica el tratamiento de datos ya que por una parte existe la conservación de este expediente, independiente de aquél que fue resultado del alta del cliente. Asimismo, obliga a las IFPE a comunicar dichos datos a las autoridades competentes.

El proceso anterior se resume en el siguiente diagrama:

Procesos que involucran el tratamiento de datos en las IFPE

Proceso:Mecanismos de seguimiento y agrupación de las operaciones



2.5. Operaciones que realizan las IFPE de conformidad con la circular 12/2018 de Banco de México y sus características

En términos de lo dispuesto por el artículo 22 de la LRITF, las IFPE son personas morales autorizadas por la CNBV, previo acuerdo del Comité Interinstitucional al que hace referencia la LRITF, para prestar de forma habitual y profesional los servicios de emisión, administración, redención y transmisión de fondos de pago electrónico a través de aplicaciones informáticas, interfaces, páginas de internet o cualquier otro medio de comunicación electrónica o digital, por medio de los siguientes actos:

1. Abrir y llevar una o más cuentas de fondos de pago electrónico por cada cliente, en las que se realicen registros de abonos equivalentes a la cantidad de fondos de pago electrónico emitidos contra la recepción de una cantidad de dinero, en moneda nacional o extranjera, o de activos virtuales determinados.
2. Realizar transferencias de fondos de pago electrónico entre sus clientes mediante los respectivos abonos y cargos en las correspondientes cuentas.
3. Realizar transferencias de determinadas cantidades de dinero en moneda nacional o, sujeto a la previa autorización de BANXICO, en moneda extranjera o de activos virtuales, mediante los respectivos abonos y cargos en las cuentas de fondos de pago electrónico, entre sus clientes y aquellos de otra institución de fondos de pago electrónico, así como cuentahabientes o usuarios de otras entidades financieras o de entidades extranjeras facultadas para realizar operaciones similares.
4. Entregar una cantidad de dinero o activos virtuales equivalente a la misma cantidad de fondos de pago electrónico en una cuenta de fondos de pago electrónico, mediante el respectivo cargo en dicha cuenta.
5. Mantener actualizado el registro de cuentas de fondos de pago electrónico y modificarlo en relación con el ingreso, transferencia y retiro de fondos de pago electrónico.

Asimismo, en términos del artículo 25 de la LRITF las IFPE pueden realizar también las siguientes operaciones:

1. Emitir, comercializar o administrar instrumentos para la disposición de fondos de pago electrónico.
2. Prestar el servicio de transmisión de dinero.
3. Prestar servicios relacionados con las redes de medios de disposición.
4. Procesar la información relacionada con los servicios de pago correspondientes a los fondos de pago electrónico o a cualquier otro medio de pago.
5. Otorgar créditos o préstamos, en la forma de sobregiros en las cuentas que administren conforme a la LRITF, derivados únicamente de la transmisión de fondos de pago electrónico, sujetos a las condiciones establecidas en la LRITF.
6. Realizar operaciones con activos virtuales, en términos de lo dispuesto en la LRITF.
7. Obtener préstamos y créditos de cualquier persona, nacional o extranjera, destinados al cumplimiento de su objeto social, salvo para la emisión de fondos de pago electrónico o el otorgamiento de crédito conforme a la fracción V del artículo 25 de la LRITF.
8. Emitir valores por cuenta propia.
9. Constituir depósitos a la vista o a plazo en entidades financieras autorizadas para recibirlos.
10. Adquirir o arrendar los bienes muebles e inmuebles necesarios para la realización de su objeto y enajenarlos cuando corresponda.
11. Poner en contacto a terceros con la finalidad de facilitar la compra, venta o cualquier otra transmisión de activos virtuales, sujeto a lo dispuesto en la LRITF.
12. Comprar, vender o, en general, transmitir activos virtuales por cuenta propia o de sus Clientes.
13. Realizar los actos necesarios para la consecución de su objeto social.

Es importante señalar que para los efectos de LRITF[82], se considera fondos de pago electrónico a aquellos fondos que estén contabilizados en un registro electrónico de cuentas transaccionales que, al efecto lleve una IFPE y que:

1. Queden referidos a:
    a. Un valor monetario equivalente a una cantidad determinada de dinero, en moneda nacional o, previa autorización de BANXICO, moneda extranjera, o
    b. Un número determinado de unidades de un activo virtual determinado por BANXICO.
2. Correspondan a una obligación de pago a cargo de su emisor, por la misma cantidad de dinero o de unidades de activos virtuales.
3. Sean emitidos contra la recepción de la cantidad de dinero o de activos virtuales, con el propósito de abonar, transferir o retirar dichos fondos, total o parcialmente mediante la instrucción que dé el tenedor de los FPE, y
4. Sean aceptados por un tercero como recepción de la cantidad de dinero o de activos virtuales respectiva.

Cabe señalar, que derivado de la emisión de FPE, el registro electrónico en las cuentas respectivas, la administración de la cuenta que permite el abono, retiro, y transferencias de FPE existe un tratamiento de datos personales que la IFPE necesita realizar para poder brindar los servicios que ofrece y que están permitidos en función de la LRITF.

Para la realización de las operaciones por parte de los clientes; en particular las órdenes de transferencia de fondos u órdenes de transferencias de fondos de pago electrónicos[83] se establece que las IFPE podrán establecer un esquema de autenticación reforzada con al menos, dos elementos independientes cuyas características se determinan en las disposiciones conjuntas (BANXICO y CNBV) del artículo 56 de la LRITF, que aún no han sido emitidas. Cabe señalar que esta autenticación la deja facultativa para las IFPE, ya que en caso de que existan reclamos por robo o extravío y la IFPE no pruebe que realizó la autenticación con dos elementos independientes, esta deberá abonar, a más tardar el segundo Día Hábil Bancario, los recursos objeto del reclamo.[84] Asimismo, las disposiciones conjuntas de BANXICO y la CNBV del artículo 56 de la LRITF deberán establecer los requisitos de autenticación para la contratación que se realice vía remota para los contratos u operaciones.

Respecto a los activos virtuales, las IFPE solo podrán emitir FPE referidos a aquellos activos virtuales que BANXICO determine cuando lo estime procedente. Las IFPE deberán solicitar a BANXICO su autorización para que puedan utilizar aquellas tecnologías asociadas a alguno de los activos virtuales. Respecto a la operación con los Activos Virtuales es necesario establecer que de conformidad con la disposición 3ª de la circular 4/2019 emitida por BANXICO las instituciones de crédito y las ITF solo podrán celebrar operaciones con activos virtuales que corresponden a Operaciones Internas[85], sujeto a la autorización de BANXICO.

El proceso para la apertura de una cuenta de fondos de pago electrónico es el siguiente: el potencial cliente[86] celebra con la IFPE un contrato de emisión y depósito mercantil de fondos de pago electrónico por cada cuenta de FPE. Antes de la celebración del contrato la IFPE deberá recabar toda la información necesaria que se estableció en el aparatado de alta de cliente para guardar el expediente del cliente.

---

[82] Art. 23 de la LRITF

[83] Disposición 17ª y 19ª de la circular 12/2018 del Banco de México.

[84] Disposición 35ª de la circular 12/2018 de Banco de México

[85] De conformidad con la disposición 2ª de la circular 4/2019 las Operaciones Internas se refieren "a las actividades que las Instituciones realicen internamente para llevar a cabo las operaciones pasivas, activas y de servicios que estas celebran con sus Clientes o que estas realicen por cuenta propia, incluyendo las actividades que realicen las Instituciones para soportar las transferencias internacionales de fondos que lleven a cabo."

[86] De conformidad a la disposición 5ª de la circular 12/2018 las "IFPE podrán abrir Cuentas de Fondos de Pago Electrónico referidos a moneda nacional, a nombre de personas físicas y morales, nacionales o extranjeras. Asimismo, sujeto a la previa autorización del Banco de México, las mencionadas instituciones podrán abrir Cuentas de Fondos de Pago Electrónico referidos a Moneda Extranjera, únicamente a nombre de personas físicas y personas morales nacionales o personas físicas extranjeras residentes en México y que acrediten su calidad migratoria mediante el documento correspondiente.

Tratándose de las Cuentas de Fondos de Pago Electrónico referidos a Moneda Extranjera, las instituciones de fondos de pago electrónico solamente podrán abrirlas a nombre de personas morales nacionales, cuando estas ultimas mantengan una cuenta de depósito en alguna Entidad Financiera, institución de Fondos de Pago Electrónico del Exterior, o entidad financiera del exterior."

2.5.1. Operaciones con moneda nacional

Respecto a las operaciones en moneda nacional que realizan las IFPE se identificaron distintos subprocesos:

1. Niveles de cuentas.

Una vez que las personas físicas o morales se convierten en Clientes de las IFPE, estas deberán clasificar a cada una de las cuentas de FPE en tres niveles en función de los criterios y requisitos para la apertura de cuenta de conformidad con lo previsto en las DCGA58.
Las cuentas se sujetan a lo siguiente:

I. Cuentas de FPE nivel 1 que una IFPE lleve a un mismo cliente, la suma de los abonos en la totalidad de las cuentas, durante el mes calendario, no podrán exceder el equivalente a 750 UDIS. En ningún momento la suma de los saldos podrá exceder 1000 UDIS.
II. Cuentas de FPE nivel 2 que una IFPE lleve a un mismo cliente, la suma de los abonos en la totalidad de dichas cuentas, durante el trascurso de mes calendario, no podrá exceder a 3,000 UDIS.
III. Cuentas de FPE nivel 3 que una IFPE lleve a un ismo cliente, la suma de los abonos no tendrá límite.

Se identificó que de forma directa se obtienen datos personales de identificación y autenticación, patrimoniales y/o financieros, crediticios y laborales para establecer los niveles de cuenta; en particular para cumplir con las políticas de identificación y conocimiento de los clientes que utilicen los servicios por parte de las IFPE como parte de las obligaciones previstas en el artículo 58 de la LTRIF y DCG, verificar y confirmar la identidad, dar cumplimiento a obligaciones previstas en las leyes, reglamento y disposiciones legales aplicables y celebrar operaciones y contratos con el Titular y realizar los actos que estime necesarios o convenientes para lograr el cumplimiento de las obligaciones derivadas de dichas operaciones y contratos para beneficio del titular o de algún tercero beneficiario.

2. Emisión de fondos de pago electrónico y abonos de recursos.

Los clientes de las IFPE podrán entregar recursos para la emisión de FPE mediante transferencias de fondos, pagos con tarjetas (débito, crédito o recargables) emitidas por Entidades Financieras o cheques y efectivo. Para el supuesto de la entrega de recursos mediante efectivo solo se en aquellos casos que la IFPE cuente con la autorización de la CNBV.

Se identificó que de forma directa se obtienen datos personales de identificación y autenticación, patrimoniales y/o financieros y transaccionales para verificar y confirmar la identidad para la emisión de FPE, dar cumplimiento a obligaciones previstas en las leyes, reglamento y disposiciones legales aplicables, realizar la emisión de fondos de pago electrónicos y el abono de recursos, realizar las acciones necesarias de administración de cuentas para la emisión y abono de recursos, verificar y confirmar la identidad para estar en posibilidad de realizar los cargos de recursos, dar cumplimiento a obligaciones previstas en las leyes, reglamento y disposiciones legales aplicables y realizar las acciones necesarias de administración de cuentas para el cargo de recursos.

3. *Cargo de recursos.*

Uno de los elementos esenciales de la administración de una cuenta es la posibilidad del cliente de disponer de los recursos de su cuenta y realizar los cargos correspondientes en la cuenta referida. La disposición 11ª de la circular 12/2018 de Banco de México permite el cargo de recursos mediante:

- Cargo de FPE por la cantidad que indique el cliente.
- Transferencias de FPE a otras cuentas de FPE referidos en la misma moneda.
- Pagos de cualquier tipo, mediante el uso de medios de disposición que la IFPE haya permitido al cliente usar.

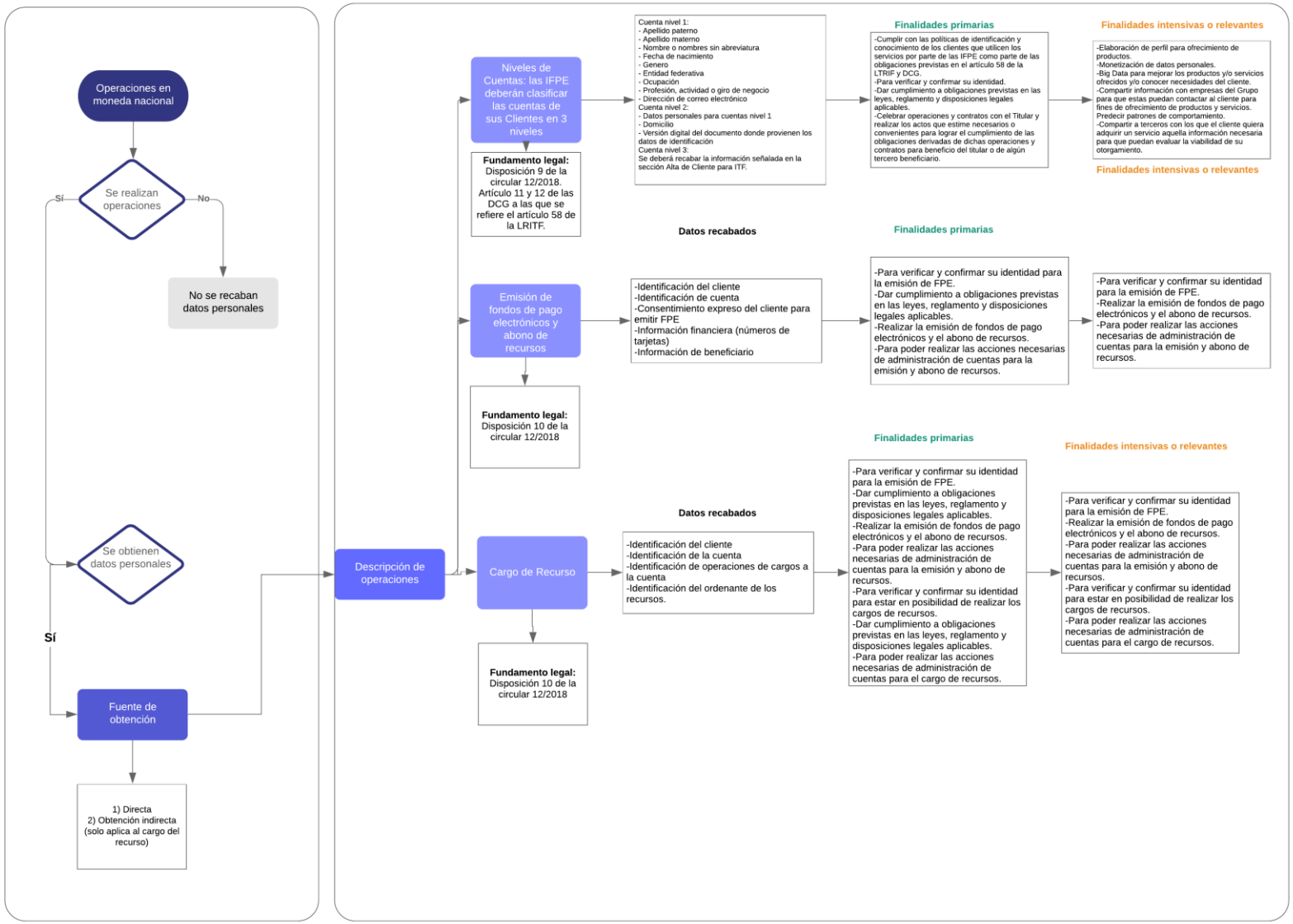
- Domiciliaciones.

El proceso anterior se resume en el siguiente diagrama:

-

Procesos que involucran el tratamiento de datos en las IFPE

Proceso: Operaciones de las IFPE
Subproceso: Operaciones en moneda nacional



2.5.2. Operaciones con moneda extranjera

Respecto de las operaciones de las IFPE con moneda se extranjera se identificó lo siguiente:

1. Emisión de Fondos de Pago Electrónico en Moneda Extranjera.

Para que las IFPE pueda realizar operaciones en moneda extranjera deberán contar con esquemas de separación de FPE que emitan referidos en moneda extranjera de aquellos que emitan referidos en moneda nacional, se identifica el tratamiento de datos personales, ya que la IFPE deberá tener mecanismos para poder identificar a cada cliente con sus respectivos FPE referidos en distinta moneda.

Además, se identificó que de forma directa se obtienen datos personales patrimoniales y/o financieros y transaccionales, verificar y confirmar su identidad para la emisión de FPE, dar cumplimiento a obligaciones previstas en las leyes, reglamento y disposiciones legales aplicables, realizar la emisión de fondos de pago electrónicos y el abono de recursos y realizar las acciones necesarias de administración de cuentas para la emisión y abono de recursos.

2. Límites de cuentas.

Se identifica el tratamiento de datos personales por parte de las IFPE en la apertura y administración de cuentas de FPE referidas en moneda extranjera, estas cuentas deberán observar las siguientes características[87]:

I. Tratándose de cuentas de FPE abiertas a nombre de personas físicas la suma de: i) los abonos en el transcurso de un mes calendario que dicho Cliente o terceros realicen a una o más Cuentas de Fondos de Pago Electrónico que la institución de fondos de pago electrónico le lleve, y ii) los abonos equivalentes a la cantidad de fondos de pago electrónico provenientes de una Institución de Fondos de Pago Electrónico del Exterior con los que la institución de fondos de pago electrónico comercialice, no podrá exceder de los diez mil Dólares o su equivalente tratándose de otra Moneda Extranjera.

II. Tratándose de Cuentas de Fondos de Pago Electrónico abiertas a nombre de personas físicas, la suma de: i) los saldos que dicho Cliente mantenga en una o más Cuentas de Fondos de Pago Electrónico que la institución de fondos de pago electrónico le lleve, y ii) los saldos equivalentes a la cantidad de fondos de pago electrónico provenientes de una Institución de Fondos de Pago Electrónico del Exterior con los que la institución de fondos de pago electrónico comercialice, no podrá exceder de los diez mil Dólares o su equivalente tratándose de otra Moneda Extranjera.

III. Tratándose de Cuentas de FPE abiertas a nombre de personas morales nacionales, la suma de los abonos no tendrá límite, a menos que pacte con el cliente.

Es necesario identificar que existe un tratamiento de datos personales por parte de las IFPE, ya que es necesarios que estas identifiquen al tipo de cliente para poder determinar si la persona física en cuestión puede abrir una cuenta de FPE referido en moneda extranjera; asimismo, es necesario tratamiento de datos personales en la apertura y administración de este tipo de cuentas.

Se identificó que de forma directa se obtienen datos personales patrimoniales y/o financieros y transaccionales para dar cumplimiento a obligaciones previstas en las leyes, reglamento y disposiciones legales aplicables para la apertura y administración de cuentas y realizar el análisis del cliente que permita a la IFPE limitar el nivel de operación de conformidad con la normatividad aplicable.

3. Abono de recursos en moneda extranjera

[87] Disposición 13ª de la circular 12/2018 de Banxico

Las IFPE que administren cuentas de FPE en moneda extrajera deberán permitir a los clientes los abonos respectivos, sujeto a la autorización de BANXICO. Se identificó que de forma directa se obtienen datos personales de identificación y autenticación, patrimoniales y/o financieros y transaccionales para verificar y confirmar la identidad para el abono de recursos en moneda extranjera en las cuentas, dar cumplimiento a obligaciones previstas en las leyes, reglamento y disposiciones legales aplicables y realizar las acciones necesarias de administración de cuentas para el abono de recursos.

4. Cargo de recursos

Las IFPE que administren cuentas de FPE referidos en moneda extranjera deberán permitir a los clientes los cargos respectivos mediante:

I. Redención de los FPE por la cantidad que indique el cliente.
II. Transferencias de FPE, y
III. Pagos de cualquier tipo, mediante el uso de una Tarjeta. En el supuesto que el Cliente sea persona física, únicamente se podrá realizar este tipo de pago a beneficiarios localizados fuera del territorio nacional.

Se identificó que de forma indirecta se obtienen datos personales de identificación y autenticación, patrimoniales y/o financieros y transaccionales para verificar y confirmar su identidad para el cargo de recursos en moneda extranjera en las cuentas, dar cumplimiento a obligaciones previstas en las leyes, reglamento y disposiciones legales aplicables, realizar las acciones necesarias de administración de cuentas para el cargo de recursos y realizar el análisis del cliente que permita a la IFPE limitar el nivel de operación de conformidad con la normatividad aplicable.

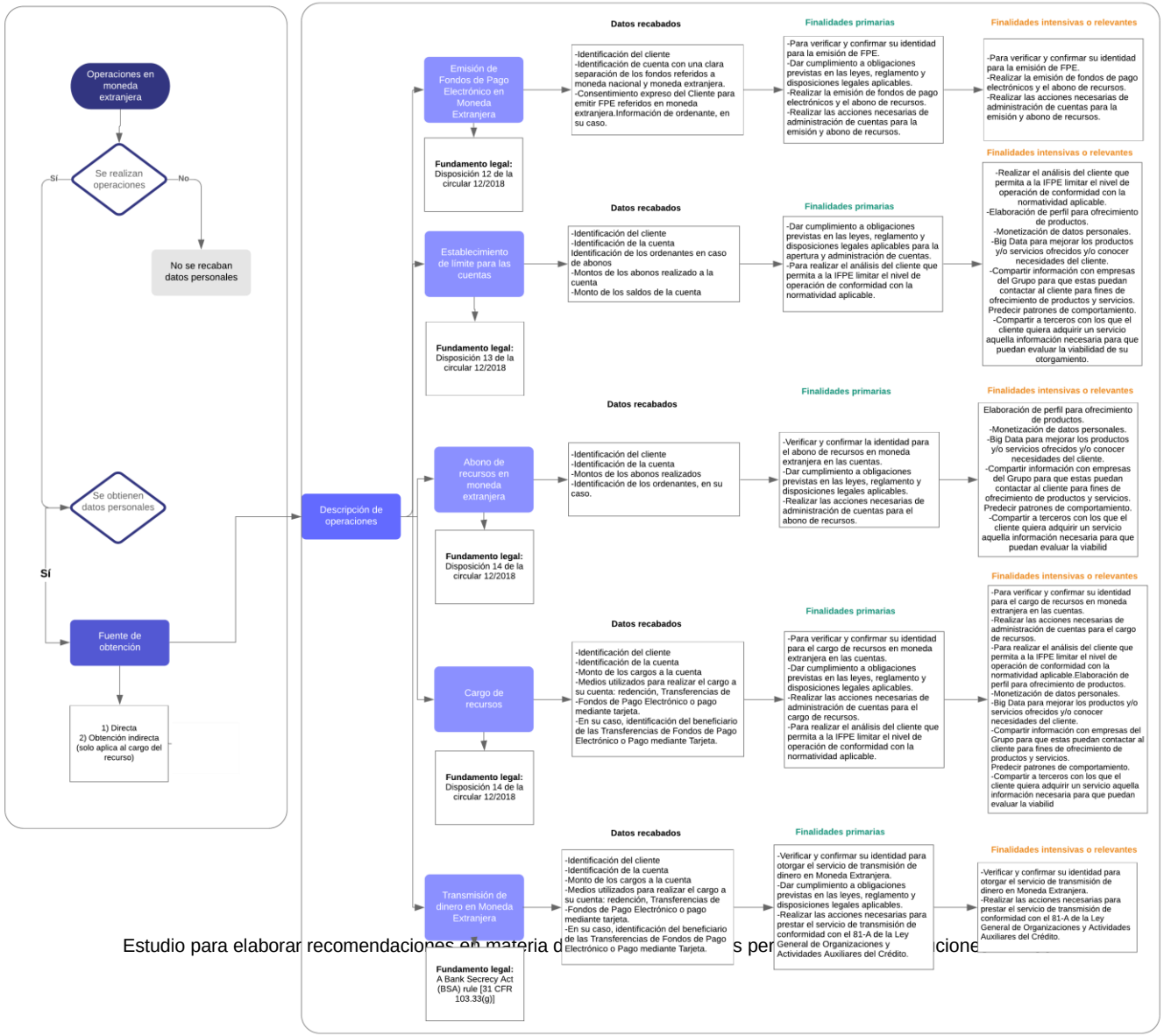
5. Transmisión de dinero en moneda extranjera

Se identificó que de forma directa se obtienen datos personales patrimoniales y/o financieros y transaccionales para verificar y confirmar su identidad para otorgar el servicio de transmisión de dinero en Moneda Extranjera, dar cumplimiento a obligaciones previstas en las leyes, reglamento y disposiciones legales aplicables y realizar las acciones necesarias para prestar el servicio de transmisión de conformidad con el 81-A de la Ley General de Organizaciones y Actividades Auxiliares del Crédito.

El proceso anterior se resume en el siguiente diagrama:

Procesos que involucran el tratamiento de datos en las IFPE

Proceso: Operaciones de las IFPE
Subproceso: Operaciones en moneda extrajera



2.6. Características de las Operaciones

Respecto a las características de las operaciones se identificó lo siguiente:

1. Sobregiros

Existen situaciones en las que el cliente al realizar una operación no complete con los FPE que se registran en su cuenta; permitiendo la normatividad poder realizar sobregiros. Estos sobregiros no podrán superar a los 15 UDIS.

Derivado del presente proceso, se identificó que de forma indirecta se obtienen datos personales de identificación y autenticación y transaccionales para verificar y confirmar su identidad para permitir sobregiros en caso de ser necesario, dar cumplimiento a obligaciones previstas en las leyes, reglamento y disposiciones legales aplicables y otorgar el permiso del sobregiro y el monto necesario.

2. Órdenes de Transferencias de Fondos de Pago Electrónicos[88]

Una de las operaciones que pueden realizar los Clientes de las IFPE son las órdenes de transferencia de FPE, estas podrán ser realizadas por los clientes a través de medios electrónicos, que ambas partes acuerden, indicando la información del Cliente emisor y la del Cliente beneficiario para realizar la transferencia. Derivado de este proceso, se identifica el tratamiento de datos para la administración de las cuentas de FPE para estar en posibilidad de abonar y cargar los respectivos FPE. Asimismo, la IFPE puede establecer un esquema de autenticación reforzada con al menos dos elementos independientes. En este sentido, la IFPE recaba datos personales cada vez que se realiza una operación, ya que es necesaria la autenticación de los clientes para poder llevar a cabo las órdenes de transferencia de FPE.

Derivado de este proceso, se identificó que de forma directa e indirecta se obtienen datos personales de identificación y autenticación, patrimoniales y/o financieros y transaccionales para verificar y confirmar su identidad para la realización de órdenes de transferencias de FPE (2FA), dar cumplimiento a obligaciones previstas en las leyes, reglamento y disposiciones legales aplicables, realizar las acciones necesarias para brindar el servicio de órdenes de transferencias de FPE, realizar las acciones necesarias de administración de cuentas para realizar los abonos y cargos correspondientes de recurso, determinar lo límites establecidos por la normatividad aplicable respecto a las transferencias realizadas y aclaraciones y seguimiento a investigaciones.

3. Cargos no reconocidos[89]

Para realizar los cargos no reconocidos la IFPE realiza tratamiento de datos personales, ya que debe establecer un proceso de reclamo de frente al cliente que permita identificarlo; asimismo, es necesario que la IFPE administre la cuenta para poder llevar a cabo los abonos derivados de dichas reclamaciones.

Cuando la IFPE reciba un aviso de reclamación por cargos no reconocidos, la IFPE deberá abonar, a mas tardar el segundo día hábil bancario posterior a aquel en que haya recibido el aviso respectivo, el monto del cargo no reconocido. La IFPE no estará obligada a realizar el abono cuando haya probado que para la operación que realizó el cliente utilizó doble factor de autenticidad.

Derivado del presente proceso, se identificó que de forma directa se obtienen datos personales de identificación y autenticación, patrimoniales y/o financieros y transaccionales para verificar y confirmar

[88] La disposición segunda de la circular 12/2018 define a las Transferencias de Fondos de Pago Electrónico como a aquella operación realizada por una misma institución de fondos de pago electrónico de conformidad con los contratos celebrados con sus Clientes para la apertura de Cuentas de Fondos de Pago Electrónico, de acuerdo con la cual dicha institución abona una cantidad determinada de fondos de pago electrónico en una de dichas Cuentas, derivado del cargo por la referida cantidad en alguna otra de esas cuentas.

[89] Disposición 18ª de la circular 12/2018 de Banxico

su identidad para hacer la revisión de la queja por cargo no reconocido, realizar el tramite correspondiente de cargos no reconocidos de conformidad con la normatividad aplicable y realizar los abonos necesarios, en su caso, de los cargos no reconocidos.

4. Órdenes de Transferencias de Fondos[90]

Respecto a las órdenes de transferencias de fondos para identificar el tratamiento de datos personales tomaremos como punto de partida la disposición 16 de las DCG115 de la LIC, existen otro tipo de datos personales que las IFPE deberán incluir en las Órdenes de Transferencias de conformidad con la circular 13/2017 (Sistemas de pagos administrados por el BANXICO y servicio de transferencias de fondos); sin embargo, el detalle se encuentra en los Manuales de Operación que se entregan a los Participantes del sistema de pagos. De conformidad con la disposición 16 las transferencias de fondos deberán incluir:

- motivo de pago
- nombre completo del Cliente
- Domicilio
- Número de referencia que la IFPE ordenante asigne.
- Identificación de cuenta: CLABE o número telefónico asociado a la cuenta.
- nombre completo del beneficiario
- Entidad Receptora
- identificador de la cuenta.

Asimismo, para las Transferencias de Fondos la IFPE deberá identificar las cuentas de FPE con:

- CLABE asignada a la cuenta de FPE, o
- 10 dígitos del número de línea telefónica móvil que indique el Cliente.

5. Emisión de tarjetas

Las IFPE podrán dar al cliente Tarjetas como medio de disposición de los recursos las cuales deberán entregarse desactivadas. Se identifica un tratamiento de datos personales para la emisión de una tarjeta, ya que la disposición por parte del cliente se traduce en una administración que deberá llevar a acabo la IFPE, donde identifique:

- Dígitos de identificación única.
- Fecha de vencimiento.
- Titular de la marca.
- Código de seguridad.
- Información que asocia una tarjeta con una cuenta de su cliente.
- Operaciones que se han realizado con la tarjeta.

Por último, también se identifica tratamiento de datos personales que se obtienen de forma directa cuando el cliente solicita a la IFPE la activación de su tarjeta. Este tratamiento se hace para la autenticación del Cliente. Cabe señalar, que en las disposiciones no se establece el proceso mediante el cual se la IFPE podrá realizar la autenticación del cliente para la activación de la tarjeta, solo menciona que será a través de los mecanismos que la IFPE disponga.

En este sentido, se identificó que de forma indirecta se obtienen datos personales de identificación y autenticación, patrimoniales y/o financieros y transaccionales para emitir un medio de disposición que el cliente podrá utilizar para poner disponer de sus recursos y administrar la cuenta del Cliente y realizar los cargos y abonos respectivos.

[90] La disposición segunda de la circular 12/2018 define a las Transferencias de Fondos a aquella operación realizada entre la institución de fondos de pago electrónico de que se trate y otra institución de fondos de pago electrónico, Entidad Financiera, entidad financiera del exterior o Institución de Fondos de Pago Electrónico del Exterior, conforme al cual la primera realiza (i) el abono en una Cuenta de Fondos de Pago Electrónico por la cantidad equivalente de dinero a la indicada en la orden respectiva que reciba, derivada del cargo que esa otra institución de fondos de pago electrónico o entidad haga en la cuenta correspondiente, o bien (ii) el cargo en una Cuenta de Fondos de Pago Electrónico equivalente a aquella cantidad de dinero que el Cliente haya indicado en la orden que emita para que, una vez realizada la redención de los referidos fondos, dicha cantidad se acredite a favor de la otra institución de fondos de pago electrónico o entidad referida a quien se envíe dicha orden para su abono en la cuenta de depósito indicada en dicha orden.

6. Transmisión de mensajes con pago con tarjetas

Para la correcta operación de las operaciones con tarjeta se identifica el tratamiento de datos personales en el cual se hace una transmisión de mensajes entre entidades financieras para estar en posibilidad de realizar el cargo y abono respectivo del pago con tarjetas. En este tratamiento se identifican los siguientes datos personales[91]:

- Nombre completo.
- Número de tarjeta.
- Número de cuenta.
- Límite de crédito.
- Saldos.
- Información de autenticación

En este sentido, se identificó que de forma indirecta se obtienen datos personales de identificación y autenticación, patrimoniales y/o financieros y transaccionales para cumplir con las medidas de seguridad de la transmisión, almacenamiento y procesamiento de la información.

7. Reclamo por robo o extravío de tarjetas/Reclamaciones por cargos no reconocidos

Como se mencionó anteriormente, es importante señalar que las IFPE podrán establecer un esquema de autenticación reforzada con al menos, dos elementos independientes para la realización de operaciones. Esta autenticación es opcional; sin embargo, si la IFPE no prueba que la operación se realizó con al menos dos elementos independientes deberá realizar el abono objeto del reclamo.

Los elementos de autenticación son los siguientes[92]:

1. Información que la institución de fondos de pago electrónico proporciona al Cliente o permite a este generar, a efecto de que solamente él la conozca, para que la pueda ingresar al sistema autorizado por dicha institución para iniciar la Operación de que se trate, tales como contraseña o número de identificación personal.
2. Información contenida, recibida o generada por medios o dispositivos electrónicos que solo posee el Cliente, incluyendo la almacenada en un circuito integrado o chip que sea procesada conforme a los estándares que el BANXICO determine en la regulación correspondiente, así como la obtenida por dispositivos generadores de contraseñas dinámicas que la institución de fondos de pago electrónico proporcione a su Cliente. Lo anterior, siempre y cuando dicha información sea generada con propiedades que impidan su duplicación o alteración y que sea información dinámica que no pueda ser utilizada en más de una ocasión.
3. Información derivada de características propias del Cliente, como aquellas de carácter biométrico, incluyendo huellas dactilares, geometría de la mano o de la cara, patrones en iris o retina, entre otros.
4. Cualquier otro elemento distinto a los previstos en los incisos anteriores que quede determinado en las disposiciones de carácter general que emitan conjuntamente BANXICO y la CNBV de conformidad con el artículo 56, segundo párrafo, de la Ley.

En este tratamiento de datos personales se identifican los siguientes datos personales:

- Número de referencia del reclamo.
- Fecha y hora del reclamo.
- Conservación de evidencia de la información proporcionada al cliente.
- Identificación de la cuenta
- Identificación del cliente o representante legal.

[91] Anexo 5, inciso A numeral 2, de las Disposiciones de Carácter General Aplicables a Redes de Medios de Disposición
[92] Disposición 35ª de la circular 12/2018 de Banxico

- Prueba de la autenticación con doble factor independiente.
- Dictamen de reversión de los abonos, en su caso:
    - Evidencia de los elementos de autenticación.
    - Hora en que realizó la operación.
    - Nombre del receptor de los pagos donde se originó la operación.

8. Contratación de Domiciliaciones

Una de las operaciones que la IFPE puede ofrecer a sus Clientes es el servicio de Domiciliación con cargo a las cuentas de FPE. De conformidad con la disposición 2ª de la circular 12/208 una domiciliación es "la ejecución de transferencias de fondos o transferencias de fondos de pago electrónico, sean individuales o recurrentes, con cargo a una cuenta de FPE, que realice la IFPE que la administre, de acuerdo con la aceptación expresa que el titular de dicha cuenta presente directamente o por medio de tercero autorizado[93].

Este proceso inicia cuando los clientes solicitan la contratación de domiciliaciones a la IFPE, se deberá obligar al tercero autorizado que cuando reciban las solicitudes respectivas recabe al menos la información la siguiente información personal:

- Motivo de la transferencia de fondos o transferencia de FPE.
- Número de identificación generado por el tercero autorizado.
- Periodicidad del cargo, incluyendo el día específico del cargo.
- Nombre de la IFPE del cliente domiciliado.
- Cualquiera de los datos de la identificación de la cuenta: CLABE o número de tarjeta.
- Monto máximo fijo del cargo autorizado por periodo de facturación.
- Temporalidad del contrato de domiciliación.
- Nombre completo del titular de la cuenta.
- Constancia del contrato.

9. Cancelación del servicio de Domiciliación

Para la cancelación del servicio la IFPE deberá atender las solicitudes de sus clientes. Estas solicitudes deberán presentarse mediante formato, el cual se incorpora a la circular 12/2018 de Banxico como Anexo 2. Derivado de los anterior, se puede identificar el tratamiento de los siguientes datos personales:

- Nombre del tercero autorizado para instruir cargos a la cuenta de FPE.
- Motivo de la Transferencia de Fondos o Transferencia de Fondos de Pago Electrónico cuya domiciliación se solicita cancelar.
- Cualquiera de los datos de identificación de la cuenta: 1) número de la tarjeta o 2) CLABE.
- Nombre completo del titular de la cuenta.
- Constancia de la cancelación.

Derivado de lo anterior, se identificó que de forma directa se obtienen datos personales de identificación y autenticación, patrimoniales y/o financieros y transaccionales para verificar y confirmar su identidad para la cancelación del servicio y realizar las acciones necesarias de administración de cuentas para la cancelación del servicio de domiciliación.

10. Objetar cargos por Domiciliación

Para la objeción de cargos por domiciliación la IFPE deberá atender dichas notificaciones realizadas por parte de los clientes, los cuales deberán presentar un formato, el cual se incorpora a la circular 12/2018 de Banxico como Anexo 3. Derivado de lo anterior, se pueden identificar el tratamiento de los siguientes datos personales:

- Monto de la devolución solicitada.

[93] La persona a la que el titular de la cuenta de FPE haya otorgado autorización para instruir cargos en dicha cuenta, para efectos de la domiciliación (disposición 2ª de la circular 12/2018 de Banxico)

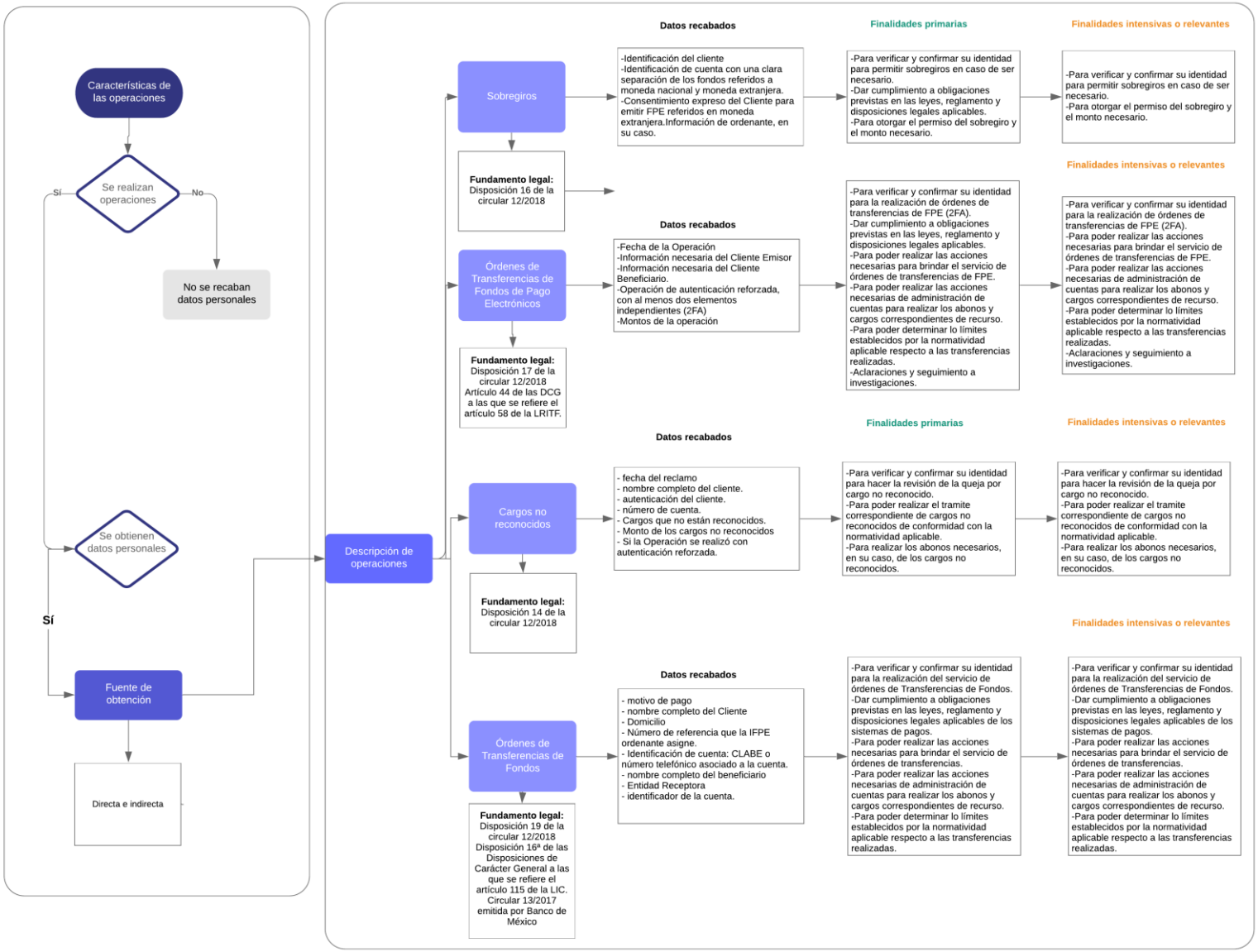
- Fecha del cargo objetado
- Cualquiera de los datos de identificación de la cuenta: 1) número de la tarjeta o 2) CLABE.
- Número de identificación del cargo generado por el Tercero Autorizado.
- Motivo de la objeción.
- Correo electrónico.
- Número telefónico.
- Nombre completo del titular de la cuenta.

Derivado de lo anterior, se identificó que de forma directa se obtienen datos personales de identificación y autenticación, patrimoniales y/o financieros y transaccionales para verificar y confirmar su identidad para hacer la revisión de la queja, realizar el tramite correspondiente de objeción de cargos no reconocidos de conformidad con la normatividad aplicable y realizar los abonos necesarios, en su caso.

El proceso anterior se resume en el siguiente diagrama:

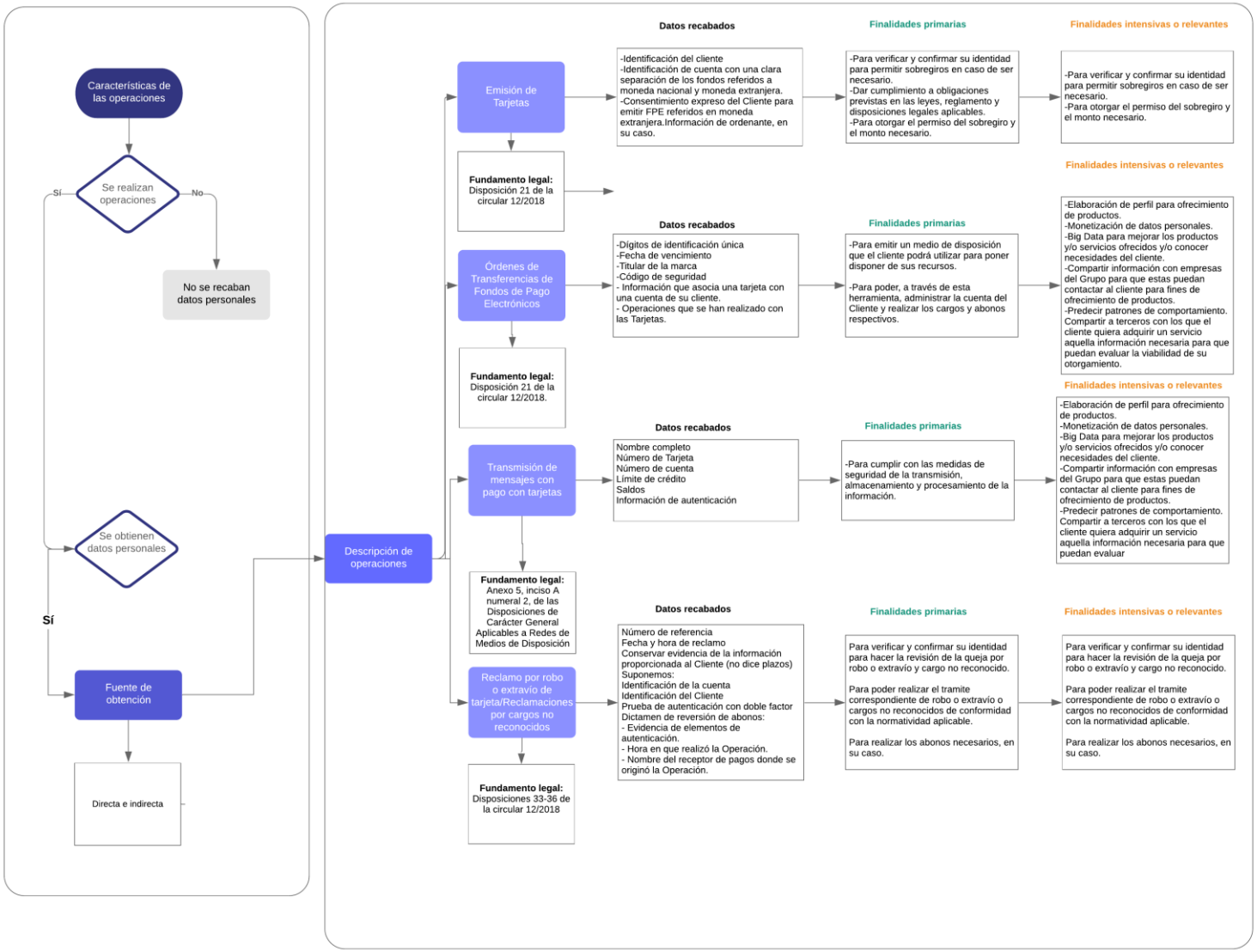
Procesos que involucran el tratamiento de datos en las IFPE

Proceso: Operaciones de las IFPE (Primera parte)
Subproceso: Características de las operaciones



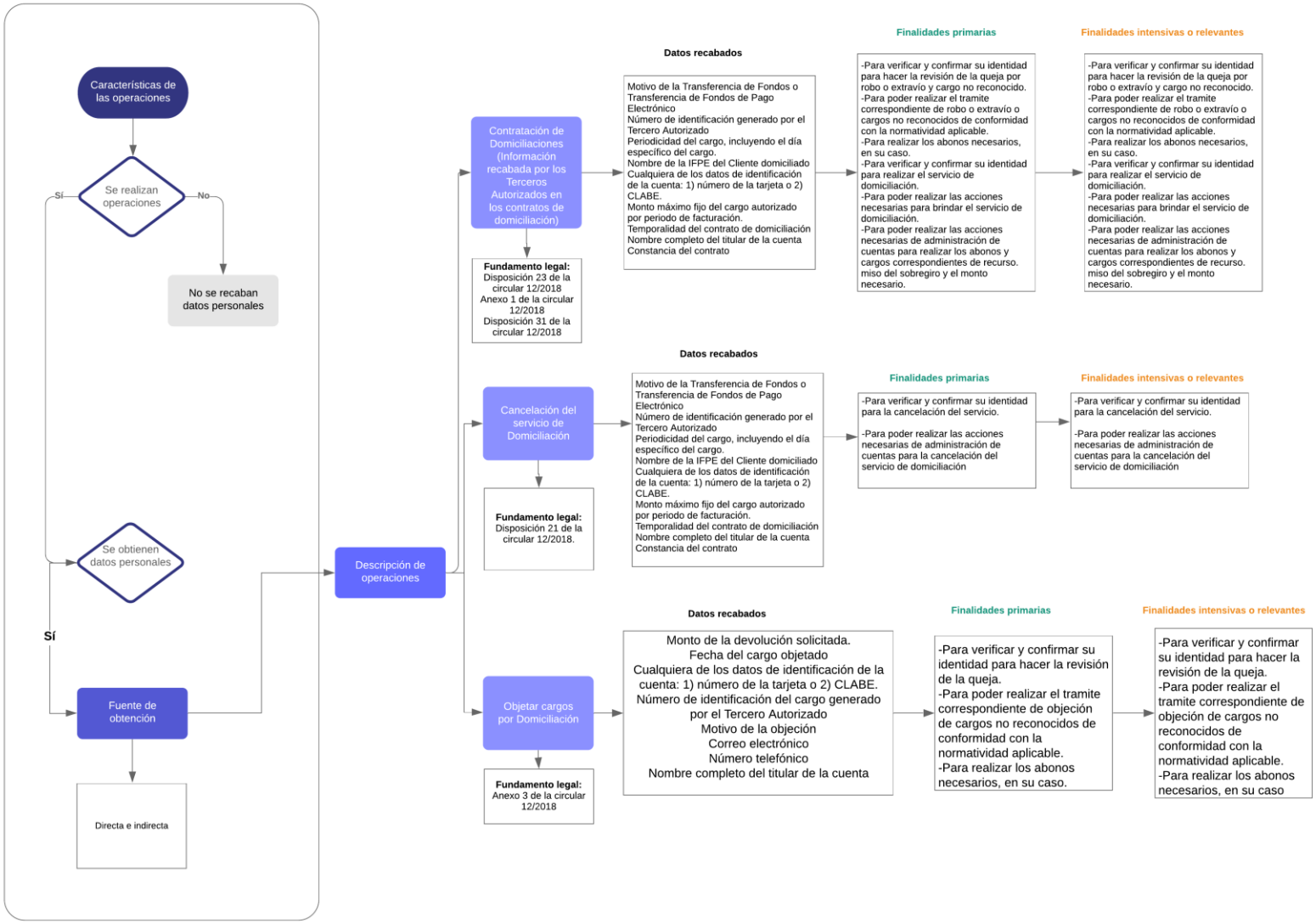
Procesos que involucran el tratamiento de datos en las IFPE

Proceso: Operaciones de las IFPE (Segunda parte)
Subproceso: Características de las operaciones



Procesos que involucran el tratamiento de datos en las IFPE

Proceso: Operaciones de las IFPE (Tercera parte)
Subproceso: Características de las operaciones



2.7. Cierre de cuentas

En este proceso se identificó la obligación de las IFPE de estipular en el contrato que celebren con sus clientes la posibilidad de que el cliente en cualquier momento pueda cerrar su cuenta de fondos de pagos electrónicos, así como redimir el saldo de los respectivos fondos a la cantidad equivalente que corresponda, la IFPE no podrá condicionar el cierre de la cuenta.

Derivado de este proceso se identifica el tratamiento de los siguientes datos personales:

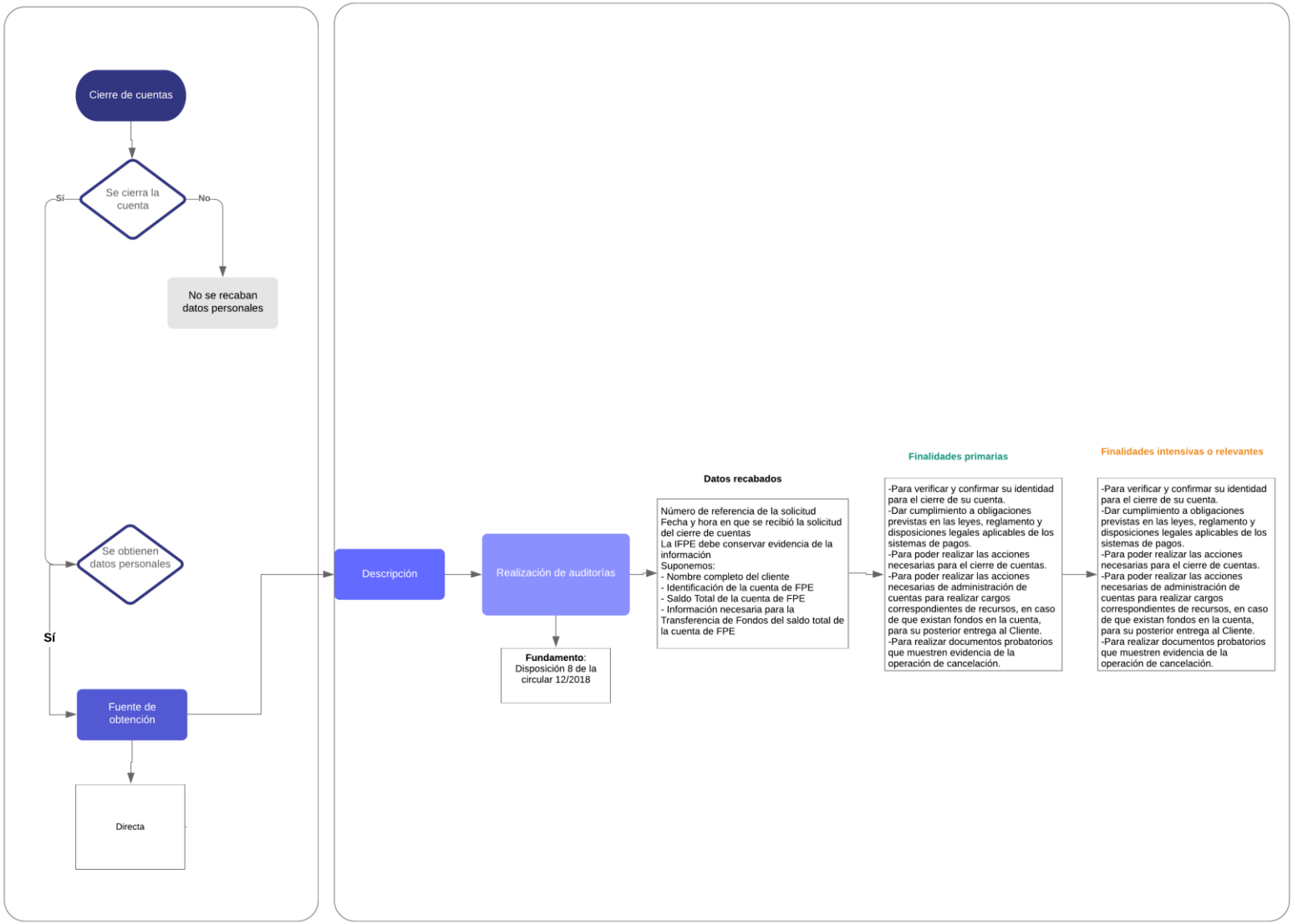
- Número de referencia de la solicitud.
- Fecha y hora en que se recibió la solicitud del cierre de cuentas.
- Evidencia de la información .
- Nombre completo del cliente
- Identificación de la cuenta de FPE
- Saldo Total de la cuenta de FPE
- Información necesaria para la Transferencia de Fondos del saldo total de la cuenta de FPE

Derivado de lo anterior se ha identificado el tratamiento de datos personales de identificación y autenticación, contacto, demográficos, ubicación geográfica, características de dispositivo electrónico, patrimoniales y/o financieros, crediticios, laborales y biométricos, obtenidos de forma directa, para verificar y confirmar su identidad para el cierre de su cuenta, dar cumplimiento a obligaciones previstas en las leyes, reglamento y disposiciones legales aplicables de los sistemas de pagos, realizar las acciones necesarias para el cierre de cuentas, realizar las acciones necesarias de administración de cuentas para realizar cargos correspondientes de recursos, en caso de que existan fondos en la cuenta, para su posterior entrega al Cliente y realizar documentos probatorios que muestren evidencia de la operación de cancelación.

El proceso anterior se resume en el siguiente diagrama:

Procesos que involucran el tratamiento de datos en las IFPE

Proceso: Cierre de cuentas



2.8. Requerimientos de información Banxico

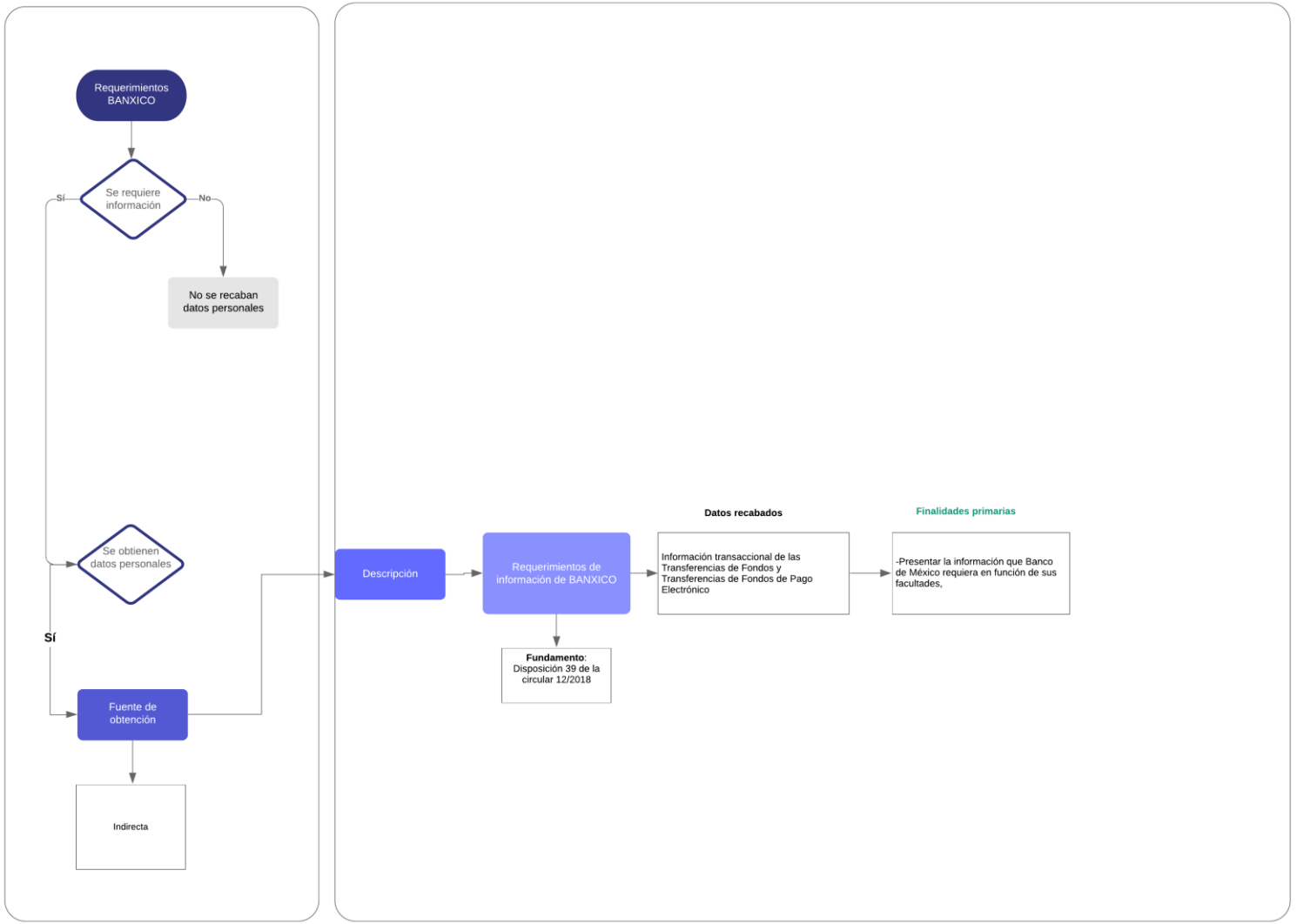
Las IFPE tienen la obligación de suministrar a BANXICO la información transaccional de las Transferencias de Fondos y Transferencias de Fondos de Pago Electrónico enviadas y recibidas por sus Clientes, así como toda información que le requiera. Derivado de este proceso se identifica el tratamiento de datos personales mediante el cual la IFPE realiza una transferencia de datos personales a la autoridad competente en función de sus facultades.

En este sentido, se identificó en este proceso un tratamiento de datos personales patrimoniales y/o financieros, obtenidos de forma indirecta, para presentar la información que BANXICO requiera en función de sus facultades.

El proceso anterior se resume en el siguiente diagrama:

Procesos que involucran el tratamiento de datos en las IFPE

Proceso: Requerimientos de información de BANXICO



2.9. Open banking

El reporte ¿Cuál es el potencial para la banca abierta en México? define al Open Banking o banca abierta como: "un sistema que permite a instituciones financieras compartir cierta información a través de APIs abiertas y seguras. Dentro de estos datos se incluye la información de consumidores que puede ser compartida, con el consentimiento de éstos, con tercero autorizados con el objetivo de recibir servicios más efectivos y eficientes".[94] En el ordenamiento jurídico mexicano este movimiento es consagrado en el artículo 76 de la LRITF es cuál establece la obligación a Entidades Financieras, los transmisores de dinero, las sociedades de información crediticia, las cámaras de compensación a que se refiere la Ley para la Transparencia y Ordenamiento de los Servicios Financieros, las ITF y las sociedades autorizadas para operar con Modelos Novedosos a establecer APIs que posibiliten la conectividad y acceso a los mismos sujetos y terceros especializados en tecnologías de la información. La información que podrán compartirse es la siguiente:

I. *Datos financieros abiertos*: son aquellos generados por las entidades mencionadas en el primer párrafo de este artículo que no contienen información confidencial, tales como información de productos y servicios que ofrecen al público general, la ubicación de sus oficinas y sucursales, cajeros automáticos u otros puntos de acceso a sus productos y servicios, entre otros y según sea aplicable;

II. *Datos agregados*: son los relativos a cualquier tipo de información estadística relacionada con operaciones realizadas por o a través de las entidades mencionadas en el primer párrafo de este artículo, sin contener un nivel de desagregación tal que puedan identificarse los datos personales o transacciones de una persona.

III. *Datos transaccionales:* son aquellos relacionados con el uso de un producto o servicio, incluyendo cuentas de depósito, créditos y medios de disposición contratados a nombre de los clientes de las entidades mencionadas en el primer párrafo de este artículo, entre otra información relacionada con las transacciones que los clientes hayan realizado o intentado realizar en su Infraestructura Tecnológica. Estos datos, en su carácter de datos personales de los clientes, solo podrán compartirse con la previa autorización expresa de éstos.

Es importante señalar, que dentro de la categoría de información que las entidades financieras del artículo 76 pueden compartirse, solamente los datos transaccionales son considerados dato personal, ya que es la única información concerniente a una persona física identificada o identificable. Asimismo, el artículo 76 establece que la información de los datos transaccionales solo podrá ser utilizada para los fines estrictamente autorizados por el cliente. Actualmente, las disposiciones de carácter general a las que se refiere el artículo 76 no han sido emitidas. Estas disposiciones deberán incluir:

1. Los estándares necesarios para la interoperabilidad de interfaces de programación de aplicaciones, incluyendo el diseño, desarrollo y mantenimiento.
2. Los mecanismos de seguridad de las interfaces para el acceso, envío u obtención de datos e información.
3. Definir la información crítica para el buen funcionamiento de las aplicaciones que requieran el uso de estas interfaces.
4. Mecanismos por medio de los cuales se obtendrá el consentimiento del cliente.

Derivado de la falta de emisión de las disposiciones no se puede conocer con certeza jurídica el proceso de Open Banking; sin embargo, describiremos aquél del Reino Unido, el cual ha sido el mayor promotor de la banca abierta a nivel mundial. El proceso de Open Banking en el Reino Unido es el siguiente:

[94] David Beardmore, et. Al. "*¿Cuál es el potencial de la banca abierta en México?: Recomendaciones y plan de trabajo para adoptar el estándar de banca abierta*", Louise Bolotin, México, abril, 2018, p.10

El ecosistema inicia cuando un cliente ve la opción de compartir sus datos con un tercero para obtener un servicio financiero personalizado. Si el cliente desea continuar será direccionado a su proveedor de datos (ej. su banco) para iniciar sesión y brindar su consentimiento expreso (sin compartir sus credenciales de log-in con el tercero). Posteriormente, el cliente será direccionado automáticamente con el tercero quien en este punto tendrá acceso, a través de APIs abiertas, a la información determinada del cliente, la cual solo podrá tratar en función de la finalidad del permiso y por el tiempo establecido de dicho cliente.[95]

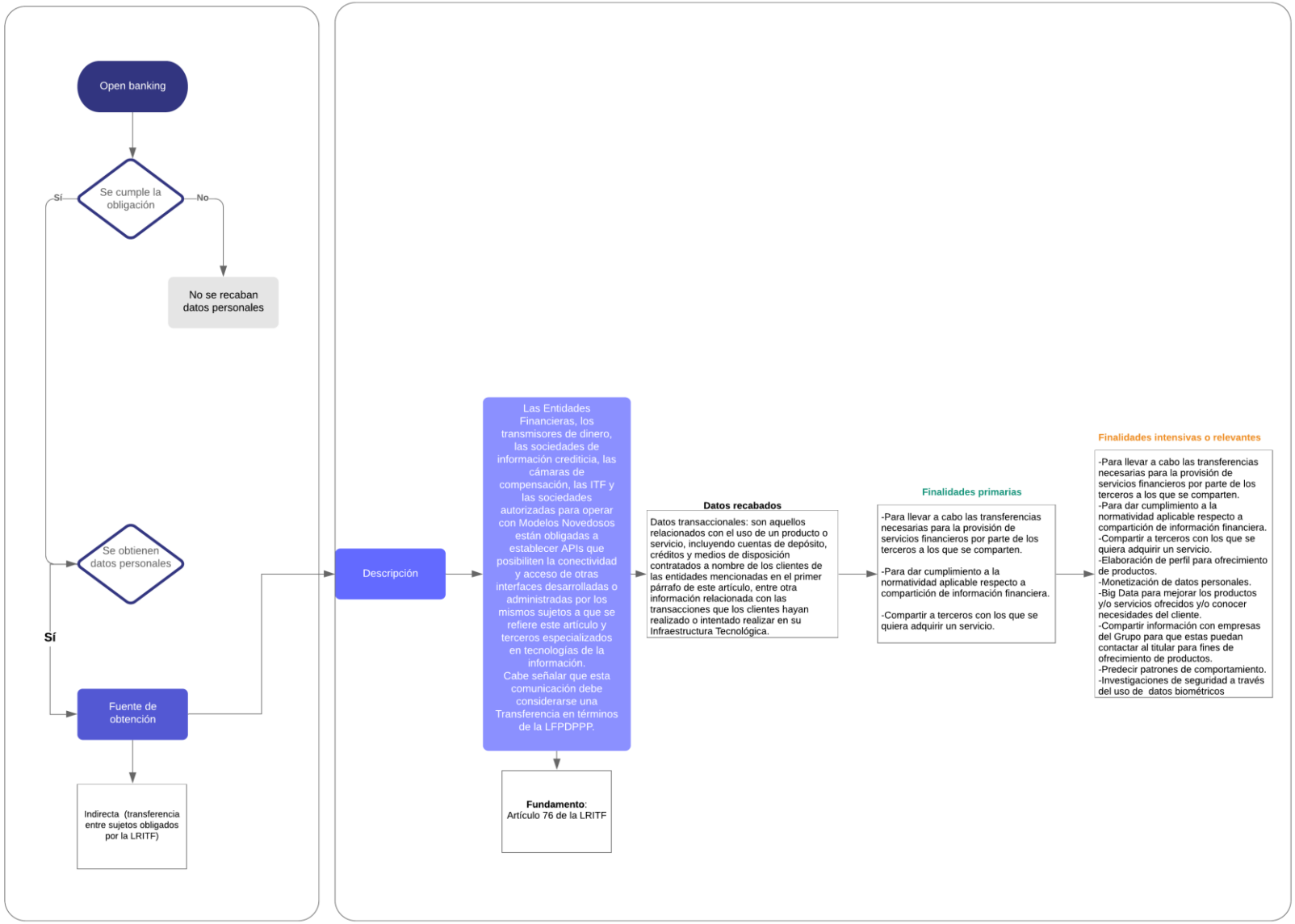
En este proceso se ha identificado que, de forma directa se obtienen datos personales de identificación y autenticación, contacto, demográficos, ubicación geográfica para llevar a cabo las transferencias necesarias para la provisión de servicios financieros por parte de los terceros a los que se comparten, dar cumplimiento a la normatividad aplicable respecto a compartición de información financiera y compartir a terceros con los que se quiera adquirir un servicio.

El proceso anterior se resume en el siguiente diagrama:

[95] Open Banking Working Group, *The Open Banking Standard (OBS): unlocking the potential of open banking to improve competition, efficiency and stimulate innovation,* Louise Bolotin, Reino Unido, Londres, 2016, p. 20
Disponible en:
https://www.paymentsforum.uk/sites/default/files/documents/Background%20Document%20No.%202%20-%20The%20Open%20Banking%20Standard%20-%20Full%20Report.pdf

Procesos que involucran el tratamiento de datos en las IFPE

Proceso: Open banking



Parte 2. “Identificación de tratamientos y riesgos en materia de protección de datos personales en las ITF”

VIII. Identificación de tratamientos y riesgos en materia de protección de datos personales

De acuerdo con lo solicitado por el INAI, en esta segunda parte realiza una descripción de los diferentes tratamientos de datos personales presentes en las ITF considerando el ciclo de vida de los datos personales tratados, en los procesos y operaciones de las ITF.

Para cumplir con lo anterior, se han elaborado una serie de tablas analíticas que contienen los siguientes elementos de análisis y que dan continuidad al Entregable 1 del Estudio:

- Identificación de los procesos y operaciones que involucran el tratamiento de datos personales.
- Identificación de las categorías y datos específicos sujetos a tratamiento en las ITF (IFPE e IFC).
- Identificación del ciclo de vida de los datos personales tratados en las ITF señalando las siguientes fases de la vida del dato: a) obtención; b) almacenamiento; c) usos (incluyendo finalidades primarias y secundarias); d) divulgación especificando los supuestos que constituyen remisiones y transferencias (en caso de transferencias se determina si estas requieren el consentimiento del titular o no); e) bloqueo, y f) supresión.
- Identificación de los tratamientos de datos personales presentes en las ITF distinguiendo en finalidades primarias y secundarias del tratamiento de los datos a partir de los procesos y subprocesos identificados en el Entregable 1 del Estudio.
- Identificación del consentimiento requerido para legitimar el tratamiento de los datos personales tanto en las finalidades primarias como las secundarias del tratamiento que se enuncian respecto de cada tipo de ITF.
- Identificación de los tratamientos de datos personales que realizan las IFPE y las IFC mediante el uso de tecnologías de análisis masivo de datos (*big data*) e inteligencia artificial (*machine learning* y *deep learning*) y los resultantes de la combinación de dichas tecnologías y datos.
- Identificación de los actores que participan en el tratamiento de los datos personales en las ITF (titular, responsables, encargados y terceros).

Es decir, se realizó una descripción de los diferentes tratamientos de datos personales que fueron identificados en los procesos del entregable 1, considerando el ciclo de vida de los datos en los procesos y operaciones propios de las ITF.

En la segunda parte del documento, se presentó una identificación de los riesgos en materia de seguridad de datos personales relacionados con el cumplimiento de la normatividad aplicable a las ITF, según estándares internacionales (norma ISO/IEC 27002:2013), así como aquellos vinculados con las posibles afectaciones que podrían presentarse en los derechos patrimoniales o morales de los titulares de datos personales y el consecuente incumplimiento a la normatividad aplicable a las ITF.

1. Tratamientos de datos personales en las IFC

A continuación, se presenta el tratamiento de datos personales en las IFC respecto a los procesos generales identificados en la sección anterior y que consistieron en alta del cliente, PLD/CFT, obligación de conservar documentos, mecanismos de seguimiento y agrupaciones de operaciones, aspectos generales de las IFC, operaciones de las IFC y *open banking*.

1.1. Alta de cliente

Como se señaló de forma previa, las IFC tienen la obligación de identificar a su cliente al momento de iniciar una relación jurídica a través de un contrato y tener registro de un expediente por cliente, el cual será conformado en función del tipo de persona. Para el alta de cliente se identificó el subproceso de

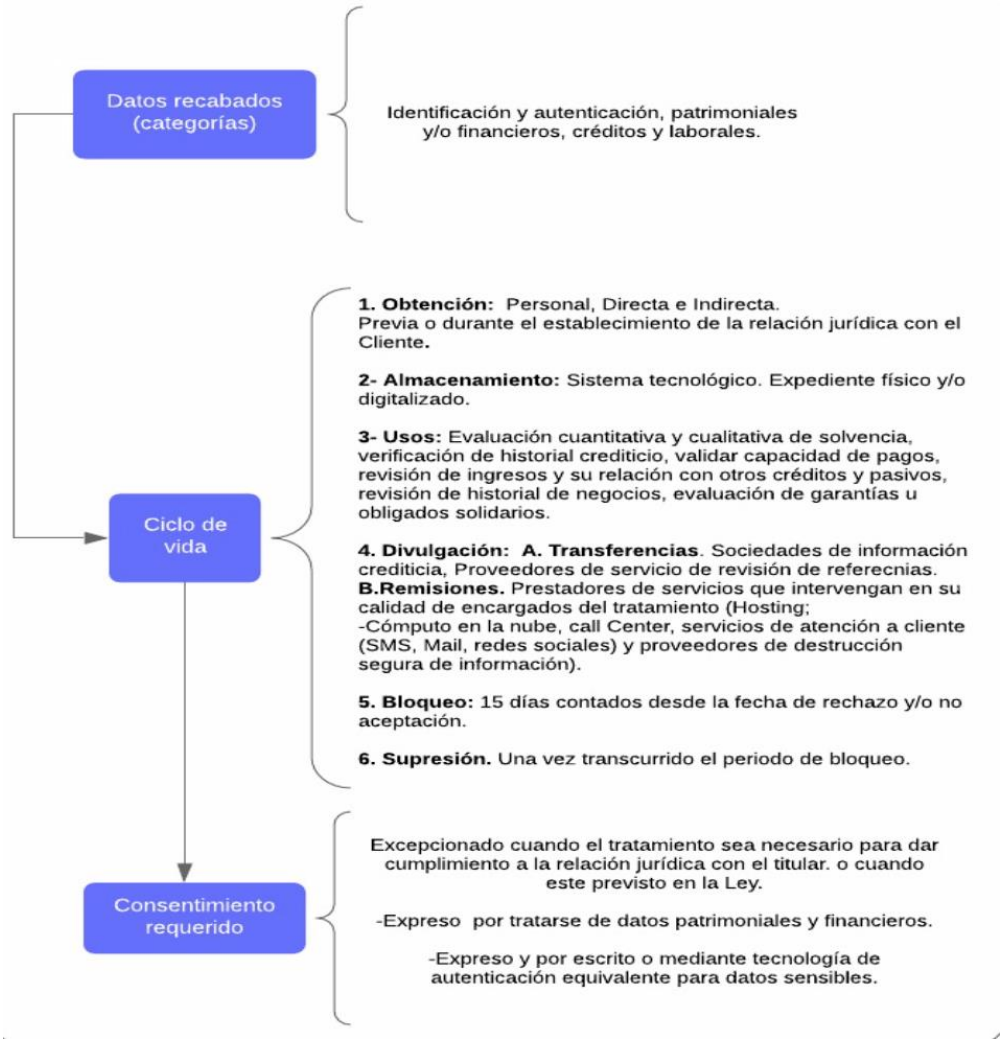
identificación de los datos personales provenientes de documento válido, el cual deberá digitalizarse[96]. El cual obtiene datos personales de identificación y autenticación, patrimoniales y financieros, crediticios y laborales.

Se identificó el siguiente ciclo de vida de los datos personales en el proceso de alta de cliente:

1) **Obtención:**
    - Personal, directa e indirecta.
    - Previa o durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
    - Sistema tecnológico.
    - Expediente físico y/o digitalizado.
3) **Usos:**
    - Evaluación cuantitativa y cualitativa de solvencia.
    - Verificar historial crediticio.
    - Validar capacidad de pagos.
    - Revisión de ingresos y su relación con otros créditos y pasivos
    - Revisión de Historial de negocios
    - Evaluación de garantes u obligados solidarios.
4) **Divulgación/otros sujetos intervinientes:**
    - ***Transferencias:***
        - Sociedades de información crediticia: se exceptúa el consentimiento por estar establecido en una disposición legal.
        - Proveedores de servicio de revisión de referencias.
    - ***Remisiones:***
        - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
        - Hosting.
        - Cómputo en la nube.
        - Call Center.
        - Servicios de atención a cliente.
        - Proveedores de destrucción segura de información.
5) **Bloqueo**: 15 días contados desde la fecha de rechazo y/o no aceptación.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

El ciclo de vida en el proceso de alta de cliente se resume en el siguiente diagrama:

[96] Para Propietarios Reales, Proveedores de Recursos y terceros autorizados, les aplicará lo dispuesto por el artículo 11 de las DCGA58, según el caso.


Datos recabados (categorías)
Identificación y autenticación, patrimoniales y/o financieros, créditos y laborales.
Ciclo de vida
1. Obtención: Personal, Directa e Indirecta. Previa o durante el establecimiento de la relación jurídica con el Cliente.
2- Almacenamiento: Sistema tecnológico. Expediente físico y/o digitalizado.
3- Usos: Evaluación cuantitativa y cualitativa de solvencia, verificación de historial crediticio, validar capacidad de pagos, revisión de ingresos y su relación con otros créditos y pasivos, revisión de historial de negocios, evaluación de garantías u obligados solidarios.
4. Divulgación: A. Transferencias. Sociedades de información crediticia, Proveedores de servicio de revisión de referecnias. B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting; -Cómputo en la nube, call Center, servicios de atención a cliente (SMS, Mail, redes sociales) y proveedores de destrucción segura de información).
5. Bloqueo: 15 días contados desde la fecha de rechazo y/o no aceptación.
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado cuando el tratamiento sea necesario para dar cumplimiento a la relación jurídica con el titular. o cuando este previsto en la Ley.
-Expreso por tratarse de datos patrimoniales y financieros.
-Expreso y por escrito o mediante tecnología de autenticación equivalente para datos sensibles.

1.2. PLD/CFT

Derivado del análisis de las operaciones de las IFC en cumplimiento a la normatividad señalada se identificaron los siguientes subprocesos en materia de PLD/CFT: 1) reportes que se deberán remitir a la SHCP; 2) intercambio de información; 3) clasificación de clientes por grado de riesgo: bajo, medio o alto; y 4) políticas de conocimiento de clientes

1.2.1.1. Reportes que se deberán remitir a la SHCP

En este subproceso se identificó que se utilizan datos de identificación y autenticación, patrimoniales y/o financieros y transaccionales para poder realizar los siguientes reportes: de operaciones relevantes, de operaciones en efectivo en moneda extranjera, de transferencias internacionales, de operaciones inusuales, de operaciones con activos virtuales y de operaciones internas preocupantes. asimismo, se identificó el siguiente ciclo de vida de los datos personales:

Se identificó el siguiente ciclo de vida de los datos personales en el subproceso de emisión de reportes a la SHCP:

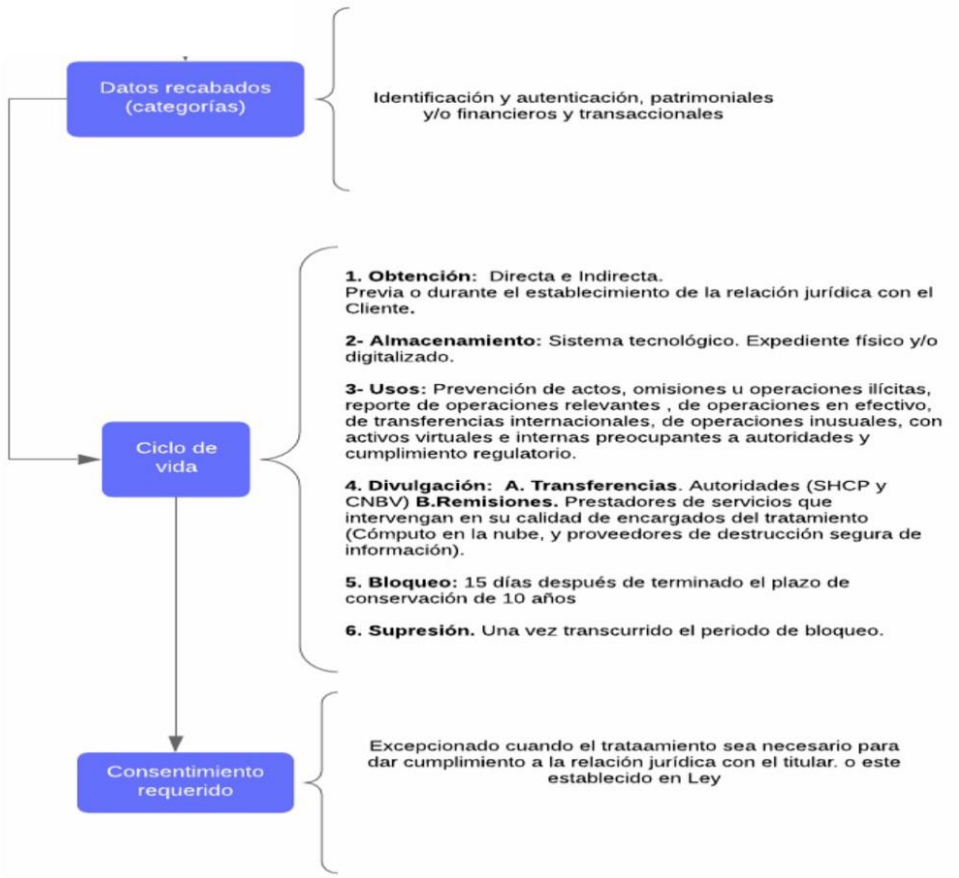
1) **Obtención:**
   - Personal, directa e indirecta.
   - Previa o durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
   - Sistema tecnológico.
   - Expediente físico y/o digitalizado.
3) **Usos:**
   - Prevención de actos, omisiones u operaciones ilícitas·
   - Reporte de operaciones relevantes, de operaciones en efectivo, de transferencias internacionales, de operaciones inusuales, con activos virtuales e internas preocupantes a autoridades.
   - Cumplimiento regulatorio,

4) **Divulgación/otros sujetos intervinientes:**
   - Transferencias:
     - SHCP.
     - CNBV.
   - Remisiones:
     - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
     - Cómputo en la nube.
     - Proveedores de destrucción segura de información.
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años[97].
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

¡

El ciclo de vida en el subproceso de emisión de reportes a la SHCP se resume en el siguiente diagrama:

[97] Artículo 25 de las Disposiciones de Carácter General a que se refiere el artículo 58 de la LRITF, fracción IV.


Datos recabados (categorías)
Identificación y autenticación, patrimoniales y/o financieros y transaccionales
Ciclo de vida
1. Obtención: Directa e Indirecta. Previa o durante el establecimiento de la relación jurídica con el Cliente.
2- Almacenamiento: Sistema tecnológico. Expediente físico y/o digitalizado.
3- Usos: Prevención de actos, omisiones u operaciones ilícitas, reporte de operaciones relevantes , de operaciones en efectivo, de transferencias internacionales, de operaciones inusuales, con activos virtuales e internas preocupantes a autoridades y cumplimiento regulatorio.
4. Divulgación: A. Transferencias. Autoridades (SHCP y CNBV) B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Cómputo en la nube, y proveedores de destrucción segura de información).
5. Bloqueo: 15 días después de terminado el plazo de conservación de 10 años
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado cuando el trataamiento sea necesario para dar cumplimiento a la relación jurídica con el titular. o este establecido en Ley

1.2.1.2. Intercambio de información

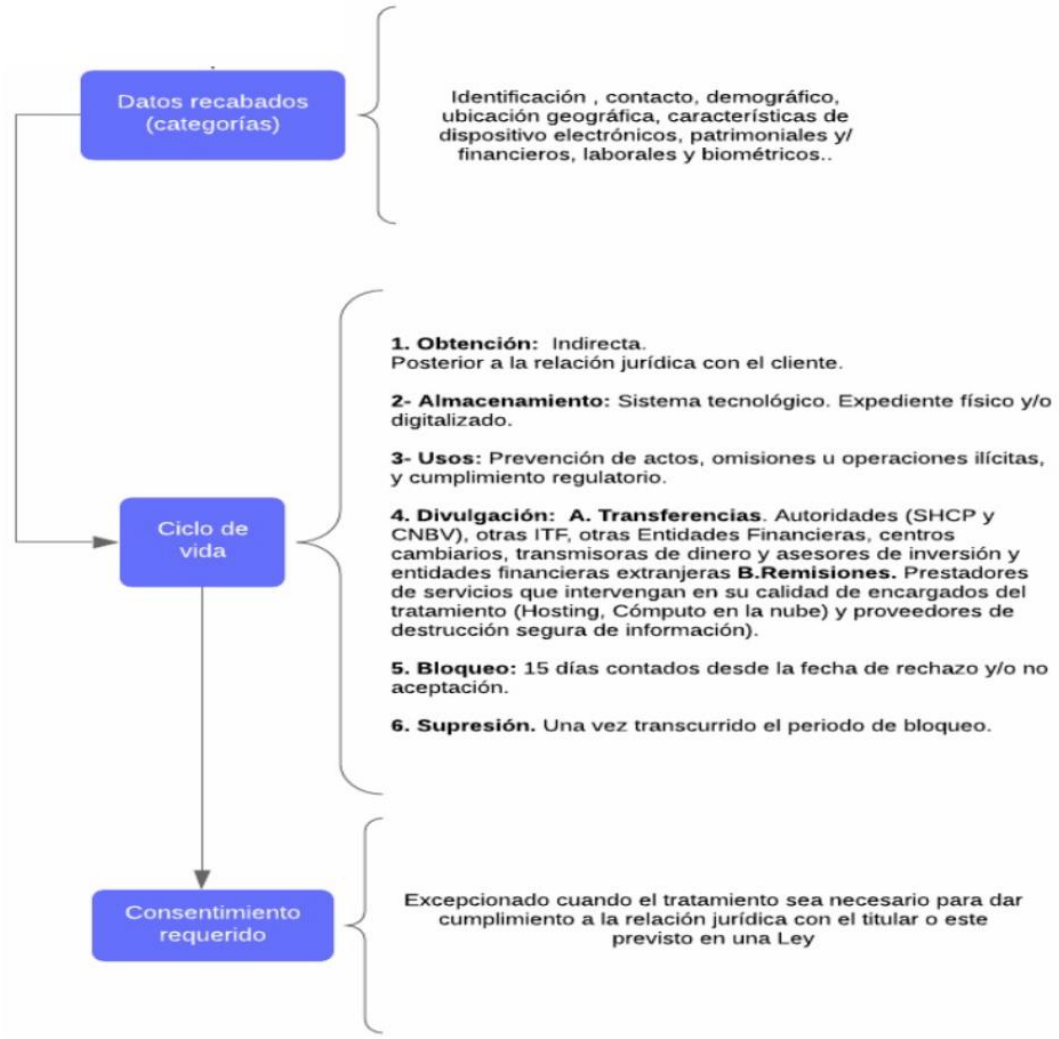
En este subproceso se identificó que se obtienen datos personales de identificación, contacto, demográficos, ubicación geográfica, características de dispositivos electrónicos, patrimoniales y/o financieros, laborales y biométricos. Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención**:
    - Indirecta.
    - Posterior al establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento**:
    - Sistema tecnológico.
    - Expediente físico y/o digitalizado.
3) **Usos**:
    - Prevención de actos, omisiones u operaciones ilícitas.
    - Cumplimiento regulatorio.

4) **Divulgación/otros sujetos intervinientes:**
    - ***Transferencias:***
        - CNBV
        - SHCP
        - Otras ITF.
        - Otras Entidades Financieras, centros cambiarios, transmisores de dinero y asesores de inversión[98].
        - Entidades Financieras Extranjeras
    - ***Remisiones***:
        - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
        - Hosting
        - Cómputo en la nube.
        - Proveedores de destrucción segura de información.
5) **Bloqueo**: 15 días contados desde la fecha de rechazo y/o no aceptación.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

El ciclo de vida de este subproceso se resume en el siguiente diagrama:

[98] Se exceptúa el consentimiento por 37.1 de la LFPDPPP y el artículo 79 de las DCGA58.

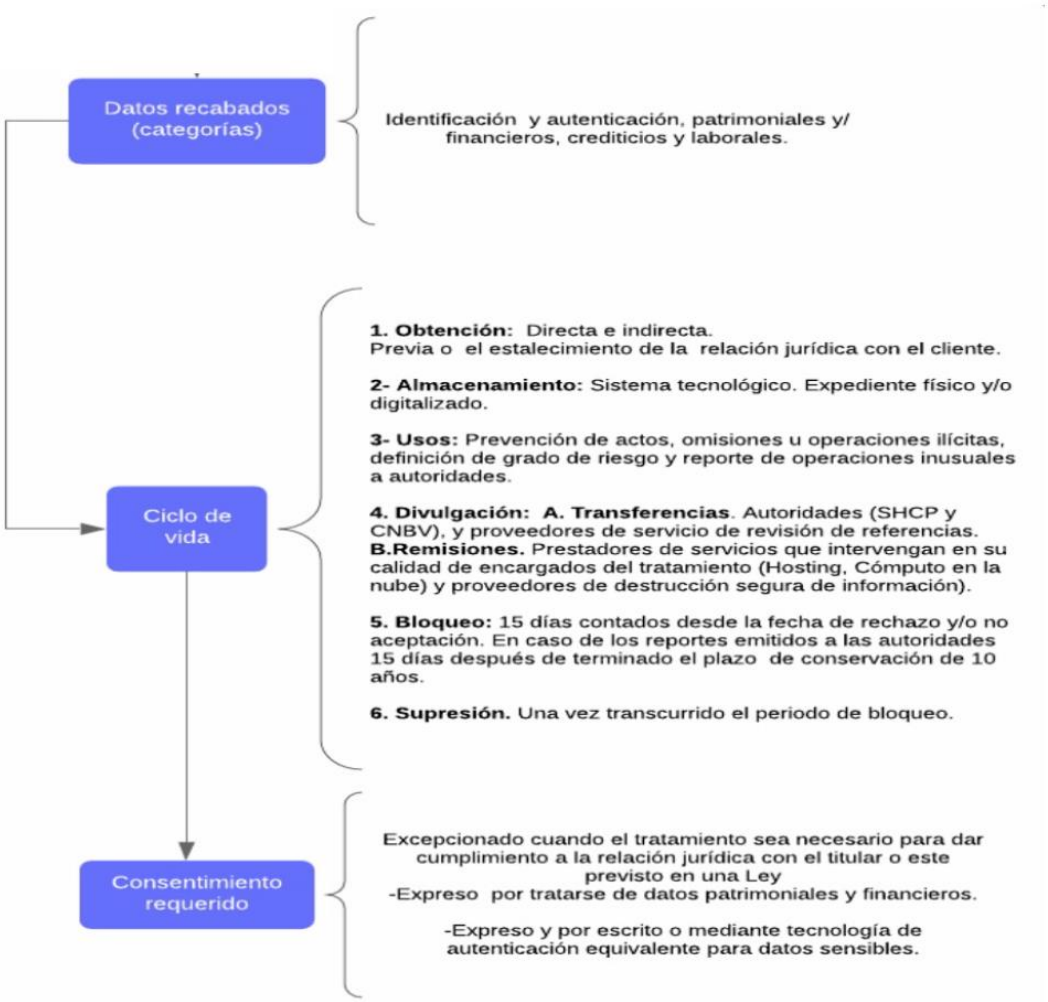

Datos recabados (categorías)
Identificación , contacto, demográfico, ubicación geográfica, características de dispositivo electrónicos, patrimoniales y/ financieros, laborales y biométricos..
Ciclo de vida
1. Obtención: Indirecta.
Posterior a la relación jurídica con el cliente.
2- Almacenamiento: Sistema tecnológico. Expediente físico y/o digitalizado.
3- Usos: Prevención de actos, omisiones u operaciones ilícitas, y cumplimiento regulatorio.
4. Divulgación: A. Transferencias. Autoridades (SHCP y CNBV), otras ITF, otras Entidades Financieras, centros cambiarios, transmisoras de dinero y asesores de inversión y entidades financieras extranjeras B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting, Cómputo en la nube) y proveedores de destrucción segura de información).
5. Bloqueo: 15 días contados desde la fecha de rechazo y/o no aceptación.
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado cuando el tratamiento sea necesario para dar cumplimiento a la relación jurídica con el titular o este previsto en una Ley

1.2.1.3. Clasificación de Clientes por Grado de Riesgo: bajo, medio o alto

En este subproceso se identificó que se obtienen datos personales de identificación y autenticación, patrimoniales y/o financieros, crediticios y laborales. Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención:**
   - Directa e indirecta.
   - Previa o durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
   - Sistema tecnológico.
   - Expediente físico y/o digitalizado.
3) **Usos:**
   - Prevención de actos, omisiones u operaciones ilícitas.
   - Definición del Grado de Riesgo.
   - Reporte de operaciones inusuales a autoridades.
4) **Divulgación/otros sujetos intervinientes:**
   - Transferencias:
     - SHCP.
     - CNBV.
     - Proveedor de servicio de revisión de referencias.
   - Remisiones:
     - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
     - Hosting.
     - Cómputo en la nube.
     - Proveedores de destrucción segura de información.
5) **Bloqueo**:
   - 15 días contados desde la fecha de rechazo y/o no aceptación.
   - En caso de los reportes emitidos a las autoridades: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión:** una vez transcurrido el periodo de bloqueo.

El ciclo de vida de este subproceso se resume en el siguiente diagrama:

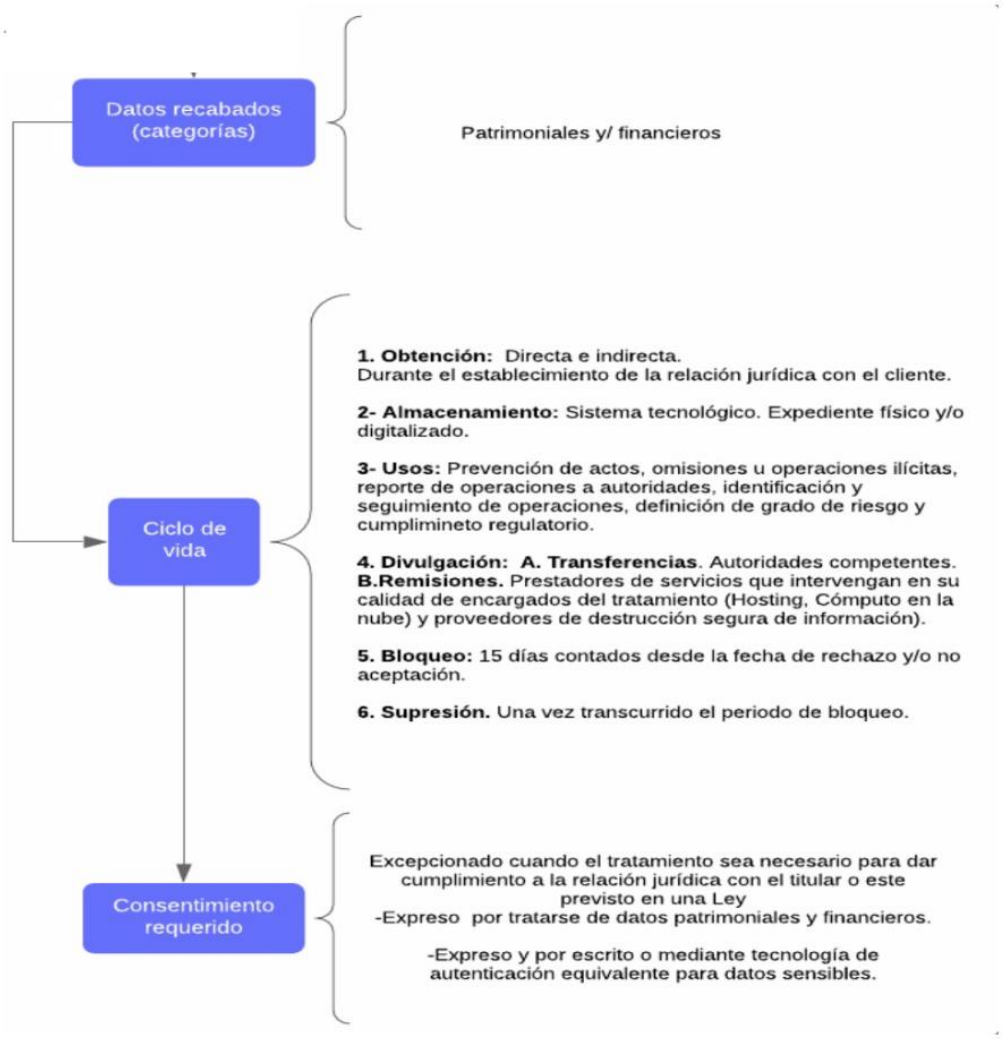

Datos recabados (categorías)
Identificación y autenticación, patrimoniales y/ financieros, crediticios y laborales.
Ciclo de vida
1. Obtención: Directa e indirecta. Previa o el estalecimiento de la relación jurídica con el cliente.
2- Almacenamiento: Sistema tecnológico. Expediente físico y/o digitalizado.
3- Usos: Prevención de actos, omisiones u operaciones ilícitas, definición de grado de riesgo y reporte de operaciones inusuales a autoridades.
4. Divulgación: A. Transferencias. Autoridades (SHCP y CNBV), y proveedores de servicio de revisión de referencias. B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting, Cómputo en la nube) y proveedores de destrucción segura de información).
5. Bloqueo: 15 días contados desde la fecha de rechazo y/o no aceptación. En caso de los reportes emitidos a las autoridades 15 días después de terminado el plazo de conservación de 10 años.
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado cuando el tratamiento sea necesario para dar cumplimiento a la relación jurídica con el titular o este previsto en una Ley
-Expreso por tratarse de datos patrimoniales y financieros.
-Expreso y por escrito o mediante tecnología de autenticación equivalente para datos sensibles.

1.2.1.4. Políticas de conocimiento de clientes

En este subproceso se identificó que se obtienen datos personales patrimoniales y/o financieros. Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención**:
    - Directa e indirecta.
    - Durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
    - Sistema tecnológico.
    - Expediente físico y/o digitalizado.
3) **Usos**:
    - Prevención de actos, omisiones u operaciones ilícitas.
    - Reporte de operaciones a autoridades.
    - Identificación y seguimiento de Operaciones.
    - Definición de Grado de Riesgo.
    - Cumplimiento Regulatorio.
4) **Divulgación/otros sujetos intervinientes:**
    - Transferencias:
        - Autoridades competentes,
    - Remisiones:
        - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
        - Hosting.
        - Cómputo en la nube.
        - Proveedores de destrucción segura de información.
5) **Bloqueo**: 15 días contados desde la fecha de rechazo y/o no aceptación.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

El ciclo de vida de este subproceso se resume en el siguiente diagrama:

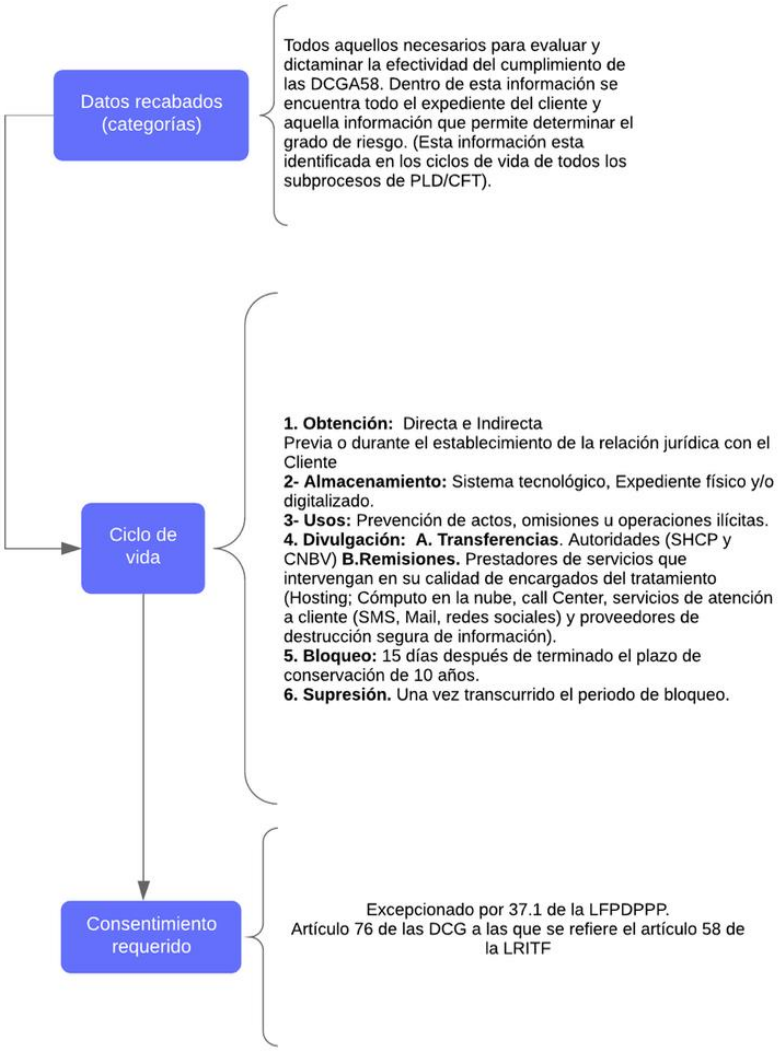

Datos recabados (categorías)
Patrimoniales y/ financieros
Ciclo de vida
1. Obtención: Directa e indirecta.
Durante el establecimiento de la relación jurídica con el cliente.
2- Almacenamiento: Sistema tecnológico. Expediente físico y/o digitalizado.
3- Usos: Prevención de actos, omisiones u operaciones ilícitas, reporte de operaciones a autoridades, identificación y seguimiento de operaciones, definición de grado de riesgo y cumplimineto regulatorio.
4. Divulgación: A. Transferencias. Autoridades competentes.
B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting, Cómputo en la nube) y proveedores de destrucción segura de información).
5. Bloqueo: 15 días contados desde la fecha de rechazo y/o no aceptación.
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado cuando el tratamiento sea necesario para dar cumplimiento a la relación jurídica con el titular o este previsto en una Ley
-Expreso por tratarse de datos patrimoniales y financieros.
-Expreso y por escrito o mediante tecnología de autenticación equivalente para datos sensibles.

1.2.1.5. Auditoría para revisar el cumplimiento de las DCGA58

En este subproceso se identificó que se obtienen todos aquellos datos necesarios para evaluar y dictaminar la efectividad del cumplimiento de las DCGA58. Dentro de esta información se encuentra todo el expediente del cliente y aquella información que permite determinar el grado de riesgo. (Esta información esta identificada en los ciclos de vida de todos los subprocesos de PLD/CFT).
Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención**:
    - Directa e indirecta.
    - Previa o durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
    - Sistema tecnológico.
    - Expediente físico y/o digitalizado.
3) **Usos:**
    - Prevención de actos, omisiones u operaciones ilícitas.
4) **Divulgación/otros sujetos intervinientes:**
    - Transferencias:
        - Autoridades competentes (SHCP y CNBV),
    - Remisiones:
        - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
        - Hosting.
        - Cómputo en la nube.
        - Call center.
        - Servicios de atención al cliente.
        - Proveedores de destrucción segura de información.
5) **Bloqueo:** 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión:** una vez transcurrido el periodo de bloqueo.

El ciclo de vida de este subproceso se resume en el siguiente diagrama:

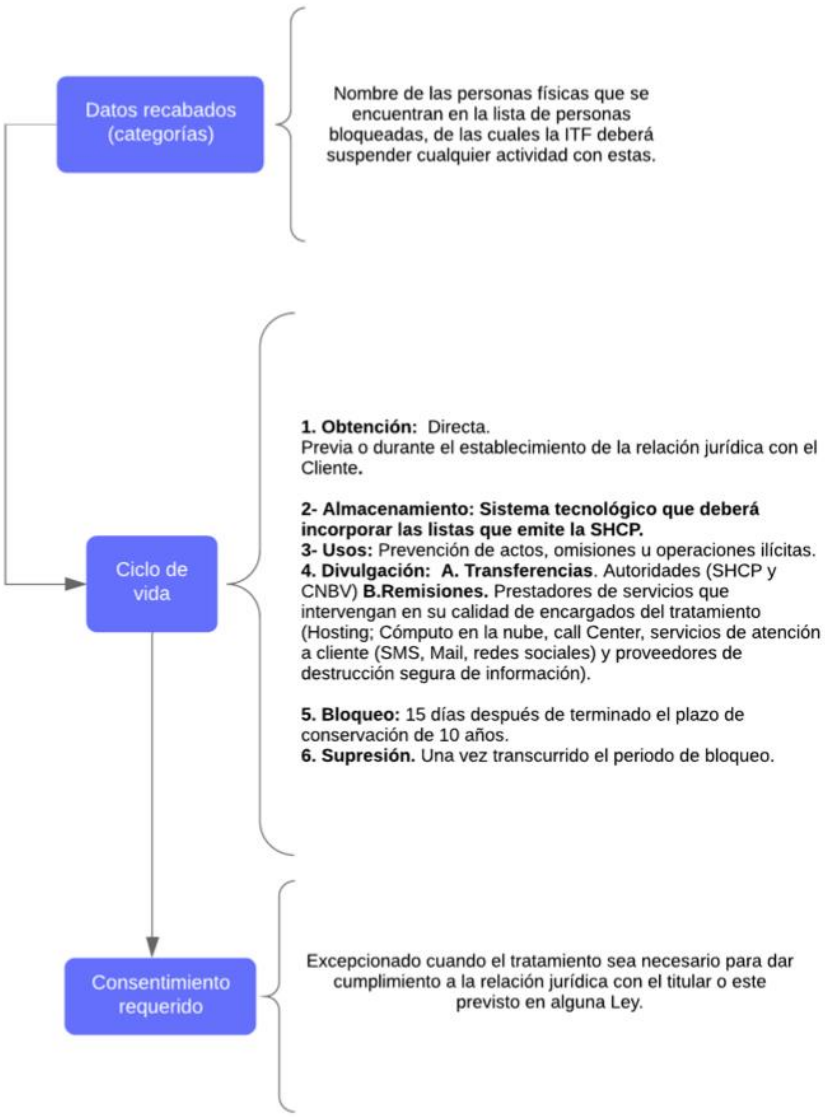

Datos recabados (categorías)
Todos aquellos necesarios para evaluar y dictaminar la efectividad del cumplimiento de las DCGA58. Dentro de esta información se encuentra todo el expediente del cliente y aquella información que permite determinar el grado de riesgo. (Esta información esta identificada en los ciclos de vida de todos los subprocesos de PLD/CFT).
Ciclo de vida
1. Obtención: Directa e Indirecta
Previa o durante el establecimiento de la relación jurídica con el Cliente
2- Almacenamiento: Sistema tecnológico, Expediente físico y/o digitalizado.
3- Usos: Prevención de actos, omisiones u operaciones ilícitas.
4. Divulgación: A. Transferencias. Autoridades (SHCP y CNBV) B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting; Cómputo en la nube, call Center, servicios de atención a cliente (SMS, Mail, redes sociales) y proveedores de destrucción segura de información).
5. Bloqueo: 15 días después de terminado el plazo de conservación de 10 años.
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado por 37.1 de la LFPDPPP.
Artículo 76 de las DCG a las que se refiere el artículo 58 de la LRITF

1.2.1.6. Obligaciones de las ITF respecto a la lista de personas bloqueadas

En este subproceso se identificó que se obtiene como dato personal el nombre de las personas físicas que se encuentran en la lista de personas bloqueadas que publica la SHCP, de las cuales la ITF deberá suspender cualquier actividad con estas.
Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención**:
    - Directa.
    - Previa o durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
    - Sistema tecnológico que deberá incorporar las listas de personas bloqueadas que emite la SHCP.
3) **Usos:**
    - Prevención de actos, omisiones u operaciones ilícitas.
4) **Divulgación/otros sujetos intervinientes:**
    - Transferencias:
        - Autoridades competentes (SHCP y CNBV),
    - Remisiones:
        - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
        - Hosting.
        - Cómputo en la nube.
        - Call Center.
        - Servicios de atención a cliente.
        - Proveedores de destrucción segura de información.
5) **Bloqueo:** 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión:** una vez transcurrido el periodo de bloqueo.

El ciclo de vida de este subproceso se resume en el siguiente diagrama:

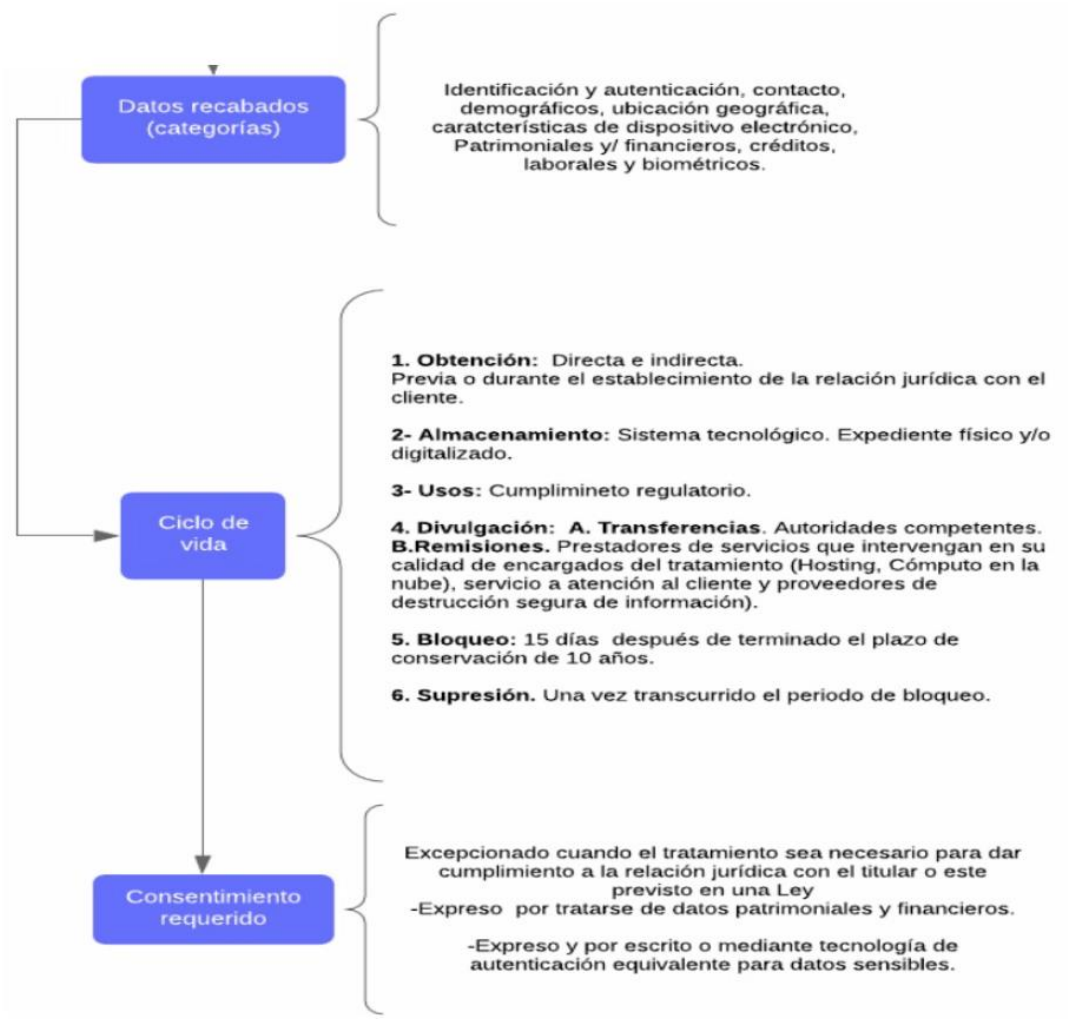

Datos recabados (categorías)
Nombre de las personas físicas que se encuentran en la lista de personas bloqueadas, de las cuales la ITF deberá suspender cualquier actividad con estas.
Ciclo de vida
1. Obtención: Directa.
Previa o durante el establecimiento de la relación jurídica con el Cliente.
2- Almacenamiento: Sistema tecnológico que deberá incorporar las listas que emite la SHCP.
3- Usos: Prevención de actos, omisiones u operaciones ilícitas.
4. Divulgación: A. Transferencias. Autoridades (SHCP y CNBV) B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting; Cómputo en la nube, call Center, servicios de atención a cliente (SMS, Mail, redes sociales) y proveedores de destrucción segura de información).
5. Bloqueo: 15 días después de terminado el plazo de conservación de 10 años.
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado cuando el tratamiento sea necesario para dar cumplimiento a la relación jurídica con el titular o este previsto en alguna Ley.

1.2.2. Obligación de conservar documentos

Las IFC tienen la obligación de conservar la información y documentación sobre las operaciones que celebre; así como, la información y documentación de la identificación de sus clientes. Derivado de lo anterior, se observó que se obtienen datos personales de identificación y autenticación, contacto, demográficos, ubicación geográfica, características de dispositivo electrónico, patrimoniales y/o financieros, crediticios, laborales y biométricos. Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención:**
    - Directa e indirecta.
    - Durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
    - Sistema tecnológico.
    - Expediente físico y/o digitalizado.
3) **Usos**:
    - Cumplimiento Regulatorio.
4) **Divulgación/otros sujetos intervinientes:**
    - Transferencias:
        - Autoridades competentes.
    - Remisiones:
        - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
        - Hosting.
        - Cómputo en la nube.
        - Servicio de atención a cliente.
        - Proveedores de destrucción segura de información.
5) **Bloqueo:** 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión:** una vez transcurrido el periodo de bloqueo.

El ciclo de vida de este subproceso se resume en el siguiente diagrama:

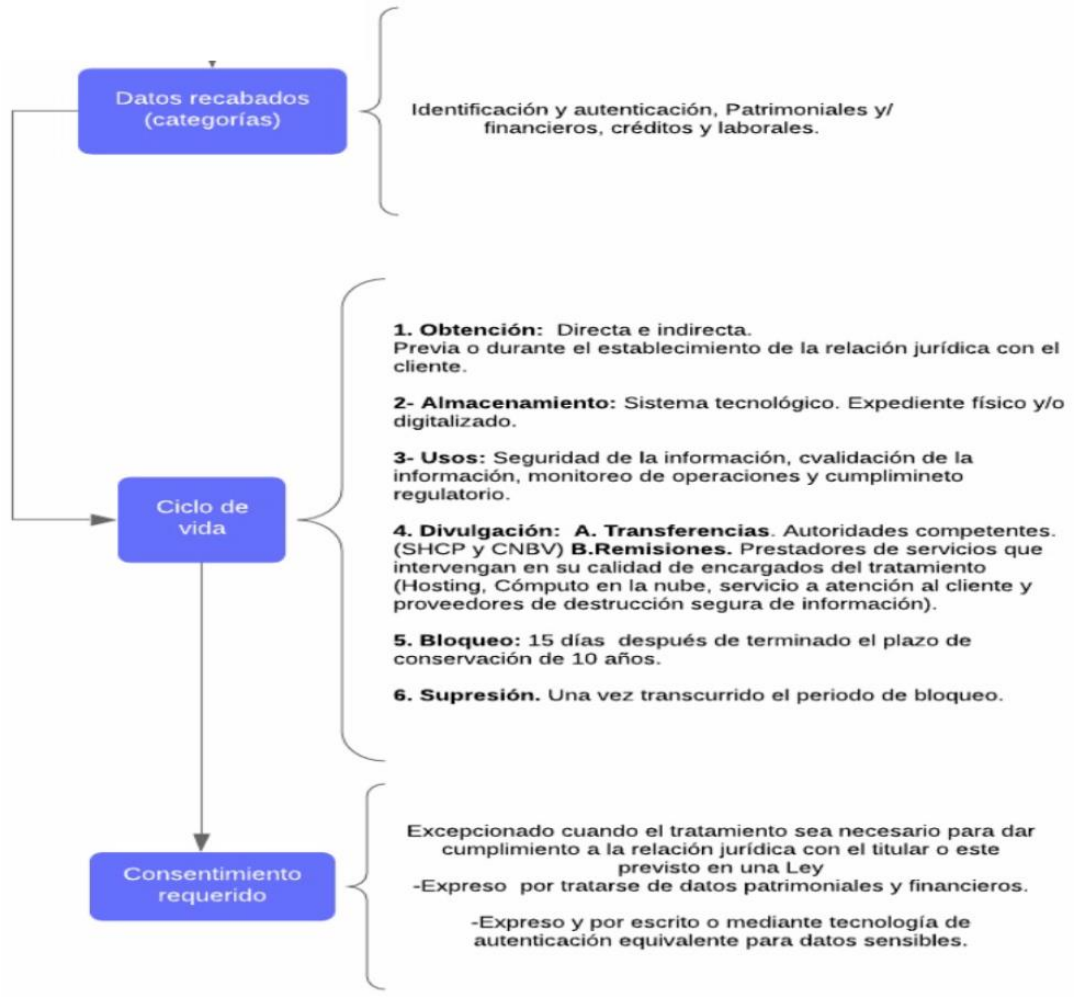

Datos recabados (categorías)
Identificación y autenticación, contacto, demográficos, ubicación geográfica, caratcterísticas de dispositivo electrónico, Patrimoniales y/ financieros, créditos, laborales y biométricos.
Ciclo de vida
1. Obtención: Directa e indirecta. Previa o durante el establecimiento de la relación jurídica con el cliente.
2- Almacenamiento: Sistema tecnológico. Expediente físico y/o digitalizado.
3- Usos: Cumplimineto regulatorio.
4. Divulgación: A. Transferencias. Autoridades competentes. B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting, Cómputo en la nube), servicio a atención al cliente y proveedores de destrucción segura de información).
5. Bloqueo: 15 días después de terminado el plazo de conservación de 10 años.
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado cuando el tratamiento sea necesario para dar cumplimiento a la relación jurídica con el titular o este previsto en una Ley
-Expreso por tratarse de datos patrimoniales y financieros.
-Expreso y por escrito o mediante tecnología de autenticación equivalente para datos sensibles.

1.2.3. Mecanismos de seguimiento y agrupaciones de operaciones

En este proceso se identificó el tratamiento de datos personales de identificación y autenticación, patrimoniales y/o financieros, crediticios y laborales) Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención:**
    - Directa e indirecta.
    - Previa o durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
    - Sistema tecnológico.
    - Expediente físico y/o digitalizado.
3) **Usos:**
    - Seguridad de la información.
    - Validación de la información.
    - Monitoreo de operaciones.
    - Cumplimiento regulatorio.
4) **Divulgación/otros sujetos intervinientes:**
    - Transferencias:
        - CNBV.
        - SHCP.
    - Remisiones:
        - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
        - Hosting.
        - Cómputo en la nube.
        - Servicio de atención a cliente.
        - Proveedores de destrucción segura de información.
5) **Bloqueo:** 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

El ciclo de vida de este subproceso se resume en el siguiente diagrama:


Datos recabados (categorías)
Identificación y autenticación, Patrimoniales y/ financieros, créditos y laborales.
Ciclo de vida
1. Obtención: Directa e indirecta. Previa o durante el establecimiento de la relación jurídica con el cliente.
2- Almacenamiento: Sistema tecnológico. Expediente físico y/o digitalizado.
3- Usos: Seguridad de la información, cvalidación de la información, monitoreo de operaciones y cumplimineto regulatorio.
4. Divulgación: A. Transferencias. Autoridades competentes. (SHCP y CNBV) B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting, Cómputo en la nube, servicio a atención al cliente y proveedores de destrucción segura de información).
5. Bloqueo: 15 días después de terminado el plazo de conservación de 10 años.
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado cuando el tratamiento sea necesario para dar cumplimiento a la relación jurídica con el titular o este previsto en una Ley
-Expreso por tratarse de datos patrimoniales y financieros.
-Expreso y por escrito o mediante tecnología de autenticación equivalente para datos sensibles.

1.2.4. Aspectos generales de las IFC

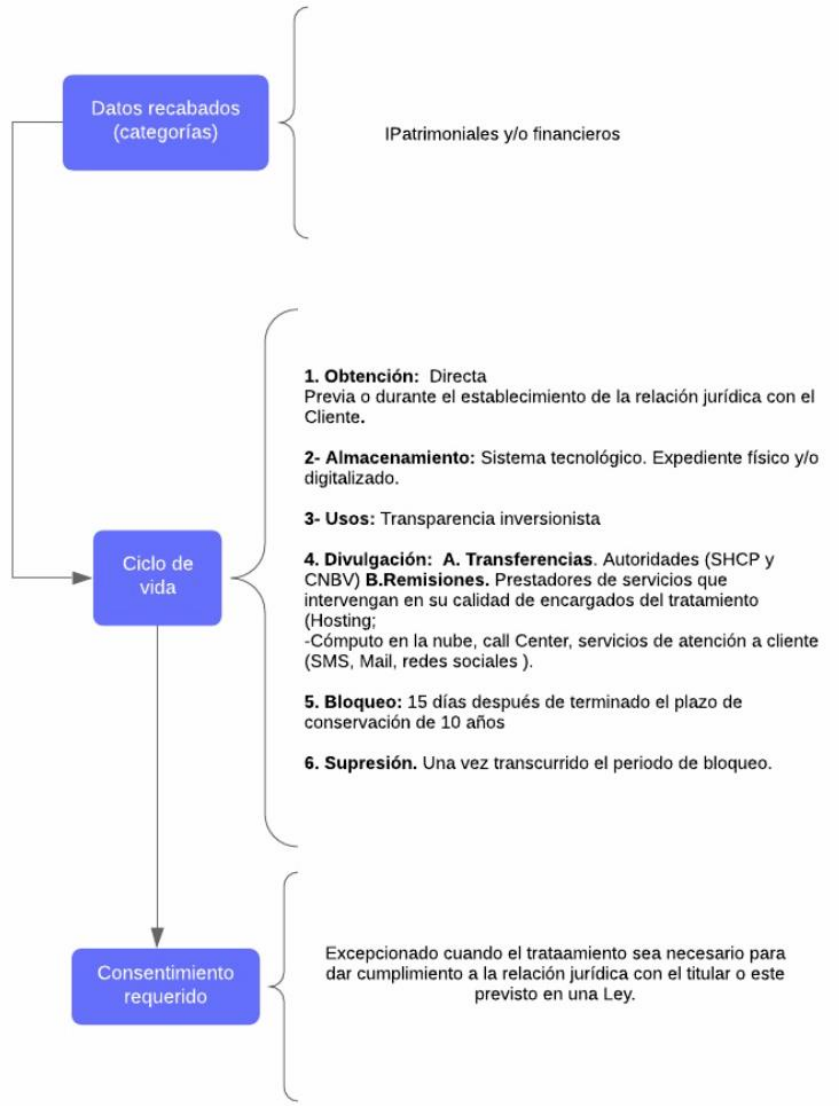
1.2.4.1. Constancia electrónica sobre riesgos

Se identificó que se obtienen datos personales patrimoniales y/o financieros. Asimismo, se identifica a continuación el ciclo de vida de los datos personales:

1) **Obtención:**
   - Directa.
   - Previa o durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
   - Sistema tecnológico.
   - Expediente físico y/o digitalizado.
3) **Usos:** Transparencia a inversionistas.

4) **Divulgación/otros sujetos intervinientes:**
   - Transferencias:
     - CNBV.
     - SHCP.
   - Remisiones:
     - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
     - Hosting.
     - Cómputo en la nube.
     - Call Center.
     - Servicios de atención al cliente.
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

El ciclo de vida de este subproceso se resume en el siguiente diagrama:


Datos recabados (categorías)
IPatrimoniales y/o financieros
Ciclo de vida
1. Obtención: Directa
Previa o durante el establecimiento de la relación jurídica con el Cliente.
2- Almacenamiento: Sistema tecnológico. Expediente físico y/o digitalizado.
3- Usos: Transparencia inversionista
4. Divulgación: A. Transferencias. Autoridades (SHCP y CNBV) B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting;
-Cómputo en la nube, call Center, servicios de atención a cliente (SMS, Mail, redes sociales).
5. Bloqueo: 15 días después de terminado el plazo de conservación de 10 años
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado cuando el trataamiento sea necesario para dar cumplimiento a la relación jurídica con el titular o este previsto en una Ley.

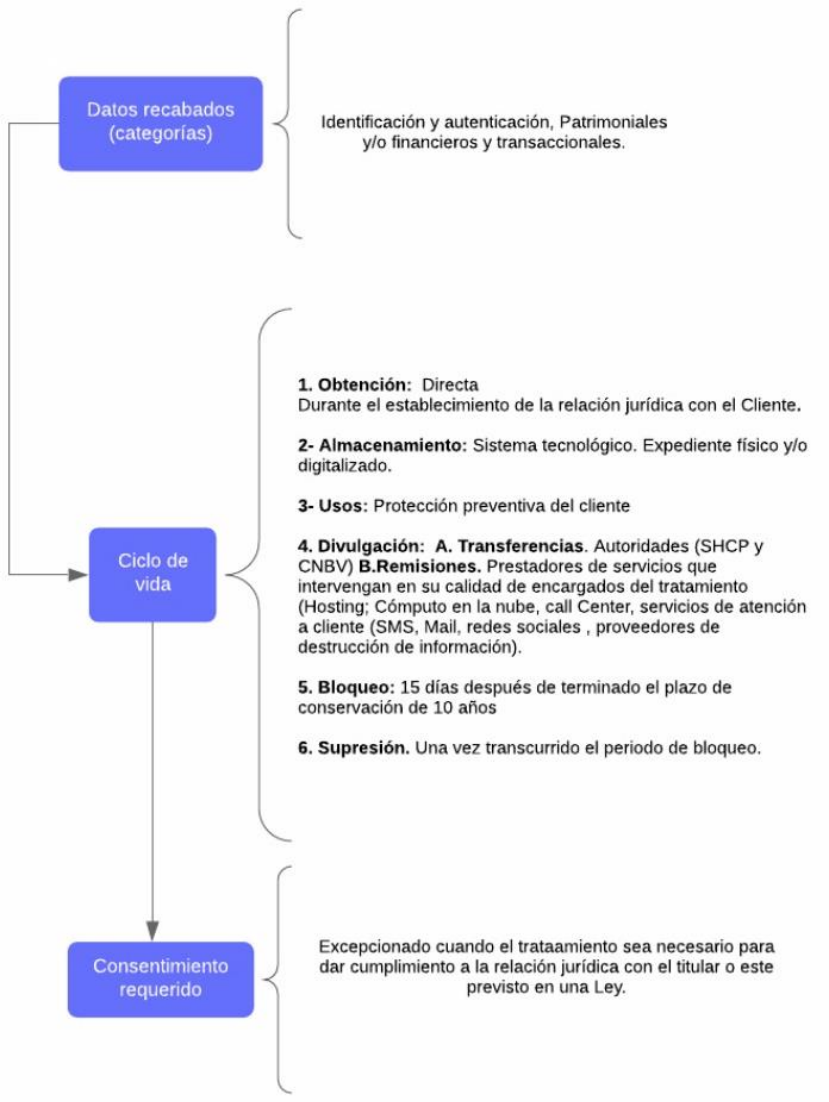
1.2.4.2. Límites de recursos que las IFC podrán mantener a nombre de clientes

Se identificó que se obtienen datos personales de identificación y autenticación, patrimoniales y/o financieros, y transaccionales. Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención:**
    - Directa.
    - Durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
    - Sistema tecnológico.
    - Expediente físico y/o digitalizado.
3) **Usos**: Protección preventiva del cliente.

4) **Divulgación/otros sujetos intervinientes:**
    - Transferencias:
        - CNBV.
        - SHCP.
    - Remisiones:
        - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
        - Hosting.
        - Cómputo en la nube.
        - Call Center.
        - Servicios de atención al cliente.
        - Proveedor de destrucción segura de la información.
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

El ciclo de vida de este subproceso se resume en el siguiente diagrama:


Datos recabados (categorías)
Identificación y autenticación, Patrimoniales y/o financieros y transaccionales.
Ciclo de vida
1. Obtención: Directa
Durante el establecimiento de la relación jurídica con el Cliente.
2- Almacenamiento: Sistema tecnológico. Expediente físico y/o digitalizado.
3- Usos: Protección preventiva del cliente
4. Divulgación: A. Transferencias. Autoridades (SHCP y CNBV) B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting; Cómputo en la nube, call Center, servicios de atención a cliente (SMS, Mail, redes sociales , proveedores de destrucción de información).
5. Bloqueo: 15 días después de terminado el plazo de conservación de 10 años
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado cuando el trataamiento sea necesario para dar cumplimiento a la relación jurídica con el titular o este previsto en una Ley.

1.2.4.3. Mandatos y comisiones

Respecto a los mandatos y comisiones se pueden identificar los siguientes:

1. **Mandatos y comisiones para Efectuar Operaciones.**

Se identificó que se obtienen datos personales de identificación y autenticación y patrimoniales y/o financieros. Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención**:
   - Directa.
   - Durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento**:
   - Sistema tecnológico.
   - Expediente físico y/o digitalizado.
3) **Usos**:
   - Cumplimiento de obligaciones contractuales.
   - Cumplimiento regulatorio.

4) **Divulgación/otros sujetos intervinientes:**
   - Transferencias:
     - CNBV.
     - SHCP.
   - Remisiones:
     - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
     - Hosting.
     - Cómputo en la nube.
     - Call Center.
     - Servicios de atención al cliente.
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

2. **Mandatos y comisiones para invertir, por cuenta de los Inversionistas, sus recursos o activos virtuales.**

Se identificó que se obtienen datos personales de identificación y autenticación y patrimoniales y/o financieros. Asimismo, se identificó el siguiente ciclo de vida de datos personales:

1) **Obtención**:
   - Directa.
   - Durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento**:
   - Sistema tecnológico.
   - Expediente físico y/o digitalizado.
3) **Usos**:
   - Cumplimiento de obligaciones contractuales.
   - Cumplimiento regulatorio.

4) **Divulgación/otros sujetos intervinientes:**
   - Transferencias:

    - CNBV.
    - SHCP.
- Remisiones:
    - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
    - Hosting.
    - Cómputo en la nube.
    - Call Center.
    - Servicios de atención al cliente.

5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

3. Mandatos y comisiones para cobranza extrajudicial.

Se identificó que se obtienen datos personales de identificación y autenticación y patrimoniales y/o financieros. Asimismo, se identificó el siguiente ciclo de vida de datos personales:

1) **Obtención**:
    - Directa.
    - Durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento**:
    - Sistema tecnológico.
    - Expediente físico y/o digitalizado.
3) **Usos**:
    - Cumplimiento de obligaciones contractuales.
    - Cumplimiento regulatorio.
4) **Divulgación/otros sujetos intervinientes:**
    - Transferencias[99]:
        - CNBV.
        - SHCP.
    - Remisiones:
        - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
        - Hosting.
        - Cómputo en la nube.
        - Call Center.
        - Servicios de atención al cliente.
        - Despacho de cobranza.
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

4. Mandatos y comisiones para representar a los Inversionistas en asambleas de accionistas, socios o cualquier órgano de decisión colegiada.

Se identificó que se obtienen datos personales de identificación y autenticación y patrimoniales y/o financieros. Asimismo, se identificó el siguiente ciclo de vida para los datos personales:

1) **Obtención**:
    - Directa.
    - Durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
    - Sistema tecnológico.

[99] Se exceptúa el consentimiento por 37.1 de la LFPDPPP y el artículo 100 de las DCG para regular las ITF.

- Expediente físico y/o digitalizado.

3) **Usos**:
   - Cumplimiento de obligaciones contractuales.
   - Cumplimiento regulatorio.
4) **Divulgación/otros sujetos intervinientes:**
   - Transferencias:
     - CNBV.
     - SHCP.
   - Remisiones:
     - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
     - Hosting.
     - Cómputo en la nube.
     - Call Center.
     - Servicios de atención al cliente.
     - Órganos de decisión colegiada.
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

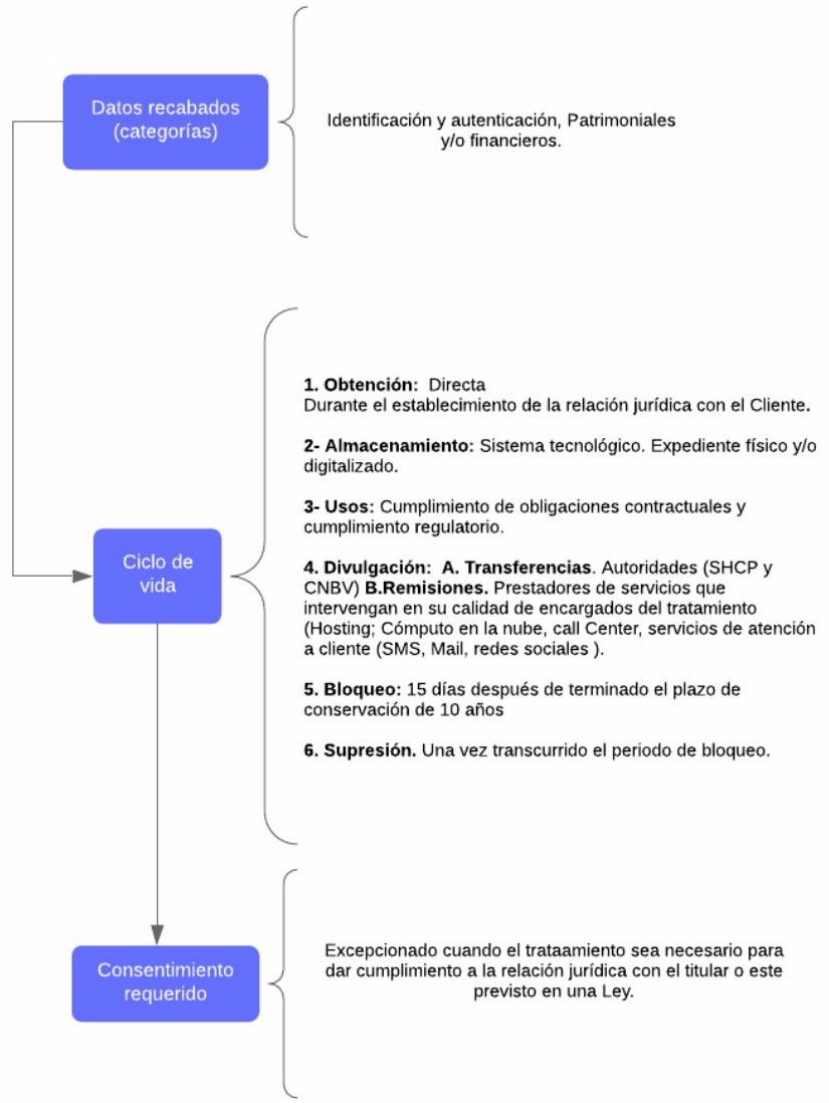
5. Informar en sus plataformas las actividades llevadas a cabo en la ejecución de mandatos y comisiones.

Se identificó que se obtienen datos personales de identificación y autenticación y patrimoniales y/o financieros. Asimismo, se identificó el siguiente ciclo de vida:

1) **Obtención**:
   - Directa.
   - Durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento**:
   - Sistema tecnológico.
   - Expediente físico y/o digitalizado.
3) **Usos**:
   - Cumplimiento de obligaciones contractuales.
   - Cumplimiento regulatorio.

4) **Divulgación/otros sujetos intervinientes:**
   - Transferencias:
     - CNBV.
     - SHCP.
   - Remisiones:
     - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
     - Hosting.
     - Cómputo en la nube.
     - Call Center.
     - Servicios de atención al cliente.
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

El ciclo de vida de este proceso se resume en el siguiente diagrama:


Datos recabados (categorías)
Identificación y autenticación, Patrimoniales y/o financieros.
Ciclo de vida
1. Obtención: Directa
Durante el establecimiento de la relación jurídica con el Cliente.
2- Almacenamiento: Sistema tecnológico. Expediente físico y/o digitalizado.
3- Usos: Cumplimiento de obligaciones contractuales y cumplimiento regulatorio.
4. Divulgación: A. Transferencias. Autoridades (SHCP y CNBV) B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting; Cómputo en la nube, call Center, servicios de atención a cliente (SMS, Mail, redes sociales).
5. Bloqueo: 15 días después de terminado el plazo de conservación de 10 años
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado cuando el trataamiento sea necesario para dar cumplimiento a la relación jurídica con el titular o este previsto en una Ley.

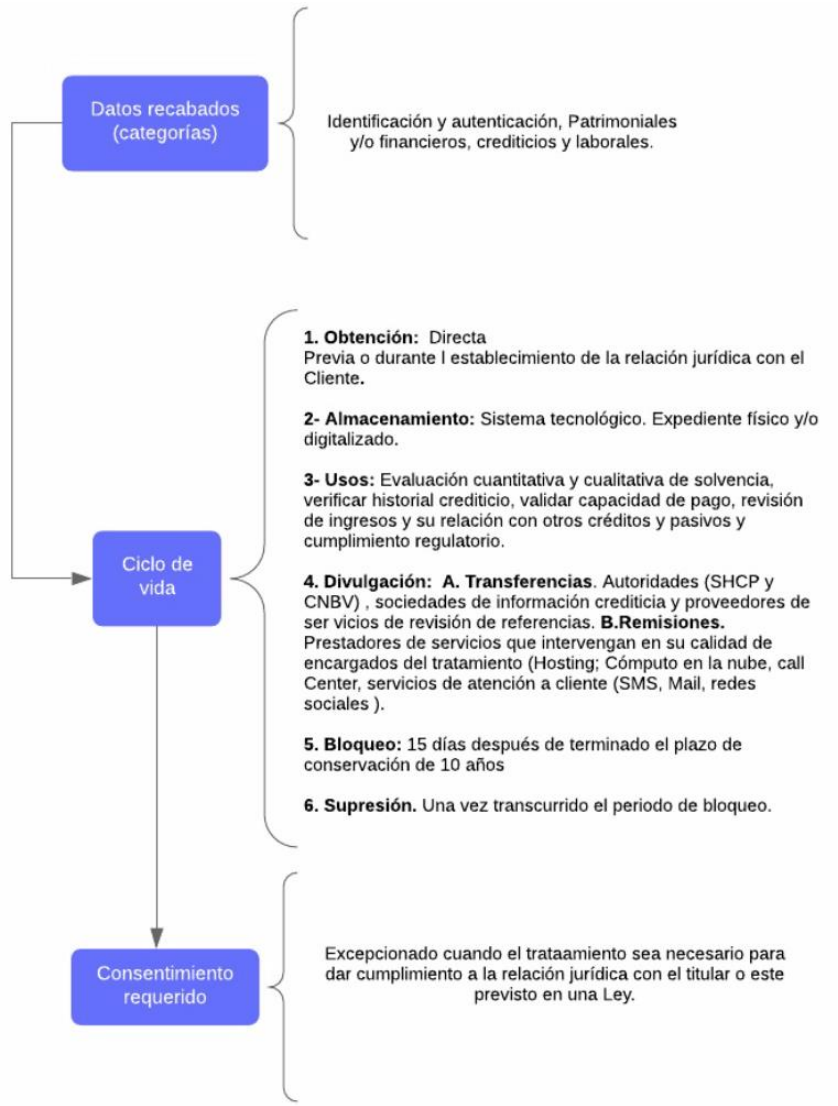
1.2.5. Operaciones de las IFC

Respecto a las operaciones se identifica el tratamiento de datos personales en la determinación del grado riesgo para cada tipo de financiamiento colectivo.

Para este tipo de operación se utiliza datos personales de identificación y autenticación, patrimoniales y financieros, crediticios y laborales. Asimismo, se identificó el siguiente ciclo de vida:

1) **Obtención:**
    - Directa e Indirecta.
    - Previa o durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
    - Sistema tecnológico.
    - Expediente físico y/o digitalizado.
3) **Usos**:
    - Evaluación cuantitativa y cualitativa de solvencia.
    - Verificar historial crediticio.
    - Validar capacidad de pago.
    - Revisión de ingresos y su relación con otros crédito y pasivos.
    - Cumplimiento regulatorio.
4) **Divulgación/otros sujetos intervinientes:**
    - Transferencias:
        - Sociedad de información crediticia.
        - SHCP.
        - CNBV.
        - Proveedores de servicio de revisión de referencias.
    - Remisiones:
        - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
        - Hosting.
        - Cómputo en la nube.
        - Call Center.
        - Servicios de atención al cliente.
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

El ciclo de vida de este proceso se resume en el siguiente diagrama:

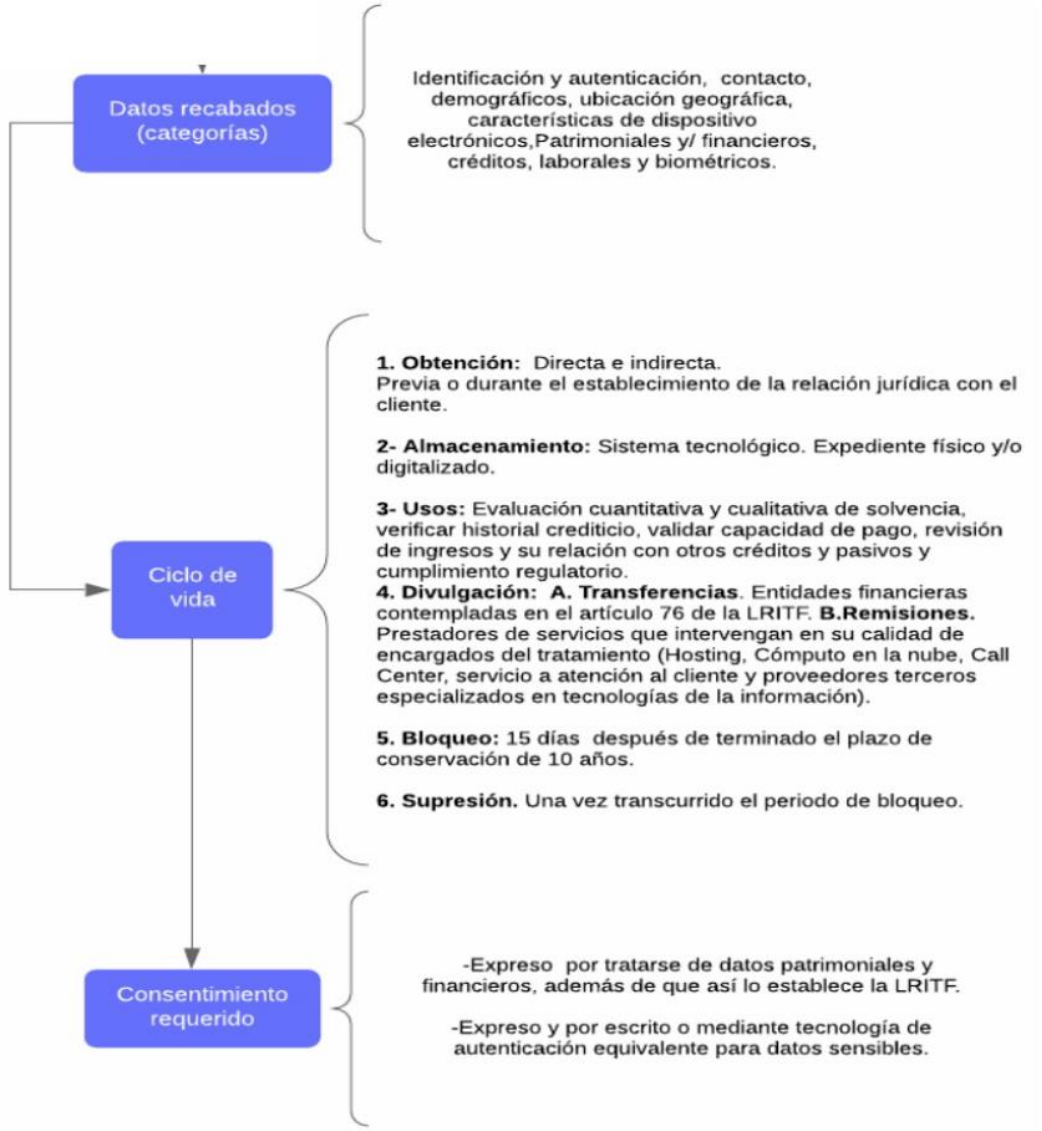

Datos recabados (categorías)
Identificación y autenticación, Patrimoniales y/o financieros, crediticios y laborales.
Ciclo de vida
1. Obtención: Directa
Previa o durante l establecimiento de la relación jurídica con el Cliente.
2- Almacenamiento: Sistema tecnológico. Expediente físico y/o digitalizado.
3- Usos: Evaluación cuantitativa y cualitativa de solvencia, verificar historial crediticio, validar capacidad de pago, revisión de ingresos y su relación con otros créditos y pasivos y cumplimiento regulatorio.
4. Divulgación: A. Transferencias. Autoridades (SHCP y CNBV) , sociedades de información crediticia y proveedores de ser vicios de revisión de referencias. B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting; Cómputo en la nube, call Center, servicios de atención a cliente (SMS, Mail, redes sociales).
5. Bloqueo: 15 días después de terminado el plazo de conservación de 10 años
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado cuando el trataamiento sea necesario para dar cumplimiento a la relación jurídica con el titular o este previsto en una Ley.

1.2.6. Open banking

En el presente apartado se identificó el tratamiento de Open Banking previsto en el articulo 76 de la LRITF, en el cual se identifico que de forma directa se obtienen datos personales de identificación y autenticación, contacto, demográficos, ubicación geográfica, características de dispositivos electrónicos, patrimoniales y/o financieros, crediticios y laborales. Asimismo, se identificó el siguiente ciclo de vida:

1) **Obtención**:
    - Directa e Indirecta
    - Previa o durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
    - Sistema tecnológico.
    - Interfaces de Programación de aplicaciones informáticas.
3) **Usos:**
    - Evaluación cuantitativa y cualitativa de solvencia.
    - Verificar historial crediticio.
    - Validar capacidad de pago.
    - Revisión de ingresos y su relación con otros crédito y pasivos.
    - Cumplimiento regulatorio.
4) **Divulgación/otros sujetos intervinientes:**
    - Transferencias: Entidades Financieras contempladas en el artículo 76 de la LRITF: es necesario el consentimiento expreso.
    - Remisiones:
        - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
        - Hosting.
        - Cómputo en la nube.
        - Call Center.
        - Servicios de atención al cliente.
        - Proveedores terceros especializados en tecnologías de la información.
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

El ciclo de vida de este proceso se resume en el siguiente diagrama:


Datos recabados (categorías)
Identificación y autenticación, contacto, demográficos, ubicación geográfica, características de dispositivo electrónicos,Patrimoniales y/ financieros, créditos, laborales y biométricos.
Ciclo de vida
1. Obtención: Directa e indirecta. Previa o durante el establecimiento de la relación jurídica con el cliente.
2- Almacenamiento: Sistema tecnológico. Expediente físico y/o digitalizado.
3- Usos: Evaluación cuantitativa y cualitativa de solvencia, verificar historial crediticio, validar capacidad de pago, revisión de ingresos y su relación con otros créditos y pasivos y cumplimiento regulatorio.
4. Divulgación: A. Transferencias. Entidades financieras contempladas en el artículo 76 de la LRITF. B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting, Cómputo en la nube, Call Center, servicio a atención al cliente y proveedores terceros especializados en tecnologías de la información).
5. Bloqueo: 15 días después de terminado el plazo de conservación de 10 años.
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
-Expreso por tratarse de datos patrimoniales y financieros, además de que así lo establece la LRITF.
-Expreso y por escrito o mediante tecnología de autenticación equivalente para datos sensibles.

2. Tratamientos de datos personales en las IFPE

A continuación, se presentan los tratamientos de datos en las IFPE reguladas por la LRITF. Los tratamientos se describen a partir de los procesos generales identificados en el entregable 1: Alta del cliente, PLD/CFT, obligación de conservar documentos, mecanismos de seguimiento y agrupaciones de operaciones, operaciones que realizan las IFPE, características de las operaciones, cierre de cuentas, requerimientos de información de BANXICO y *open banking*.

2.1. Alta de cliente

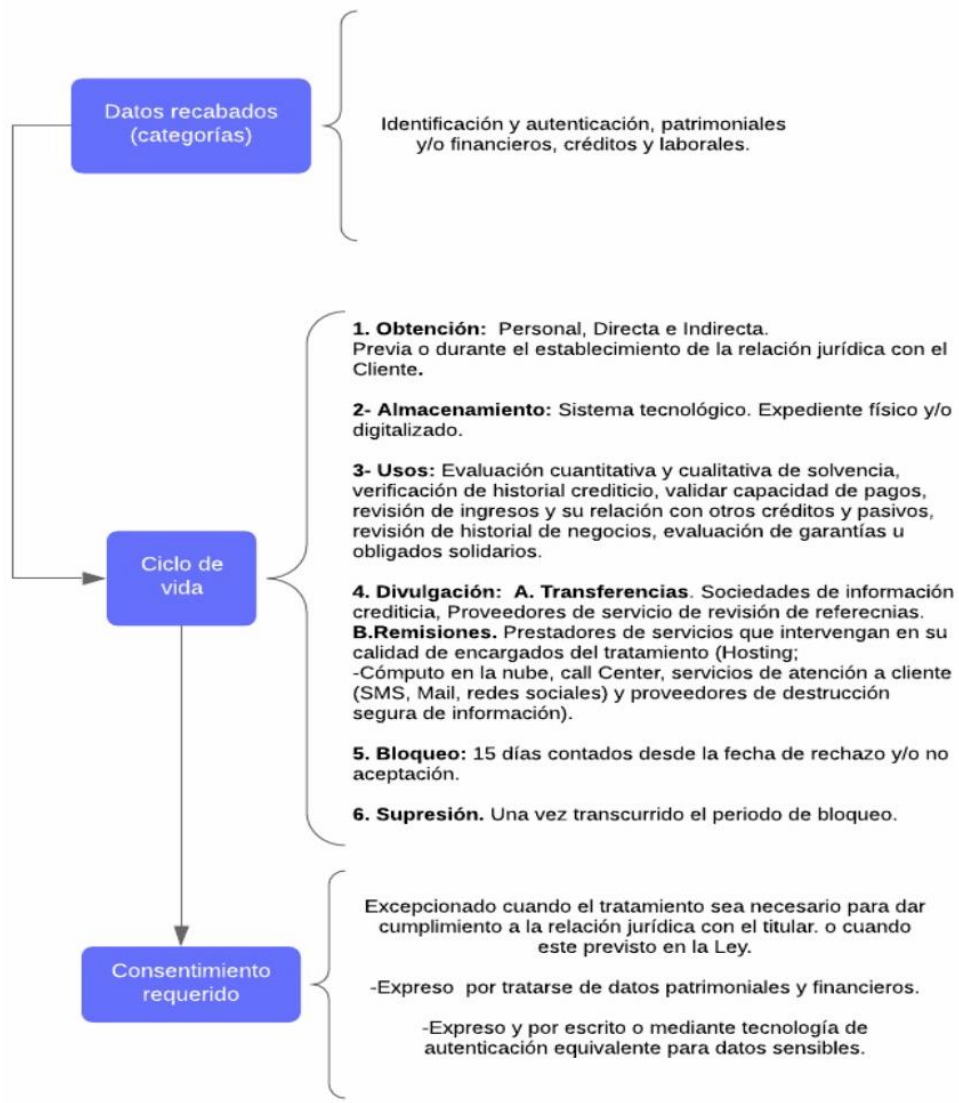
Como se señaló de forma previa, las IFPE tienen la obligación de identificar a su cliente al momento de iniciar una relación jurídica a través de un contrato y tener registro de un expediente por cliente, el cual será conformado en función del tipo de persona. Para el alta de cliente se identificó el subproceso de identificación de los datos personales provenientes de documento válido, el cual deberá digitalizarse[100]. El cual obtiene datos personales de identificación y autenticación, patrimoniales y financieros, crediticios y laborales.

Se identificó el siguiente ciclo de vida de los datos personales en el proceso de alta de cliente:

1) **Obtención:**
   - Personal, directa e indirecta.
   - Previa o durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
   - Sistema tecnológico.
   - Expediente físico y/o digitalizado.
3) **Usos:**
   - Evaluación cuantitativa y cualitativa de solvencia.
   - Verificar historial crediticio.
   - Validar capacidad de pagos.
   - Revisión de ingresos y su relación con otros créditos y pasivos
   - Revisión de Historial de negocios
   - Evaluación de garantes u obligados solidarios.
4) **Divulgación/otros sujetos intervinientes:**
   - ***Transferencias:***
     - Sociedades de información crediticia: se exceptúa el consentimiento por estar establecido en una disposición legal.
     - Proveedores de servicio de revisión de referencias.
   - ***Remisiones:***
     - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
     - Hosting.
     - Cómputo en la nube.
     - Call Center.
     - Servicios de atención a cliente.
     - Proveedores de destrucción segura de información.
5) **Bloqueo**: 15 días contados desde la fecha de rechazo y/o no aceptación.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

El ciclo de vida en el proceso de alta de cliente se resume en el siguiente diagrama:

[100] Para Propietarios Reales, Proveedores de Recursos y terceros autorizados, les aplicará lo dispuesto por el artículo 11 de las DCGA58, según el caso.


Datos recabados (categorías)
Identificación y autenticación, patrimoniales y/o financieros, créditos y laborales.
Ciclo de vida
1. Obtención: Personal, Directa e Indirecta. Previa o durante el establecimiento de la relación jurídica con el Cliente.
2- Almacenamiento: Sistema tecnológico. Expediente físico y/o digitalizado.
3- Usos: Evaluación cuantitativa y cualitativa de solvencia, verificación de historial crediticio, validar capacidad de pagos, revisión de ingresos y su relación con otros créditos y pasivos, revisión de historial de negocios, evaluación de garantías u obligados solidarios.
4. Divulgación: A. Transferencias. Sociedades de información crediticia, Proveedores de servicio de revisión de referecnias. B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting; -Cómputo en la nube, call Center, servicios de atención a cliente (SMS, Mail, redes sociales) y proveedores de destrucción segura de información).
5. Bloqueo: 15 días contados desde la fecha de rechazo y/o no aceptación.
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado cuando el tratamiento sea necesario para dar cumplimiento a la relación jurídica con el titular. o cuando este previsto en la Ley.
-Expreso por tratarse de datos patrimoniales y financieros.
-Expreso y por escrito o mediante tecnología de autenticación equivalente para datos sensibles.

2.2. PLD/CFT

Derivado del análisis de las operaciones de las IFPE en cumplimiento a la normatividad señalada se identificaron los siguientes subprocesos en materia de PLD/CFT: 1) reportes que se deberán remitir a la SHCP; 2) intercambio de información; 3) clasificación de clientes por grado de riesgo: bajo, medio o alto; y 4) políticas de conocimiento de clientes; 5) listado de personas bloqueadas y 6) práctica de auditorías.

2.2.1. Reportes que se deberán remitir a la SHCP

En este subproceso se identificó que se utilizan datos de identificación y autenticación, patrimoniales y/o financieros y transaccionales para poder realizar los siguientes reportes: de operaciones relevantes, de operaciones en efectivo en moneda extranjera, de transferencias internacionales, de operaciones inusuales, de operaciones con activos virtuales y de operaciones internas preocupantes. asimismo, se identificó el siguiente ciclo de vida de los datos personales:

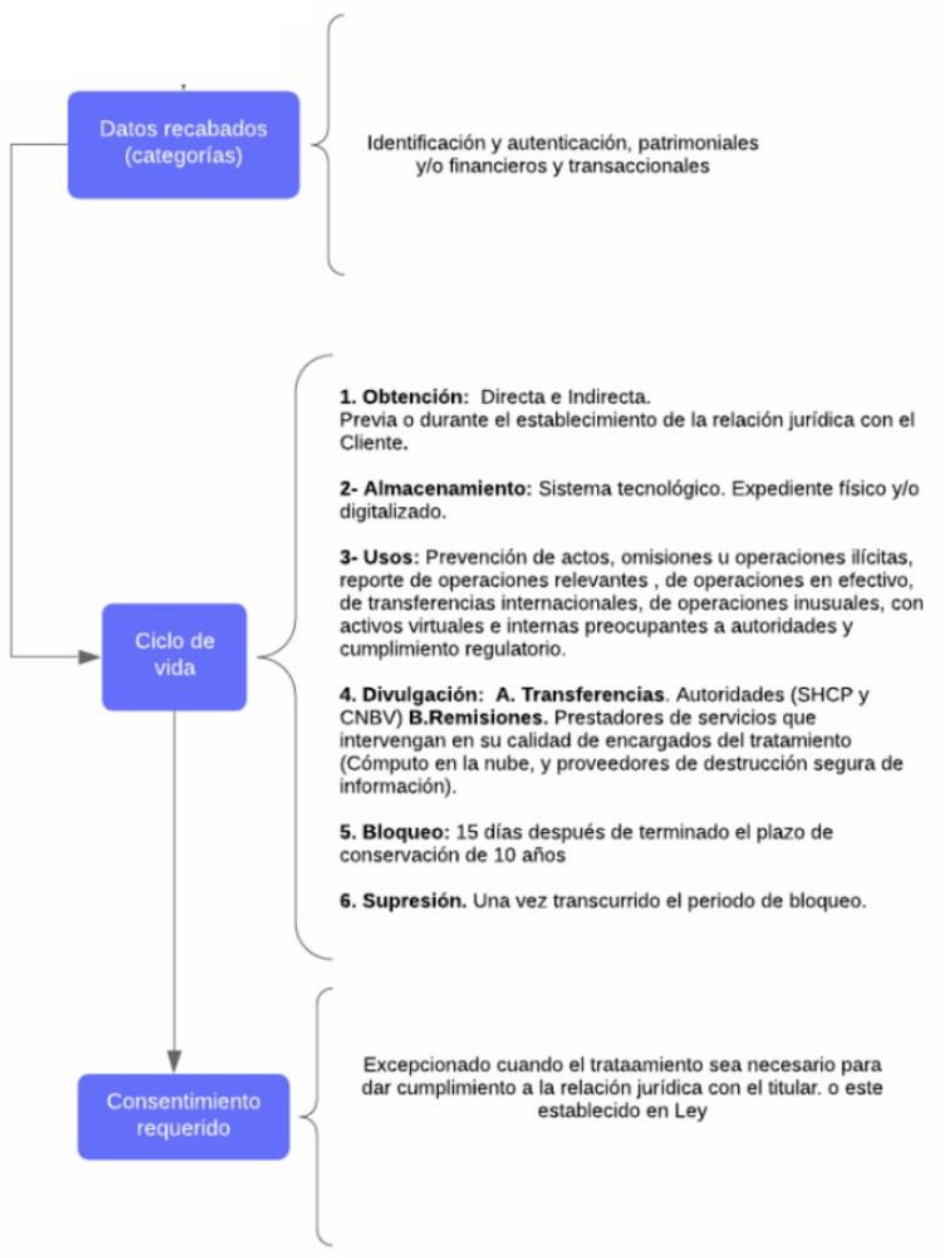
Se identificó el siguiente ciclo de vida de los datos personales en el subproceso de emisión de reportes a la SHCP:

1) **Obtención:**
   - Personal, directa e indirecta.
   - Previa o durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
   - Sistema tecnológico.
   - Expediente físico y/o digitalizado.
3) **Usos:**
   - Prevención de actos, omisiones u operaciones ilícitas.
   - Reporte de operaciones relevantes, de operaciones en efectivo, de transferencias internacionales, de operaciones inusuales, con activos virtuales e internas preocupantes a autoridades.
   - Cumplimiento regulatorio,

4) **Divulgación/otros sujetos intervinientes:**
   - Transferencias;
     - SHCP.
     - CNBV.
   - Remisiones:
     - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
     - Cómputo en la nube.
     - Proveedores de destrucción segura de información.
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años[101].
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

El ciclo de vida en el subproceso de emisión de reportes a la SHCP se resume en el siguiente diagrama:

[101] Artículo 25 de las Disposiciones de Carácter General a que se refiere el artículo 58 de la LRITF, fracción IV.


Datos recabados (categorías)
Identificación y autenticación, patrimoniales y/o financieros y transaccionales
Ciclo de vida
1. Obtención: Directa e Indirecta. Previa o durante el establecimiento de la relación jurídica con el Cliente.
2- Almacenamiento: Sistema tecnológico. Expediente físico y/o digitalizado.
3- Usos: Prevención de actos, omisiones u operaciones ilícitas, reporte de operaciones relevantes , de operaciones en efectivo, de transferencias internacionales, de operaciones inusuales, con activos virtuales e internas preocupantes a autoridades y cumplimiento regulatorio.
4. Divulgación: A. Transferencias. Autoridades (SHCP y CNBV) B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Cómputo en la nube, y proveedores de destrucción segura de información).
5. Bloqueo: 15 días después de terminado el plazo de conservación de 10 años
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado cuando el trataamiento sea necesario para dar cumplimiento a la relación jurídica con el titular. o este establecido en Ley

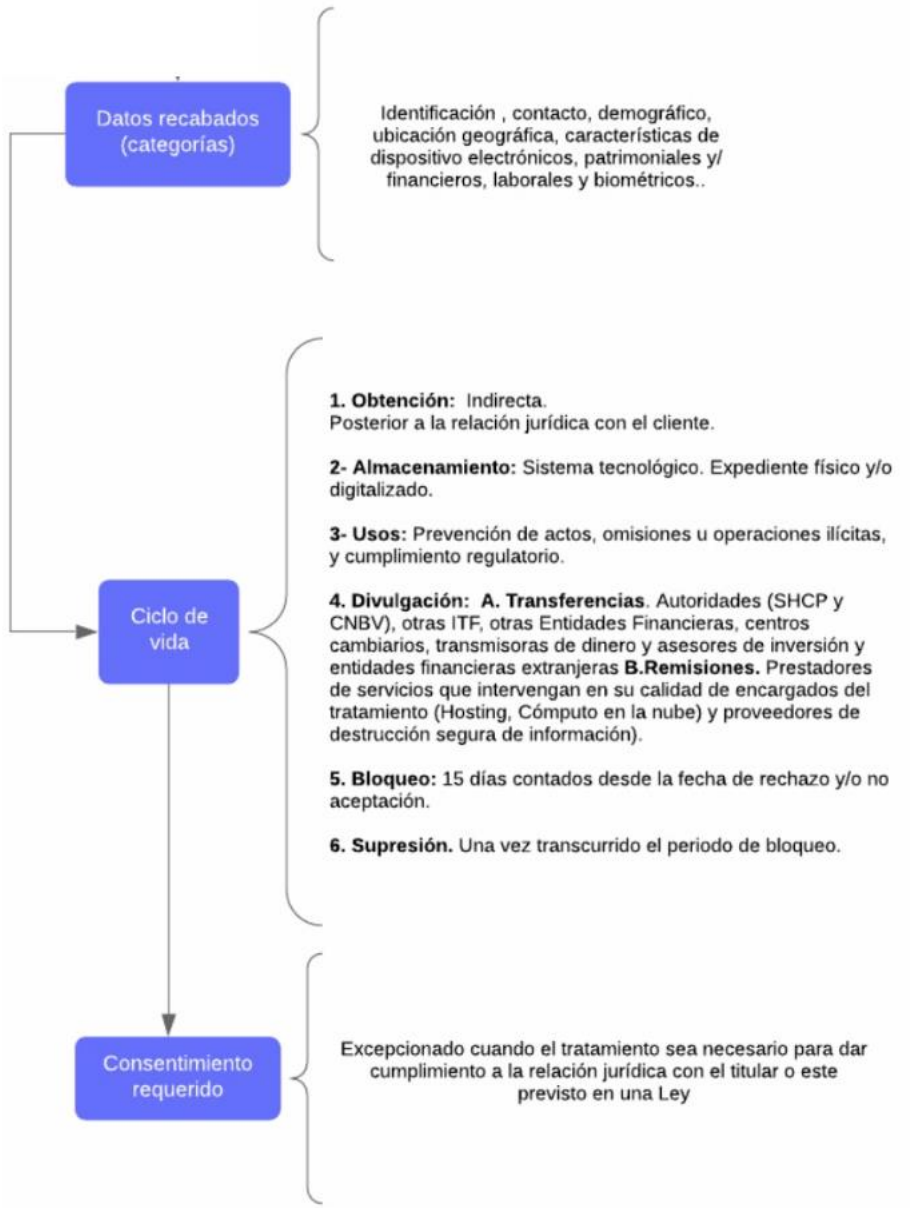
2.2.2. Intercambio de información

En este subproceso se identificó que se obtienen datos personales de identificación, contacto, demográficos, ubicación geográfica, características de dispositivos electrónicos, patrimoniales y/o financieros, laborales y biométricos. Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención**:
    - Indirecta.
    - Posterior al establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento**:
    - Sistema tecnológico.
    - Expediente físico y/o digitalizado.
3) **Usos**:
    - Prevención de actos, omisiones u operaciones ilícitas.
    - Cumplimiento regulatorio.

4) **Divulgación/otros sujetos intervinientes:**
    - ***Transferencias:***
        - CNBV
        - SHCP
        - Otras ITF
        - Otras Entidades Financieras, centros cambiarios, transmisores de dinero y asesores de inversión.
        - Entidades Financieras Extranjeras
    - ***Remisiones***:
        - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
        - Hosting
        - Cómputo en la nube.
        - Proveedores de destrucción segura de información.
5) **Bloqueo**: 15 días contados desde la fecha de rechazo y/o no aceptación.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

El ciclo de vida de este subproceso se resume en el siguiente diagrama:

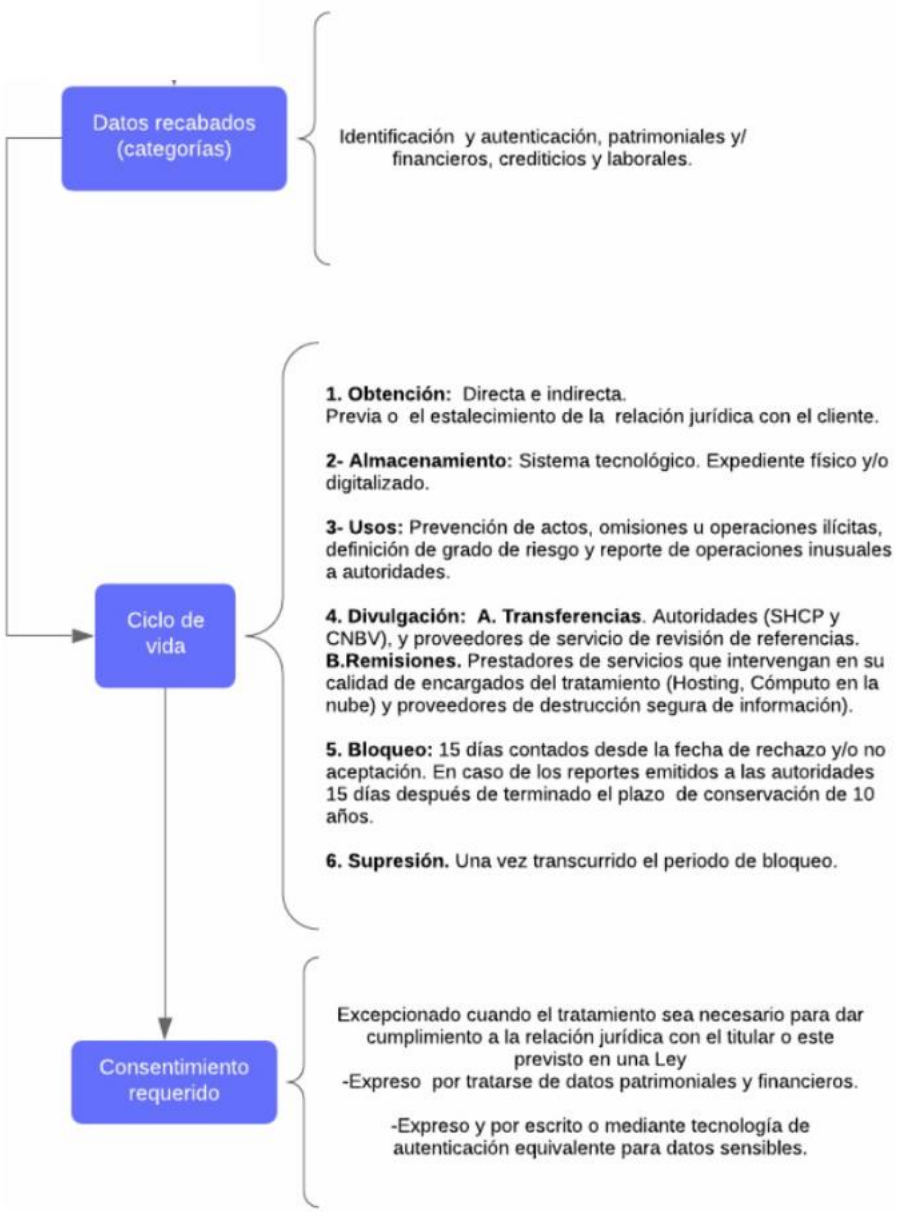

Datos recabados (categorías)
Identificación , contacto, demográfico, ubicación geográfica, características de dispositivo electrónicos, patrimoniales y/ financieros, laborales y biométricos..
Ciclo de vida
1. Obtención: Indirecta.
Posterior a la relación jurídica con el cliente.
2- Almacenamiento: Sistema tecnológico. Expediente físico y/o digitalizado.
3- Usos: Prevención de actos, omisiones u operaciones ilícitas, y cumplimiento regulatorio.
4. Divulgación: A. Transferencias. Autoridades (SHCP y CNBV), otras ITF, otras Entidades Financieras, centros cambiarios, transmisoras de dinero y asesores de inversión y entidades financieras extranjeras B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting, Cómputo en la nube) y proveedores de destrucción segura de información).
5. Bloqueo: 15 días contados desde la fecha de rechazo y/o no aceptación.
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado cuando el tratamiento sea necesario para dar cumplimiento a la relación jurídica con el titular o este previsto en una Ley

2.2.3. Clasificación de Clientes por Grado de Riesgo: bajo, medio o alto

En este subproceso se identificó que se obtienen datos personales de identificación y autenticación, patrimoniales y/o financieros, crediticios y laborales. Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención:**
   - Directa e indirecta.
   - Previa o durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
   - Sistema tecnológico.
   - Expediente físico y/o digitalizado.
3) **Usos:**
   - Prevención de actos, omisiones u operaciones ilícitas.
   - Definición del Grado de Riesgo.
   - Reporte de operaciones inusuales a autoridades.
4) **Divulgación/otros sujetos intervinientes:**
   - Transferencias:
     - SHCP.
     - CNBV.
     - Proveedor de servicio de revisión de referencias.
   - Remisiones:
     - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
     - Hosting.
     - Cómputo en la nube.
     - Proveedores de destrucción segura de información.
5) **Bloqueo**:
   - 15 días contados desde la fecha de rechazo y/o no aceptación.
   - En caso de los reportes emitidos a las autoridades: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión:** una vez transcurrido el periodo de bloqueo.

El ciclo de vida de este subproceso se resume en el siguiente diagrama:

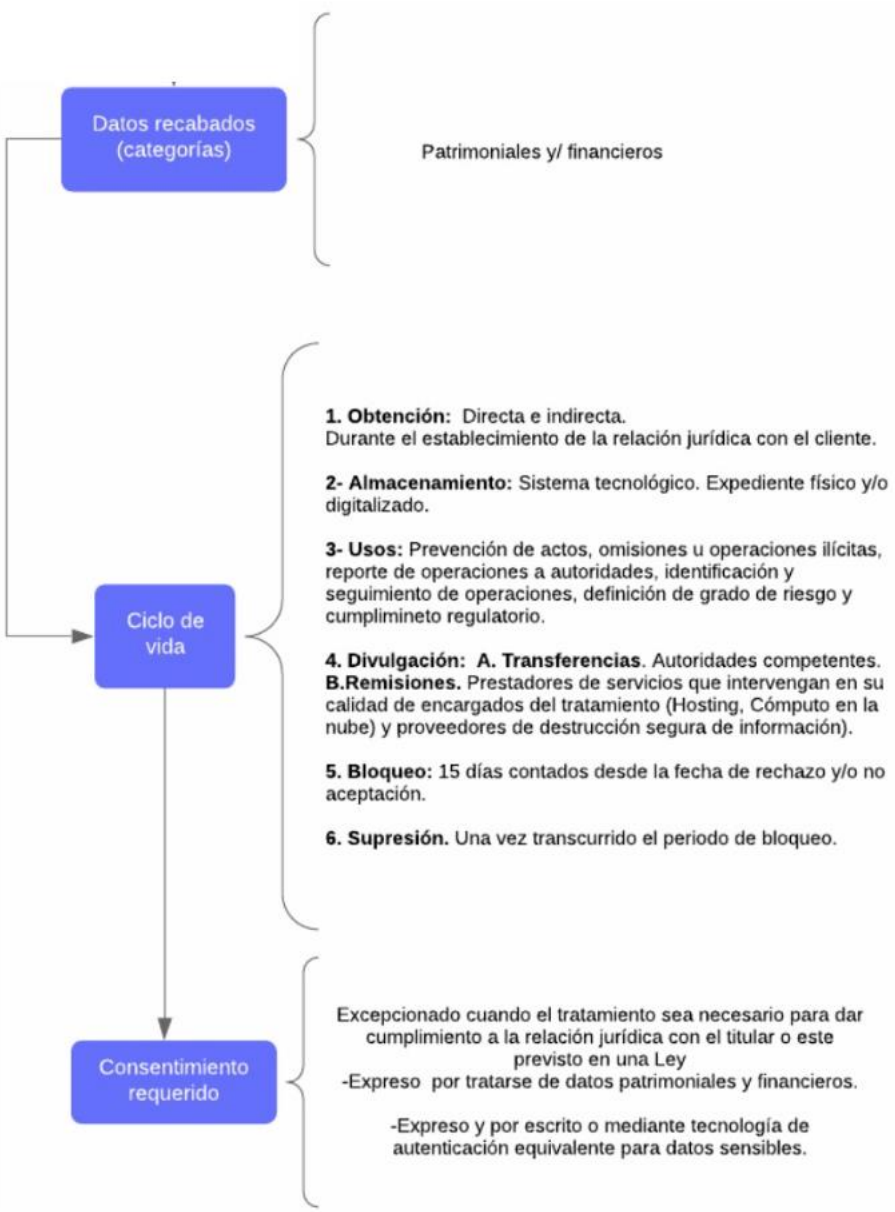

Datos recabados (categorías)
Identificación y autenticación, patrimoniales y/ financieros, crediticios y laborales.
Ciclo de vida
1. Obtención: Directa e indirecta.
Previa o el estalecimiento de la relación jurídica con el cliente.
2- Almacenamiento: Sistema tecnológico. Expediente físico y/o digitalizado.
3- Usos: Prevención de actos, omisiones u operaciones ilícitas, definición de grado de riesgo y reporte de operaciones inusuales a autoridades.
4. Divulgación: A. Transferencias. Autoridades (SHCP y CNBV), y proveedores de servicio de revisión de referencias.
B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting, Cómputo en la nube) y proveedores de destrucción segura de información).
5. Bloqueo: 15 días contados desde la fecha de rechazo y/o no aceptación. En caso de los reportes emitidos a las autoridades 15 días después de terminado el plazo de conservación de 10 años.
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado cuando el tratamiento sea necesario para dar cumplimiento a la relación jurídica con el titular o este previsto en una Ley
-Expreso por tratarse de datos patrimoniales y financieros.
-Expreso y por escrito o mediante tecnología de autenticación equivalente para datos sensibles.

2.2.4. Políticas de conocimiento de clientes

En este subproceso se identificó que se obtienen datos personales patrimoniales y/o financieros. Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención**:
    - Directa e indirecta.
    - Durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
    - Sistema tecnológico.
    - Expediente físico y/o digitalizado.
3) **Usos**:
    - Prevención de actos, omisiones u operaciones ilícitas.
    - Reporte de operaciones a autoridades.
    - Identificación y seguimiento de Operaciones.
    - Definición de Grado de Riesgo.
    - Cumplimiento Regulatorio.
4) **Divulgación/otros sujetos intervinientes:**
    - Transferencias:
        - Autoridades competentes.
    - Remisiones:
        - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
        - Hosting.
        - Cómputo en la nube.
        - Proveedores de destrucción segura de información.
5) **Bloqueo**: 15 días contados desde la fecha de rechazo y/o no aceptación.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

El ciclo de vida de este subproceso se resume en el siguiente diagrama:

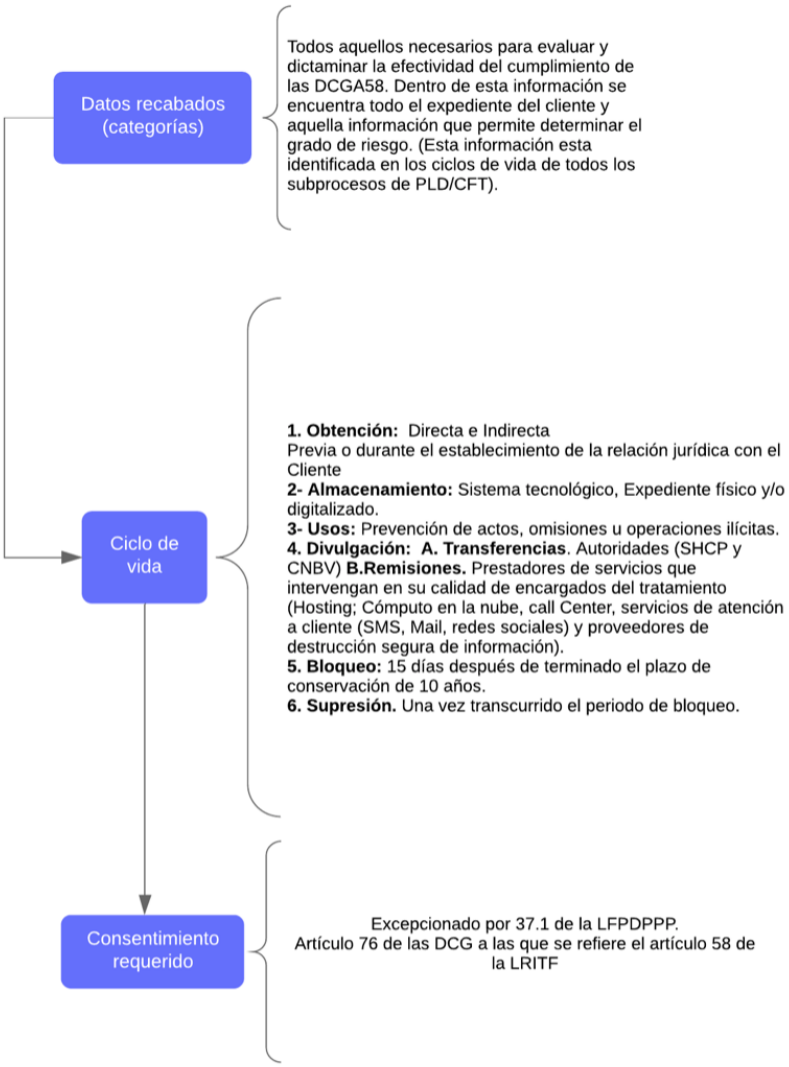

Datos recabados (categorías)
Patrimoniales y/ financieros
Ciclo de vida
1. Obtención: Directa e indirecta.
Durante el establecimiento de la relación jurídica con el cliente.
2- Almacenamiento: Sistema tecnológico. Expediente físico y/o digitalizado.
3- Usos: Prevención de actos, omisiones u operaciones ilícitas, reporte de operaciones a autoridades, identificación y seguimiento de operaciones, definición de grado de riesgo y cumplimineto regulatorio.
4. Divulgación: A. Transferencias. Autoridades competentes.
B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting, Cómputo en la nube) y proveedores de destrucción segura de información).
5. Bloqueo: 15 días contados desde la fecha de rechazo y/o no aceptación.
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado cuando el tratamiento sea necesario para dar cumplimiento a la relación jurídica con el titular o este previsto en una Ley
-Expreso por tratarse de datos patrimoniales y financieros.
-Expreso y por escrito o mediante tecnología de autenticación equivalente para datos sensibles.

2.2.5. Auditoría para revisar el cumplimiento de las DCGA58

En este subproceso se identificó que se obtienen todos aquellos datos necesarios para evaluar y dictaminar la efectividad del cumplimiento de las DCGA58. Dentro de esta información se encuentra todo el expediente del cliente y aquella información que permite determinar el grado de riesgo. (Esta información esta identificada en los ciclos de vida de todos los subprocesos de PLD/CFT).
Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención**:
    - Directa e indirecta.
    - Previa o durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
    - Sistema tecnológico.
    - Expediente físico y/o digitalizado.
3) **Usos:**
    - Prevención de actos, omisiones u operaciones ilícitas.
4) **Divulgación/otros sujetos intervinientes:**
    - Transferencias:
        - Autoridades competentes (SHCP y CNBV),
    - Remisiones:
        - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
        - Hosting.
        - Cómputo en la nube.
        - Call center.
        - Servicios de atención al cliente.
        - Proveedores de destrucción segura de información.
5) **Bloqueo:** 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión:** una vez transcurrido el periodo de bloqueo.

El ciclo de vida de este subproceso se resume en el siguiente diagrama:

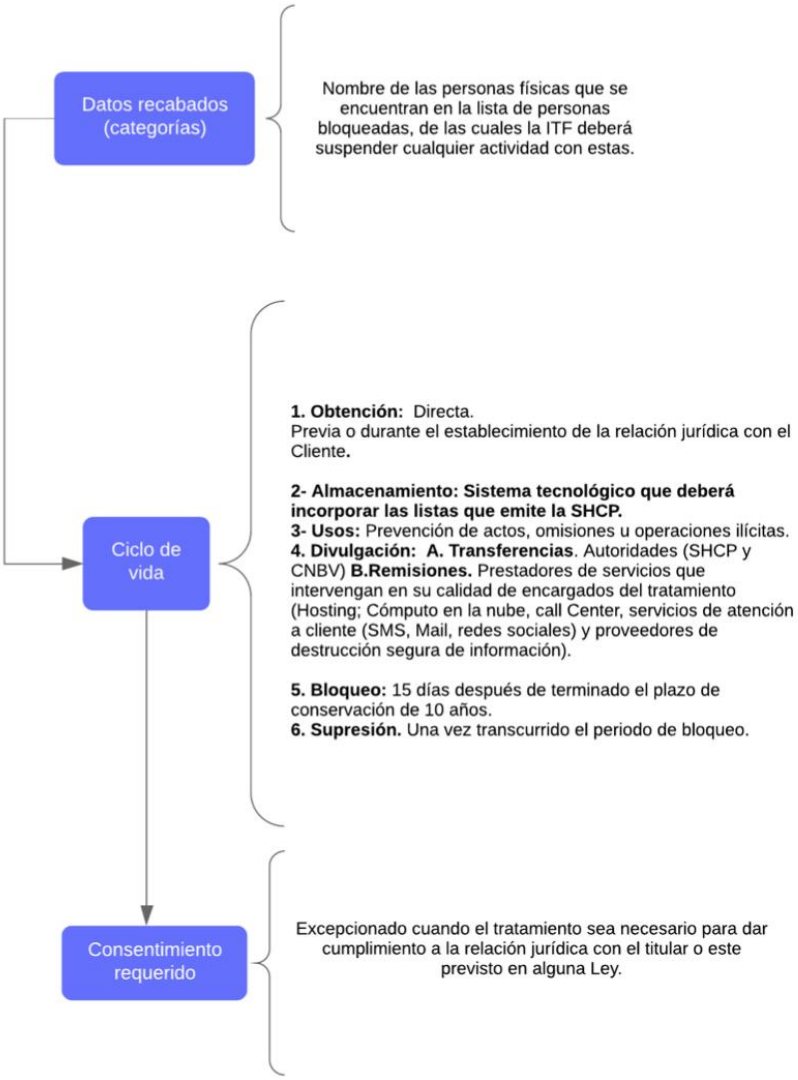

Datos recabados (categorías)
Todos aquellos necesarios para evaluar y dictaminar la efectividad del cumplimiento de las DCGA58. Dentro de esta información se encuentra todo el expediente del cliente y aquella información que permite determinar el grado de riesgo. (Esta información esta identificada en los ciclos de vida de todos los subprocesos de PLD/CFT).
Ciclo de vida
1. Obtención: Directa e Indirecta
Previa o durante el establecimiento de la relación jurídica con el Cliente
2- Almacenamiento: Sistema tecnológico, Expediente físico y/o digitalizado.
3- Usos: Prevención de actos, omisiones u operaciones ilícitas.
4. Divulgación: A. Transferencias. Autoridades (SHCP y CNBV) B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting; Cómputo en la nube, call Center, servicios de atención a cliente (SMS, Mail, redes sociales) y proveedores de destrucción segura de información).
5. Bloqueo: 15 días después de terminado el plazo de conservación de 10 años.
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado por 37.1 de la LFPDPPP.
Artículo 76 de las DCG a las que se refiere el artículo 58 de la LRITF

2.2.6. Obligaciones de las ITF respecto a la lista de personas bloqueadas

En este subproceso se identificó que se obtiene como dato personal el nombre de las personas físicas que se encuentran en la lista de personas bloqueadas que publica la SHCP, de las cuales la ITF deberá suspender cualquier actividad con estas.
Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención**:
    - Directa.
    - Previa o durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
    - Sistema tecnológico que deberá incorporar las listas de personas bloqueadas que emite la SHCP.
3) **Usos:**
    - Prevención de actos, omisiones u operaciones ilícitas.
4) **Divulgación/otros sujetos intervinientes:**
    - Transferencias:
        - Autoridades competentes (SHCP y CNBV),
    - Remisiones:
        - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
        - Hosting.
        - Cómputo en la nube.
        - Call Center.
        - Servicios de atención a cliente.
        - Proveedores de destrucción segura de información.
5) **Bloqueo:** 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión:** una vez transcurrido el periodo de bloqueo.

El ciclo de vida de este subproceso se resume en el siguiente diagrama:

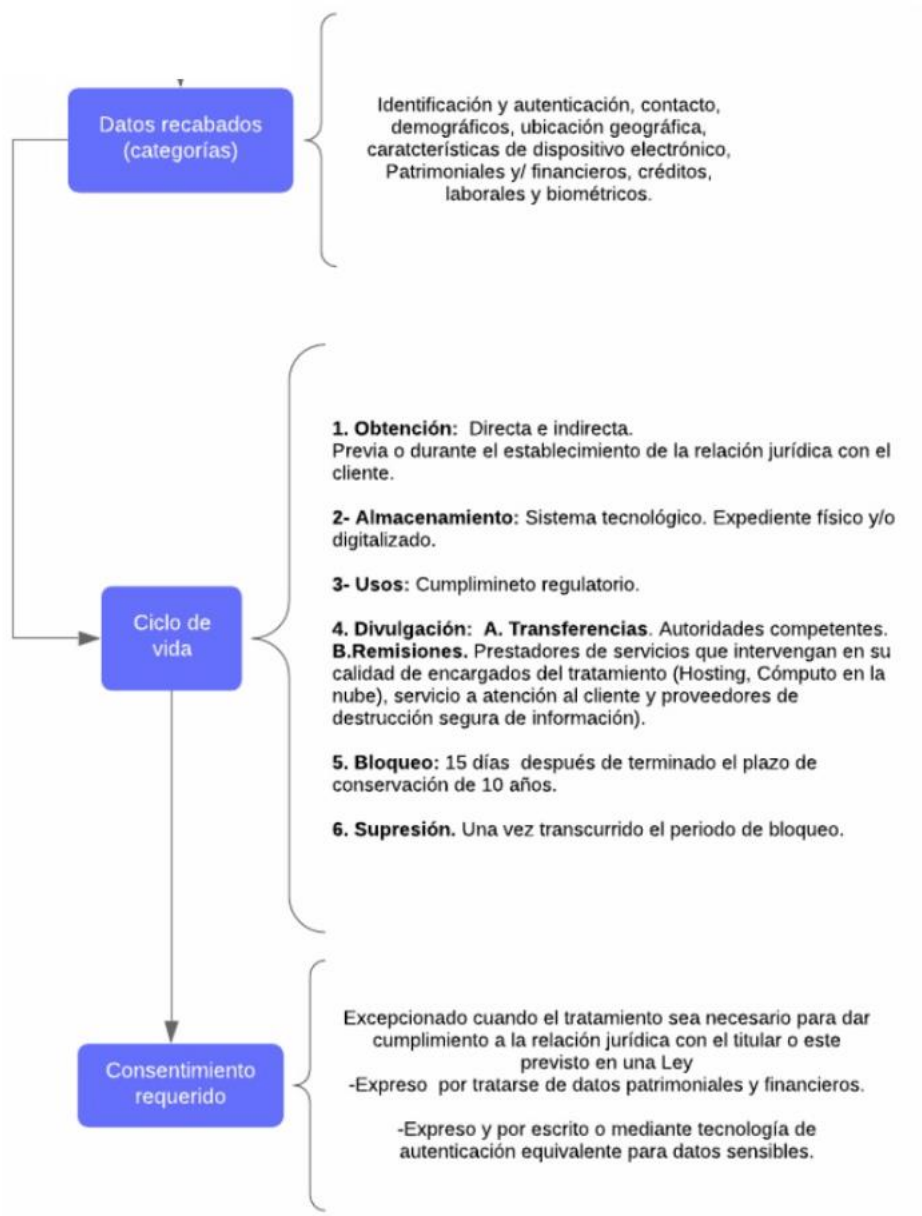

Datos recabados (categorías)
Nombre de las personas físicas que se encuentran en la lista de personas bloqueadas, de las cuales la ITF deberá suspender cualquier actividad con estas.
Ciclo de vida
1. Obtención: Directa.
Previa o durante el establecimiento de la relación jurídica con el Cliente.
2- Almacenamiento: Sistema tecnológico que deberá incorporar las listas que emite la SHCP.
3- Usos: Prevención de actos, omisiones u operaciones ilícitas.
4. Divulgación: A. Transferencias. Autoridades (SHCP y CNBV) B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting; Cómputo en la nube, call Center, servicios de atención a cliente (SMS, Mail, redes sociales) y proveedores de destrucción segura de información).
5. Bloqueo: 15 días después de terminado el plazo de conservación de 10 años.
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado cuando el tratamiento sea necesario para dar cumplimiento a la relación jurídica con el titular o este previsto en alguna Ley.

2.3. Obligación de conservar documentos

Las IFPE tienen la obligación de conservar la información y documentación sobre las operaciones que celebre; así como, la información y documentación de la identificación de sus clientes. Derivado de lo anterior, se observó que se obtienen datos personales de identificación y autenticación, contacto, demográficos, ubicación geográfica, características de dispositivo electrónico, patrimoniales y/o financieros, crediticios, laborales y biométricos. Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención:**
    - Directa e indirecta.
    - Durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
    - Sistema tecnológico.
    - Expediente físico y/o digitalizado.
3) **Usos**:
    - Cumplimiento Regulatorio.
4) **Divulgación/otros sujetos intervinientes:**
    - Transferencias:
        - Autoridades competentes.
    - Remisiones:
        - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
        - Hosting.
        - Cómputo en la nube.
        - Servicio de atención a cliente.
        - Proveedores de destrucción segura de información.
5) **Bloqueo:** 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión:** una vez transcurrido el periodo de bloqueo.

El ciclo de vida de este subproceso se resume en el siguiente diagrama:


Datos recabados (categorías)
Identificación y autenticación, contacto, demográficos, ubicación geográfica, caratcterísticas de dispositivo electrónico, Patrimoniales y/ financieros, créditos, laborales y biométricos.
Ciclo de vida
1. Obtención: Directa e indirecta. Previa o durante el establecimiento de la relación jurídica con el cliente.
2- Almacenamiento: Sistema tecnológico. Expediente físico y/o digitalizado.
3- Usos: Cumplimineto regulatorio.
4. Divulgación: A. Transferencias. Autoridades competentes. B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting, Cómputo en la nube), servicio a atención al cliente y proveedores de destrucción segura de información).
5. Bloqueo: 15 días después de terminado el plazo de conservación de 10 años.
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado cuando el tratamiento sea necesario para dar cumplimiento a la relación jurídica con el titular o este previsto en una Ley
-Expreso por tratarse de datos patrimoniales y financieros.
-Expreso y por escrito o mediante tecnología de autenticación equivalente para datos sensibles.

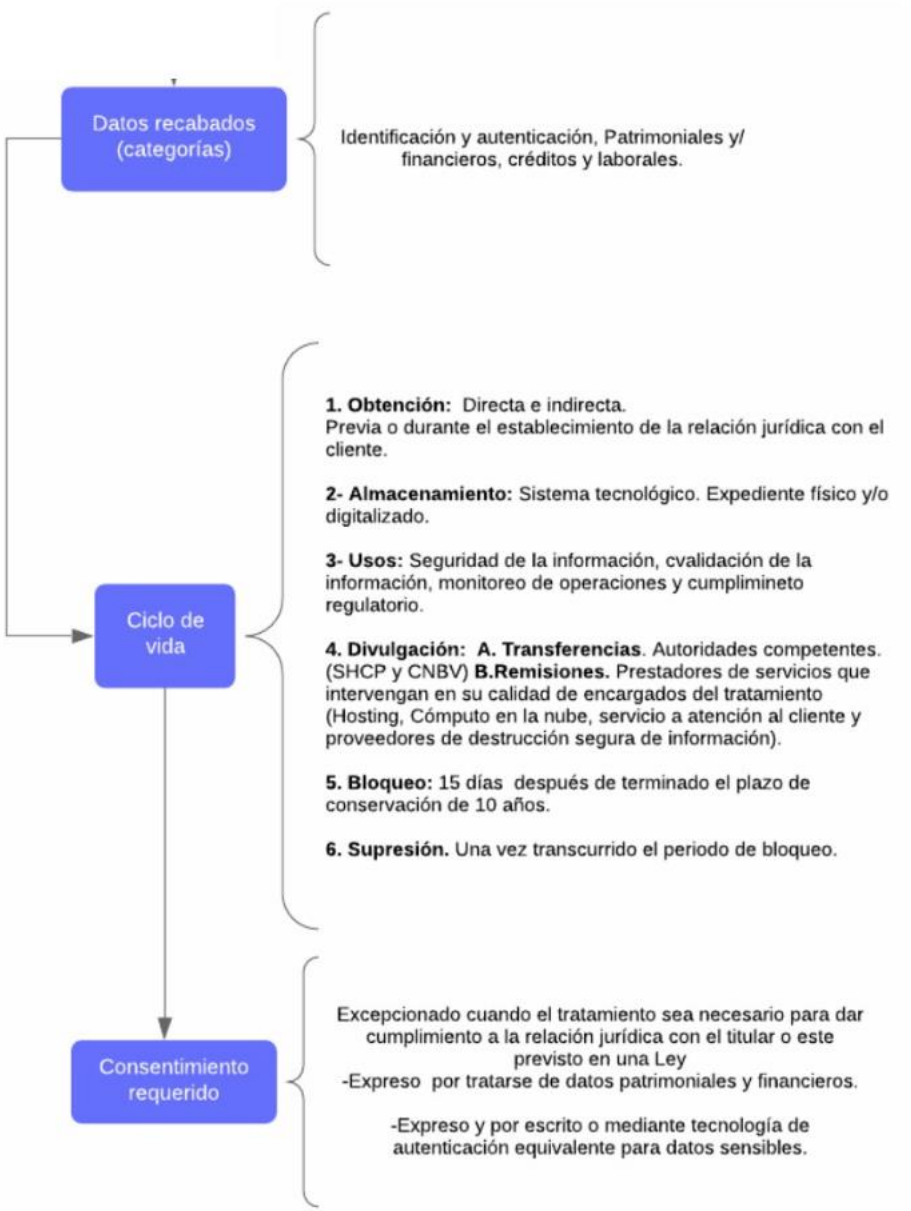
2.4. Mecanismos de seguimiento y agrupaciones de operaciones

En este proceso se identificó el tratamiento de datos personales de identificación y autenticación, patrimoniales y/o financieros, crediticios y laborales) Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención:**
   - Directa e indirecta.
   - Previa o durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
   - Sistema tecnológico.
   - Expediente físico y/o digitalizado.
3) **Usos**:
   - Seguridad de la información.
   - Validación de la información.
   - Monitoreo de operaciones.
   - Cumplimiento regulatorio.
4) **Divulgación/otros sujetos intervinientes:**
   - Transferencias[102]:
     - CNBV.
     - SHCP.
   - Remisiones:
     - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
     - Hosting.
     - Cómputo en la nube.
     - Servicio de atención a cliente.
     - Proveedores de destrucción segura de información.
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

El ciclo de vida de este subproceso se resume en el siguiente diagrama:

[102] Se exceptúa el consentimiento por 37.1 de la LFPDPPP y artículo 73 de la LRITF.


Datos recabados (categorías)
Identificación y autenticación, Patrimoniales y/ financieros, créditos y laborales.
Ciclo de vida
1. Obtención: Directa e indirecta. Previa o durante el establecimiento de la relación jurídica con el cliente.
2- Almacenamiento: Sistema tecnológico. Expediente físico y/o digitalizado.
3- Usos: Seguridad de la información, cvalidación de la información, monitoreo de operaciones y cumplimineto regulatorio.
4. Divulgación: A. Transferencias. Autoridades competentes. (SHCP y CNBV) B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting, Cómputo en la nube, servicio a atención al cliente y proveedores de destrucción segura de información).
5. Bloqueo: 15 días después de terminado el plazo de conservación de 10 años.
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado cuando el tratamiento sea necesario para dar cumplimiento a la relación jurídica con el titular o este previsto en una Ley
-Expreso por tratarse de datos patrimoniales y financieros.
-Expreso y por escrito o mediante tecnología de autenticación equivalente para datos sensibles.

2.5. Operaciones que realizan las IFPE

La Circular 12/2018 emitida por BANXICO establece las disposiciones de carácter general aplicables a las operaciones de las IFPE. Derivado del análisis a dicha circular se han identificado los siguientes subprocesos y tratamientos de datos personales:

2.5.1. Operaciones con moneda nacional

Respecto a las operaciones nacionales se identificaron las siguientes:

1. Niveles de cuentas.

Se identificó que se obtienen datos personales de identificación y autenticación, patrimoniales y/o financieros, crediticios y laborales. Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención:**
   - Directa e indirecta.
   - Previa o durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
   - Sistema tecnológico.
   - Expediente físico y/o digitalizado.
3) **Usos**:
   - Clasificar a los clientes conforme a su perfil transaccional.
   - Limitar las operaciones permitidas de los Clientes.
4) **Divulgación/otros sujetos intervinientes:**
   - Transferencias[103]:
     - Proveedores de servicios de revisión de monitoreo de transacciones.
     - Proveedor de servicio de transferencias.
   - Remisiones:
     - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
     - Hosting.
     - Cómputo en la nube.
     - Call Center.
     - Servicios de atención al cliente.
     - Proveedores de destrucción segura de información.
5) **Bloqueo**: 15 días contados desde la fecha de rechazo y/o no aceptación.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

2. Emisión de fondos de pago electrónico y abonos de recursos.

Se identificó que se obtienen datos personales de identificación y autenticación, patrimoniales y/o financieros y transaccionales. Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

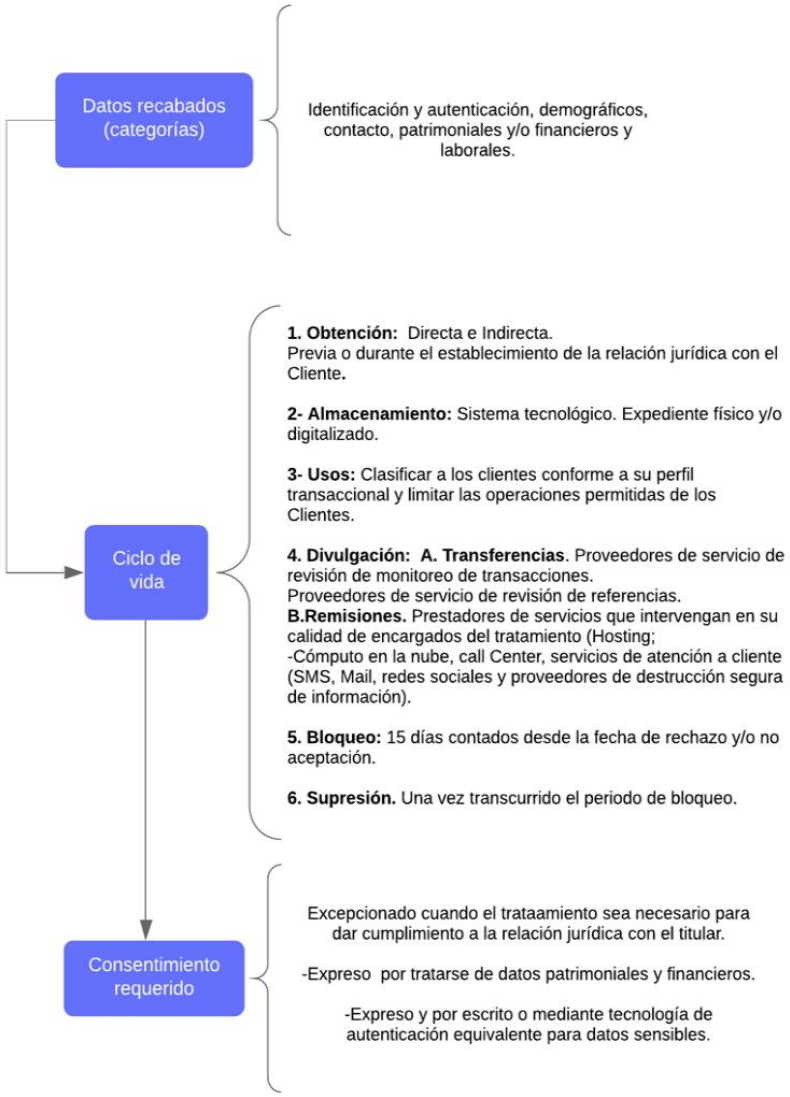
1) **Obtención:**
   - Directa e indirecta.
   - Previa o durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
   - Sistema tecnológico.

[103] Se exceptúa el consentimiento por 37.1 de la LFPDPPP.

- Expediente físico y/o digitalizado.

3) **Usos**:
   - Cumplimiento regulatorio.
   - Cumplimiento de las obligaciones derivadas del contrato de servicios.
4) **Divulgación/otros sujetos intervinientes:**
   - Transferencias:
     - SHCP.
     - CNBV.
   - Remisiones:
     - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
     - Hosting.
     - Cómputo en la nube.
     - Call Center.
     - Servicios de atención al cliente.
     - Proveedores de destrucción segura de información.
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

El ciclo de vida de este proceso se resume en el siguiente diagrama:


Datos recabados (categorías)
Identificación y autenticación, demográficos, contacto, patrimoniales y/o financieros y laborales.
Ciclo de vida
1. Obtención: Directa e Indirecta.
Previa o durante el establecimiento de la relación jurídica con el Cliente.
2- Almacenamiento: Sistema tecnológico. Expediente físico y/o digitalizado.
3- Usos: Clasificar a los clientes conforme a su perfil transaccional y limitar las operaciones permitidas de los Clientes.
4. Divulgación: A. Transferencias. Proveedores de servicio de revisión de monitoreo de transacciones.
Proveedores de servicio de revisión de referencias.
B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting;
-Cómputo en la nube, call Center, servicios de atención a cliente (SMS, Mail, redes sociales y proveedores de destrucción segura de información).
5. Bloqueo: 15 días contados desde la fecha de rechazo y/o no aceptación.
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado cuando el trataamiento sea necesario para dar cumplimiento a la relación jurídica con el titular.
-Expreso por tratarse de datos patrimoniales y financieros.
-Expreso y por escrito o mediante tecnología de autenticación equivalente para datos sensibles.

2.5.2. Operaciones con moneda extranjera

Respecto a las operaciones nacionales se identificaron las siguientes:

1. Emisión de Fondos de Pago Electrónico en Moneda Extranjera.

Se identificó que se obtienen datos personales patrimoniales y/o financieros y transaccionales. Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención:**
   - Directa.
   - Previa o durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
   - Sistema tecnológico.
   - Expediente físico y/o digitalizado.
3) **Usos**:
   - Cumplimiento regulatorio.
   - Cumplimiento de las obligaciones derivadas del contrato de servicios.
4) **Divulgación/otros sujetos intervinientes:**
   - Transferencias:
     - SHCP.
     - CNBV.
   - Remisiones:
     - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
     - Hosting.
     - Cómputo en la nube.
     - Call Center.
     - Servicios de atención al cliente.
     - Proveedores de destrucción segura de información.
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

2. Límites de cuentas.

Se identificó que se obtienen datos personales patrimoniales y/o financieros y transaccionales. Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención**:
   - Directa e indirecta.
   - Previa o durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento**:
   - Sistema tecnológico.
   - Expediente físico y/o digitalizado.
3) **Usos:**
   - Cumplimiento regulatorio.
   - Cumplimiento de las obligaciones derivadas del contrato de servicios.
4) **Divulgación/otros sujetos intervinientes:**
   - Transferencias:
     - SHCP.
     - CNBV.
   - Remisiones:

    - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
    - Hosting.
    - Cómputo en la nube.
    - Call Center.
    - Servicios de atención al cliente.
    - Proveedores de destrucción segura de información.
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

3. Abono de recursos en moneda extranjera

Se identificó que se obtienen datos personales de identificación y autenticación, patrimoniales y/o financieros y transaccionales. Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención**:
    - Directa e indirecta.
    - Previa o durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento**:
    - Sistema tecnológico.
    - Expediente físico y/o digitalizado.
3) **Usos**:
    - Cumplimiento regulatorio.
    - Cumplimiento de las obligaciones derivadas del contrato de servicios.
4) **Divulgación/otros sujetos intervinientes:**
    - Transferencias:
        - SHCP.
        - CNBV.
    - Remisiones:
        - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
        - Hosting.
        - Cómputo en la nube.
        - Call Center.
        - Servicios de atención al cliente.
        - Proveedores de destrucción segura de información.
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

4. Cargo de recursos

Se identificó que se obtienen datos personales de identificación y autenticación, patrimoniales y/o financieros y transaccionales. Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención**:
    - Directa e indirecta.
    - Previa o durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
    - Sistema tecnológico.
    - Expediente físico y/o digitalizado.
3) **Usos**:
    - Cumplimiento regulatorio.
    - Cumplimiento de las obligaciones derivadas del contrato de servicios.
4) **Divulgación/otros sujetos intervinientes:**

- Transferencias:
    - SHCP.
    - CNBV.
- Remisiones:
    - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
    - Hosting.
    - Cómputo en la nube.
    - Call Center.
    - Servicios de atención al cliente.
    - Proveedores de destrucción segura de información.

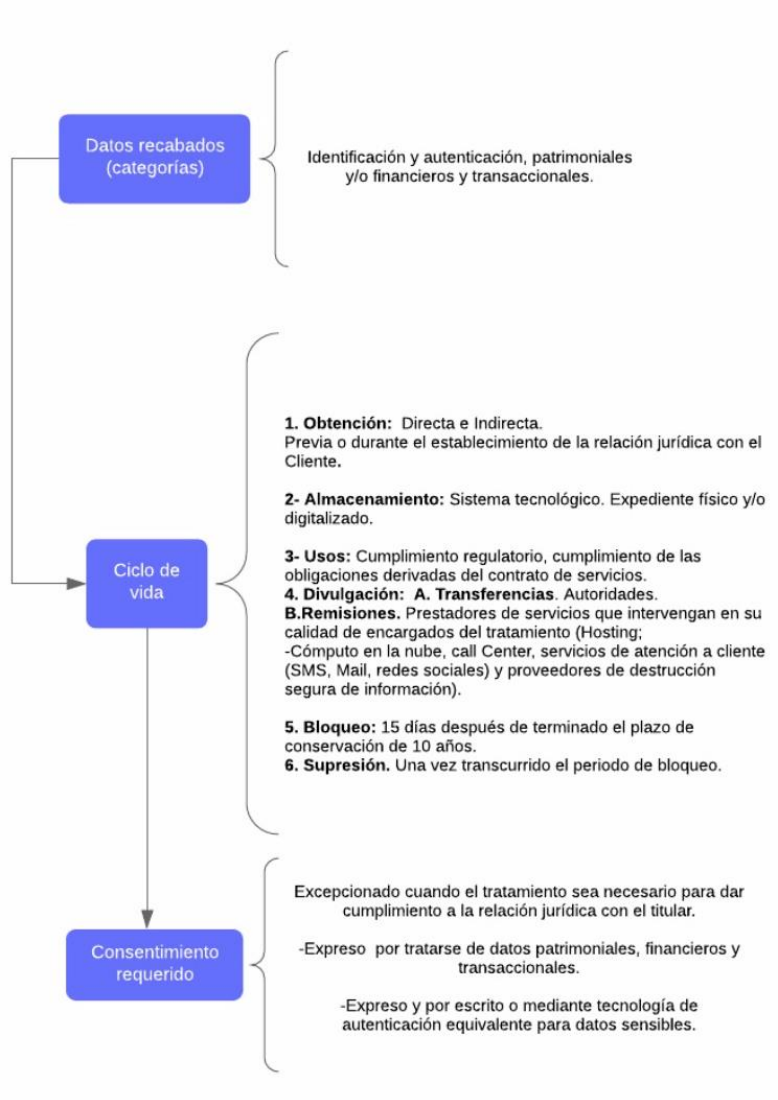
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

5. Transmisión de dinero en moneda extranjera

Se identificó que se obtienen datos personales patrimoniales y/o financieros y transaccionales. Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención:**
    - Directa.
    - Previa o durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento**:
    - Sistema tecnológico.
    - Expediente físico y/o digitalizado.
3) **Usos:**
    - Cumplimiento regulatorio.
    - Cumplimiento de las obligaciones derivadas del contrato de servicios.
4) **Divulgación/otros sujetos intervinientes:**
    - Transferencias:
        - SHCP.
        - CNBV.
    - Remisiones:
        - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
        - Hosting.
        - Cómputo en la nube.
        - Call Center.
        - Servicios de atención al cliente.
        - Proveedores de destrucción segura de información.
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

El ciclo de vida de este proceso se resume en el siguiente diagrama:


Datos recabados (categorías)
Identificación y autenticación, patrimoniales y/o financieros y transaccionales.
Ciclo de vida
1. Obtención: Directa e Indirecta.
Previa o durante el establecimiento de la relación jurídica con el Cliente.
2- Almacenamiento: Sistema tecnológico. Expediente físico y/o digitalizado.
3- Usos: Cumplimiento regulatorio, cumplimiento de las obligaciones derivadas del contrato de servicios.
4. Divulgación: A. Transferencias. Autoridades.
B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting;
-Cómputo en la nube, call Center, servicios de atención a cliente (SMS, Mail, redes sociales) y proveedores de destrucción segura de información).
5. Bloqueo: 15 días después de terminado el plazo de conservación de 10 años.
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado cuando el tratamiento sea necesario para dar cumplimiento a la relación jurídica con el titular.
-Expreso por tratarse de datos patrimoniales, financieros y transaccionales.
-Expreso y por escrito o mediante tecnología de autenticación equivalente para datos sensibles.

2.5.3. Operaciones de conformidad con la circular 12/2018 de BANXICO

Respecto de las operaciones conforme a la circular 12/2018 de BANXICO se identificó lo siguiente:

1. Sobregiros

Se identificó que se obtienen datos personales de identificación y autenticación y transaccionales. Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención**: Indirecta.
2) **Almacenamiento: Sistema tecnológico.**
3) **Usos**:
    - Cumplimiento regulatorio.
    - Cumplimiento de las obligaciones derivadas del contrato de servicios.
4) **Tratamientos identificados:**
5) **Divulgación/otros sujetos intervinientes:**
    - Transferencias:
        - SHCP.
        - CNBV.
    - Remisiones:
        - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
        - Hosting.
        - Cómputo en la nube.
        - Call Center.
        - Servicios de atención al cliente.
        - Proveedores de destrucción segura de información.
6) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
7) **Supresión**: una vez transcurrido el periodo de bloqueo.

2. Órdenes de Transferencias de Fondos de Pago Electrónicos

Se identificó que se obtienen datos personales de identificación y autenticación, patrimoniales y/o financieros y transaccionales. Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención**:
    - Directa.
    - Indirecta.
2) **Almacenamiento**:
    - Sistema tecnológico.
    - Expediente físico y/o digitalizado.
3) **Usos**: Cumplimiento de las obligaciones derivadas del contrato de servicios.
4) **Divulgación/otros sujetos intervinientes:**
    - Transferencias:
        - SHCP.
        - CNBV.
    - Remisiones:
        - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
        - Hosting.

    - Cómputo en la nube.
    - Call Center.
    - Servicios de atención al cliente.
    - Proveedores de destrucción segura de información.
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

3. Cargos no reconocidos

Se identificó que se obtienen datos personales de identificación y autenticación, patrimoniales y/o financieros y transaccionales. Asimismo, se identificó el siguiente ciclo de vida para los datos personales:

1) **Obtención**: Directa.
2) **Almacenamiento**:
    - Sistema tecnológico.
    - Expediente físico y/o digitalizado.
3) **Usos**:
    - Cumplimiento regulatorio.
    - Cumplimiento de las obligaciones derivadas del contrato de servicios.
4) **Divulgación/otros sujetos intervinientes:**
    - Transferencias:
        - CNBV.
        - SHCP.
    - Remisiones:
        - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
        - Hosting.
        - Cómputo en la nube.
        - Call Center.
        - Servicios de atención al cliente.
        - Proveedores de destrucción segura de información.
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

4. Órdenes de Transferencias de Fondos

Se identificó que se obtienen datos personales de identificación y autenticación, patrimoniales y/o financieros y transaccionales. Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención:**
    - Directa.
    - Indirecta.
2) **Almacenamiento:**
    - Sistema tecnológico.
    - Expediente físico y/o digitalizado.
3) **Usos**:
    - Cumplimiento regulatorio.
    - Cumplimiento de las obligaciones derivadas del contrato de servicios.
4) **Divulgación/otros sujetos intervinientes:**
    - Transferencias:
        - CNBV.
        - SHCP.

    - Instituciones receptoras de transferencias.[104]
  - Remisiones:
    - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
    - Hosting.
    - Cómputo en la nube.
    - Call Center.
    - Servicios de atención al cliente.
    - Proveedores de destrucción segura de información.
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

5. Transmisión de mensajes con pago con tarjetas

Se identificó que se obtienen datos personales de identificación y autenticación, patrimoniales y/o financieros y transaccionales. Asimismo, se identificó el siguiente ciclo de vida para los datos personales:

1) **Obtención**: Indirecta.
2) **Almacenamiento**:
   - Sistema tecnológico.
   - Expediente físico y/o digitalizado.
3) **Usos**:
   - Cumplimiento regulatorio.
   - Cumplimiento de las obligaciones derivadas del contrato de servicios.

4) **Divulgación/otros sujetos intervinientes:**
   - Transferencias:
     - SHCP.
     - CNBV.
     - Instituciones receptoras de transferencias.[105]
   - Remisiones:
     - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
     - Hosting.
     - Cómputo en la nube.
     - Call Center.
     - Servicios de atención al cliente.
     - Proveedores de destrucción segura de información.
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

6. Reclamo por robo o extravío de tarjetas/Reclamaciones por cargos no reconocidos

Se identificó que se obtienen datos personales de identificación y autenticación, patrimoniales y/o financieros y transaccionales. Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención:**
   - Directa.
   - Indirecta.
2) **Almacenamiento:**
   - Sistema tecnológico.

[104] Se exceptúa el consentimiento por 37.1 de la LFPDPPP y disposición 12 de la circular 14/2017.
[105] Se exceptúa el consentimiento por 37.1 de la LFPDPPP y disposición 12 de la circular 14/2017.

- Expediente físico y/o digitalizado.

3) **Usos**: Cumplimiento de las obligaciones derivadas del contrato de servicios.

4) **Divulgación/otros sujetos intervinientes:**
   - Transferencias: CNBV.
   - Remisiones:
     - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
     - Hosting.
     - Cómputo en la nube.
     - Call Center.
     - Servicios de atención al cliente.
     - Proveedores de destrucción segura de información.
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

7. Contratación de Domiciliaciones

Se identificó que se obtienen datos personales de identificación y autenticación, patrimoniales y/o financieros y transaccionales. Asimismo, se identificó el siguiente ciclo de vida para los datos personales:

1) **Obtención**: Directa.
2) **Almacenamiento:**
   - Sistema tecnológico.
   - Expediente físico y/o digitalizado.
3) **Usos**: Cumplimiento de las obligaciones derivadas del contrato de servicios.

4) **Divulgación/otros sujetos intervinientes:**
   - Transferencias:
     - CNBV.
     - SHCP.
   - Remisiones:
     - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
     - Hosting.
     - Cómputo en la nube.
     - Call Center.
     - Servicios de atención al cliente.
     - Proveedores de destrucción segura de información.
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.
7) **Actores involucrados:**
   - Titular: Cliente.
   - Responsable: IFPE.
   - Encargados:
     - Prestadores de servicio que intervengan en su calidad de encargados del tratamiento.
     - Hosting.
     - Cómputo en la nube.
     - Call Center
     - Proveedores de destrucción segura de información.
   - Terceros:
     - CNBV.
     - SHCP.

8. Cancelación del servicio de Domiciliación

Se identificó que se obtienen datos personales de identificación y autenticación, patrimoniales y/o financieros y transaccionales. Asimismo, se identificó el siguiente ciclo de vida de los datos personales:

1) **Obtención**: Directa.
2) **Almacenamiento**:
    - Sistema tecnológico.
    - Expediente físico y/o digitalizado.
3) **Usos**: Cumplimiento de las obligaciones derivadas del contrato de servicios.

4) **Divulgación/otros sujetos intervinientes:**
    - Transferencias:
        - CNBV.
        - SHCP.
    - Remisiones:
        - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
        - Hosting.
        - Cómputo en la nube.
        - Call Center.
        - Servicios de atención al cliente.
        - Proveedores de destrucción segura de información.
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

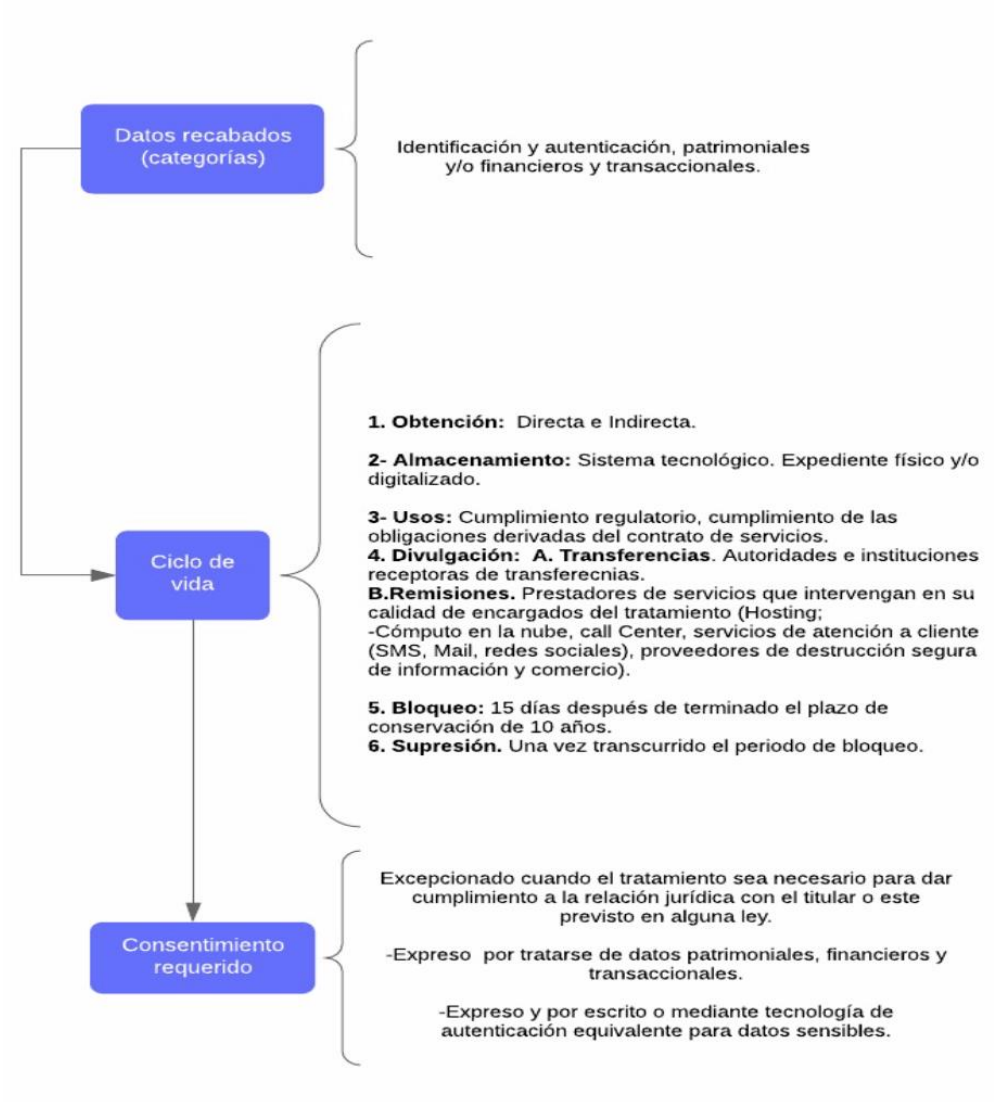
9. Objetar cargos por Domiciliación

Se identificó que se obtienen datos personales de identificación y autenticación, patrimoniales y/o financieros y transaccionales. Asimismo, se identificó el siguiente ciclo de vida para los datos personales:

1) **Obtención**: Directa.
2) **Almacenamiento:**
    - Sistema tecnológico.
    - Expediente físico y/o digitalizado.
3) **Usos**: Cumplimiento de las obligaciones derivadas del contrato de servicios.

4) **Divulgación/otros sujetos intervinientes:**
    - Transferencias:
        - CNBV.
        - SHCP.
    - Remisiones:
        - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
        - Hosting.
        - Cómputo en la nube.
        - Call Center.
        - Servicios de atención al cliente.
        - Proveedores de destrucción segura de información.
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

El ciclo de vida de este proceso se resume en el siguiente diagrama:


Datos recabados (categorías)
Identificación y autenticación, patrimoniales y/o financieros y transaccionales.
Ciclo de vida
1. Obtención: Directa e Indirecta.
2- Almacenamiento: Sistema tecnológico. Expediente físico y/o digitalizado.
3- Usos: Cumplimiento regulatorio, cumplimiento de las obligaciones derivadas del contrato de servicios.
4. Divulgación: A. Transferencias. Autoridades e instituciones receptoras de transferecnias.
B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting;
-Cómputo en la nube, call Center, servicios de atención a cliente (SMS, Mail, redes sociales), proveedores de destrucción segura de información y comercio).
5. Bloqueo: 15 días después de terminado el plazo de conservación de 10 años.
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado cuando el tratamiento sea necesario para dar cumplimiento a la relación jurídica con el titular o este previsto en alguna ley.
-Expreso por tratarse de datos patrimoniales, financieros y transaccionales.
-Expreso y por escrito o mediante tecnología de autenticación equivalente para datos sensibles.

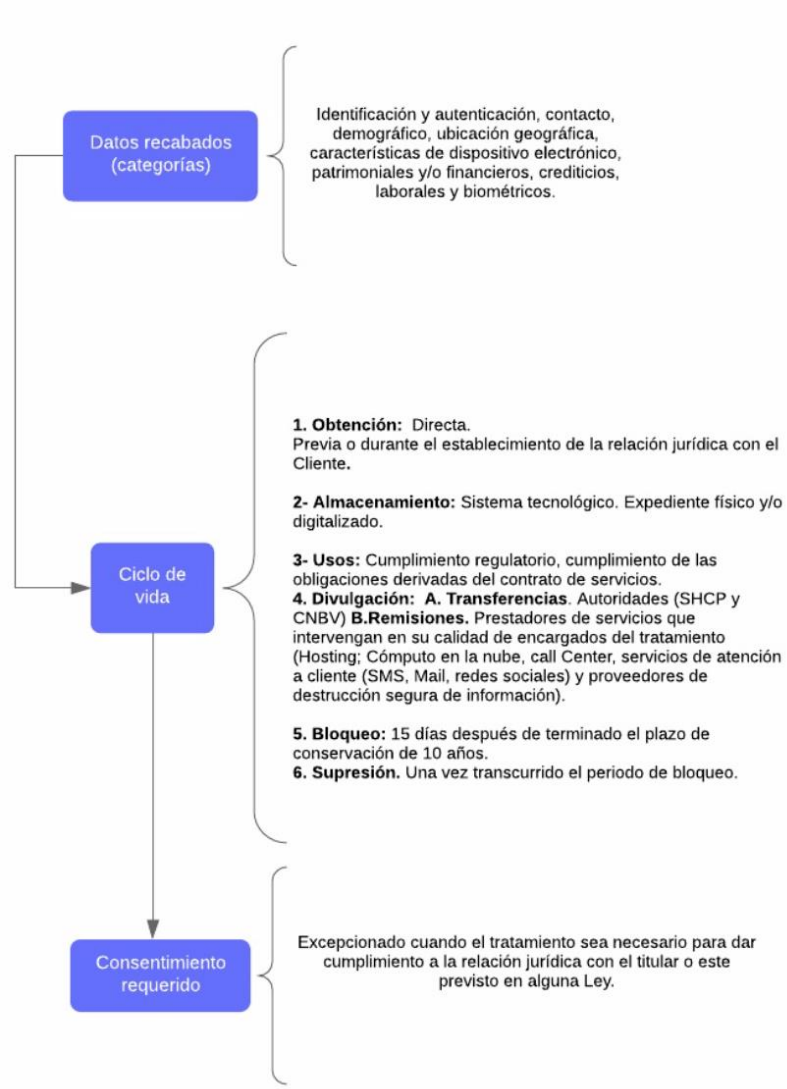
2.6. Cierre de cuentas

Existe la obligación de las IFPE de estipular en el contrato que celebren con sus clientes la posibilidad de que el cliente en cualquier momento pueda cerrar su cuenta de fondos de pagos electrónicos. Derivado de lo anterior se ha identificado el tratamiento de datos personales de identificación y autenticación, contacto, demográficos, ubicación geográfica, características de dispositivo electrónico, patrimoniales y/o financieros, crediticios, laborales y biométricos. Asimismo, se identificó el siguiente ciclo de vida para los datos personales:

1) **Obtención**:
    - Directa.
    - Previa o durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
    - Sistema tecnológico.
    - Expediente físico y/o digitalizado.
3) **Usos**:
    - Cumplimiento regulatorio.
    - Cumplimiento de las obligaciones derivadas del contrato de servicios.

4) **Divulgación/otros sujetos intervinientes:**
    - Transferencias:
        - CNBV.
        - SHCP.
    - Remisiones:
        - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
        - Hosting.
        - Cómputo en la nube.
        - Call Center.
        - Servicios de atención al cliente.
        - Proveedores de destrucción segura de información.
5) Bloqueo: 15 días después de terminado el plazo de conservación de 10 años.
6) Supresión: una vez transcurrido el periodo de bloqueo.

El ciclo de vida de este proceso se resume en el siguiente diagrama:

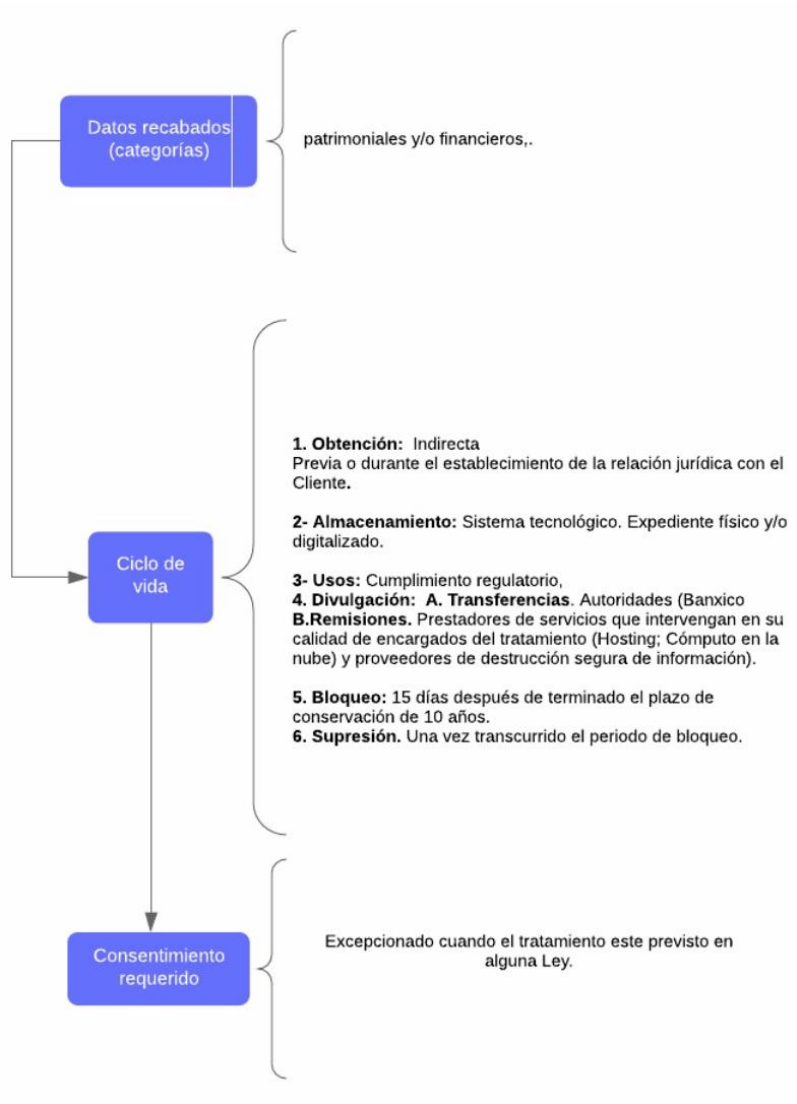

Datos recabados (categorías)
Identificación y autenticación, contacto, demográfico, ubicación geográfica, características de dispositivo electrónico, patrimoniales y/o financieros, crediticios, laborales y biométricos.
Ciclo de vida
1. Obtención: Directa.
Previa o durante el establecimiento de la relación jurídica con el Cliente.
2- Almacenamiento: Sistema tecnológico. Expediente físico y/o digitalizado.
3- Usos: Cumplimiento regulatorio, cumplimiento de las obligaciones derivadas del contrato de servicios.
4. Divulgación: A. Transferencias. Autoridades (SHCP y CNBV) B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting; Cómputo en la nube, call Center, servicios de atención a cliente (SMS, Mail, redes sociales) y proveedores de destrucción segura de información).
5. Bloqueo: 15 días después de terminado el plazo de conservación de 10 años.
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado cuando el tratamiento sea necesario para dar cumplimiento a la relación jurídica con el titular o este previsto en alguna Ley.

2.7. Requerimientos de información de BANXICO

Se identificó la obligación de las IFPE de suministrar a BANXICO la información transaccional de las Transferencias de Fondos y Transferencias de Fondos de Pago Electrónico enviadas y recibidas por sus Clientes. En este sentido, se identificó en este proceso un tratamiento de datos personales patrimoniales y/o financieros. Asimismo, se identifica el siguiente ciclo de vida:

1) **Obtención:**
    - Directa.
    - Previa o durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
    - Sistema tecnológico.
    - Expediente físico y/o digitalizado.
3) **Usos**:
    - Cumplimiento regulatorio.
4) **Divulgación/otros sujetos intervinientes:**
    - Transferencias: Banxico
    - Remisiones:
        - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
        - Hosting.
        - Cómputo en la nube.
        - Proveedores de destrucción segura de información.
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

El ciclo de vida de este proceso se resume en el siguiente diagrama:

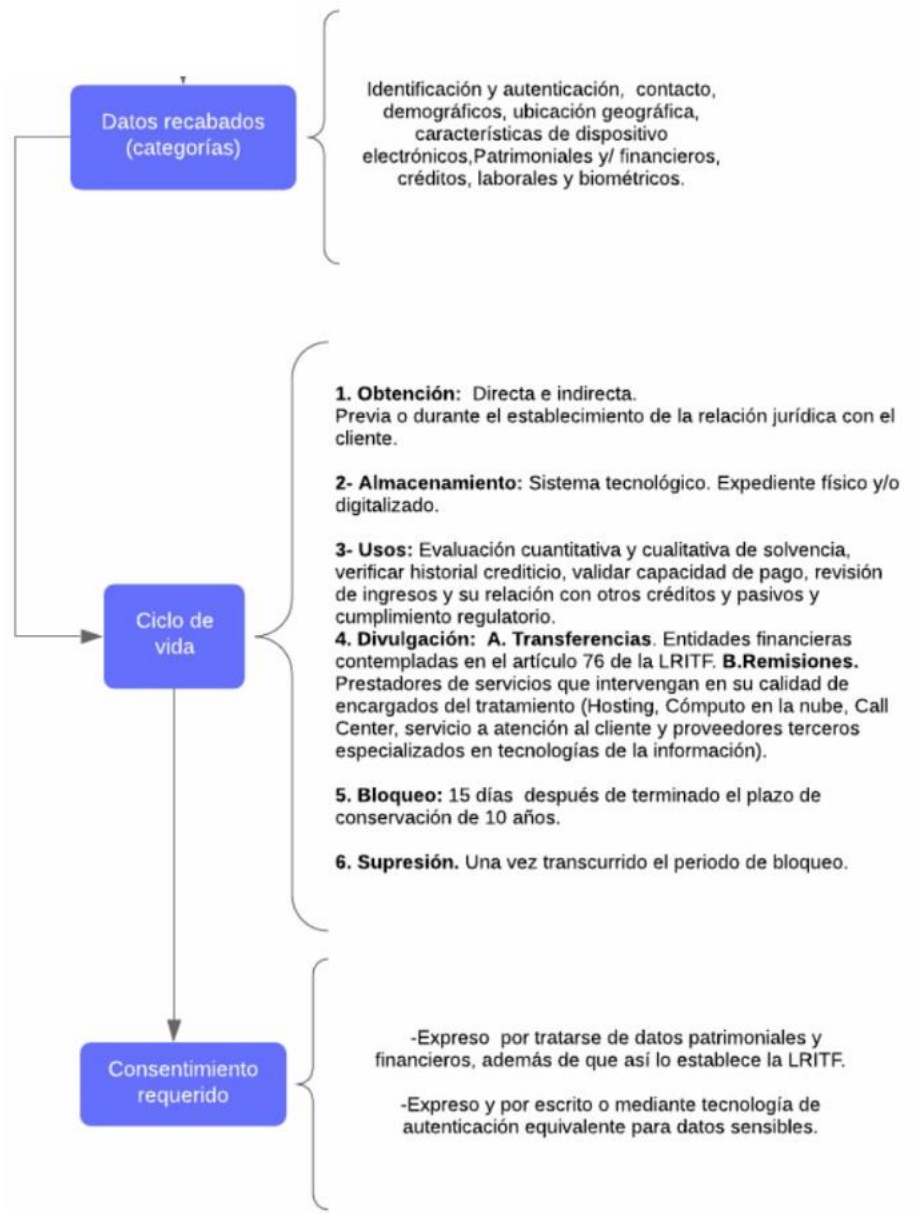

Datos recabados (categorías)
patrimoniales y/o financieros,.
Ciclo de vida
1. Obtención: Indirecta
Previa o durante el establecimiento de la relación jurídica con el Cliente.
2- Almacenamiento: Sistema tecnológico. Expediente físico y/o digitalizado.
3- Usos: Cumplimiento regulatorio,
4. Divulgación: A. Transferencias. Autoridades (Banxico
B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting; Cómputo en la nube) y proveedores de destrucción segura de información).
5. Bloqueo: 15 días después de terminado el plazo de conservación de 10 años.
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
Excepcionado cuando el tratamiento este previsto en alguna Ley.

2.8. Open banking

En el presente apartado se identificó el tratamiento de Open Banking previsto en el articulo 76 de la LRITF, en el cual se identifico que de forma directa se obtienen datos personales de identificación y autenticación, contacto, demográficos, ubicación geográfica, características de dispositivos electrónicos, patrimoniales y/o financieros, crediticios y laborales. Asimismo, se identificó el siguiente ciclo de vida:

1) **Obtención**:
    - Directa e Indirecta
    - Previa o durante el establecimiento de la relación jurídica con el Cliente.
2) **Almacenamiento:**
    - Sistema tecnológico.
    - Interfaces de Programación de aplicaciones informáticas.
3) **Usos:**
    - Evaluación cuantitativa y cualitativa de solvencia.
    - Verificar historial crediticio.
    - Validar capacidad de pago.
    - Revisión de ingresos y su relación con otros crédito y pasivos.
    - Cumplimiento regulatorio.
4) **Divulgación/otros sujetos intervinientes:**
    - Transferencias: Entidades Financieras contempladas en el artículo 76 de la LRITF: es necesario el consentimiento expreso.
    - Remisiones:
        - Prestador de servicios que intervengan en su calidad de encargado del tratamiento.
        - Hosting.
        - Cómputo en la nube.
        - Call Center.
        - Servicios de atención al cliente.
        - Proveedores terceros especializados en tecnologías de la información.
5) **Bloqueo**: 15 días después de terminado el plazo de conservación de 10 años.
6) **Supresión**: una vez transcurrido el periodo de bloqueo.

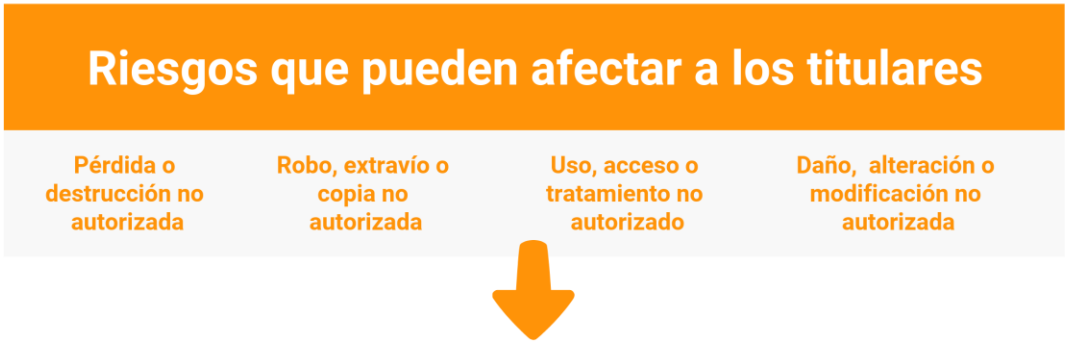
El ciclo de vida de este proceso se resume en el siguiente diagrama:


Datos recabados (categorías)
Identificación y autenticación, contacto, demográficos, ubicación geográfica, características de dispositivo electrónicos,Patrimoniales y/ financieros, créditos, laborales y biométricos.
Ciclo de vida
1. Obtención: Directa e indirecta.
Previa o durante el establecimiento de la relación jurídica con el cliente.
2- Almacenamiento: Sistema tecnológico. Expediente físico y/o digitalizado.
3- Usos: Evaluación cuantitativa y cualitativa de solvencia, verificar historial crediticio, validar capacidad de pago, revisión de ingresos y su relación con otros créditos y pasivos y cumplimiento regulatorio.
4. Divulgación: A. Transferencias. Entidades financieras contempladas en el artículo 76 de la LRITF. B.Remisiones. Prestadores de servicios que intervengan en su calidad de encargados del tratamiento (Hosting, Cómputo en la nube, Call Center, servicio a atención al cliente y proveedores terceros especializados en tecnologías de la información).
5. Bloqueo: 15 días después de terminado el plazo de conservación de 10 años.
6. Supresión. Una vez transcurrido el periodo de bloqueo.
Consentimiento requerido
-Expreso por tratarse de datos patrimoniales y financieros, además de que así lo establece la LRITF.
-Expreso y por escrito o mediante tecnología de autenticación equivalente para datos sensibles.

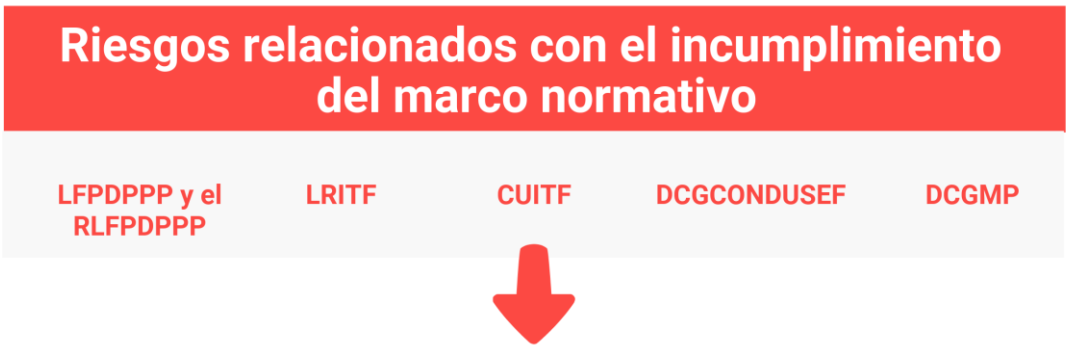
3. Identificación de riesgos

En esta parte del entregable 2 se realizó una identificación de riesgos en materia de seguridad de datos personales a partir de lo siguiente:

- **Señalamiento de los riesgos a la seguridad de los datos personales que podrían afectar a los titulares** como vulneraciones de seguridad según lo dispuesto en el artículo 63 del RLFPDPPP (pérdida o destrucción no autorizada; robo, extravío o copia no autorizada; uso, acceso o tratamiento no autorizado, o el daño, la alteración o modificación no autorizada).



- **Señalamiento de los riesgos relacionados con el posible incumplimiento al marco normativo** compuesto por la LFPDPPP, su Reglamento y demás normatividad aplicable a las ITF como la LRITF, la CUITF, las DCGA58, las DCGCONDUSEF, las DCGMP, entre otras.



3.1. Riesgos en materia de seguridad de la información que podrían afectar a los titulares

Para determinar los riesgos en materia de seguridad de la información se consideró como elemento objetivo del análisis la definición de "vulneración" prevista en el artículo 63 del RLFPDPPP y la probabilidad de que uno de los elementos calificados como pérdida o destrucción no autorizada; robo, extravío o copia no autorizada; uso, acceso o tratamiento no autorizado, o el daño, la alteración o modificación no autorizada pudiera presentarse en las ITF como resultado de los distintos procesos, subprocesos y tratamientos identificados en las ITF. Asimismo, respecto de cada uno de los riesgos identificados se presentó un listado ejemplificativo de los distintos controles previstos en el estándar internacional de seguridad *ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls* que podrían verse comprometidos como resultado de la actualización de una vulneración de seguridad. Estos controles son los siguientes:

- Políticas de seguridad de información.

- Organización de Seguridad de la Información.
- Seguridad de Recursos Humanos.
- Gestión de activos.
- Control de acceso.
- Criptografía.
- Seguridad física y del entorno.
- Seguridad en las operaciones.
- Seguridad en las comunicaciones.
- Adquisición, desarrollo y mantenimientos de sistemas.
- Relacionamiento con los proveedores.
- Gestión de incidentes de seguridad de la información.
- Aspectos de seguridad de la información de la gestión de la continuidad de negocios.
- Cumplimiento.

Como resultado del análisis realizado en los procesos, subprocesos y tratamientos de datos personales en las ITF se identificó lo siguiente:

- Se detectó una posible vulneración a los principios de licitud, lealtad y calidad en el tratamiento de Identificación del cliente. Mientras que se detectaron posibles vulneraciones a los principios de licitud, consentimiento, lealtad y finalidad en el tratamiento de Autenticación del cliente.
- Se identificaron posibles vulneraciones a los principios de licitud, lealtad y responsabilidad, así como posible incumplimiento a los deberes de seguridad y confidencialidad, en los tratamientos de Servicios de pago de terceros (agregadores), consulta y elaboración de listas negras.
- Para el caso del *Uso de cookies, web beacons y tecnologías similares y del uso de Servicios de verificación de la identidad de terceros,* se identificaron posibles vulneraciones a los principios de licitud, lealtad, información, consentimiento y responsabilidad.
- Se detectaron posibles vulneraciones de los principios de licitud, lealtad, finalidad, información y responsabilidad en los tratamientos de elaboración de perfiles mediante IA, aprendizaje de máquinas y el uso de técnicas de big data.
- Respecto al tratamiento de asesoría robótica se identificaron posibles vulneraciones a los principios de licitud, lealtad y responsabilidad y, en el caso de atención a clientes por medio de terceros (atención a clientes mediante centros de contacto, chatbots, correo electrónico) KYC se detectó un posible incumplimiento al principio de responsabilidad y a los deberes de seguridad y confidencialidad.
- Respecto al tratamiento de cobranza por parte de terceros (encargados) se detectó un posible incumplimiento a los principios de finalidad y de responsabilidad así como posible incumplimiento a los deberes de seguridad y confidencialidad. Y en lo relativo al tratamiento de Scoring crediticio podría existir una vulneración a los principios de licitud, lealtad y calidad.
- El uso de datos de redes sociales representa un riesgo en el incumplimiento a los principios de licitud, lealtad, finalidad y responsabilidad. Mientras que el envío de publicidad Personalizada y ofrecimiento de productos y servicios podría implicar el incumplimiento a los principios de licitud y consentimiento.
- Finalmente, para los tratamientos de KYC se detectó un posible incumplimiento a los principios de calidad y responsabilidad; la segmentación de clientes trae consigo el riesgo de incumplimiento a los principios de licitud, lealtad, proporcionalidad, y responsabilidad; mientras que en el caso de almacenamiento en infraestructura de cómputo en la nube se detectó un posible incumplimiento a los principios seguridad y confidencialidad así como un posible incumplimiento al principio de responsabilidad.
- Respecto a los riesgos que podrían afectar a los titulares, se identifican como riesgos posibles la discriminación y exclusión del uso de los servicios financieros en los tratamientos de Identificación del cliente, Servicios de verificación de la identidad de terceros, consulta y elaboración de listas negras, segmentación de clientes, elaboración de perfiles mediante IA, aprendizaje de máquinas y el uso de técnicas de *big data*.

- Por último, se identifican riesgos de conductas ilícitas como fraude o robo de identidad en perjuicio del titular, en los tratamientos de Identificación del cliente, autenticación del cliente y servicios de verificación de la identidad de terceros.

En lo que concierne a los controles identificados en la norma *ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls* se identificó lo siguiente:

- En el contexto de **Políticas de Seguridad de la Información** se resalta la importancia de contar con dichas políticas para asegurar que al interior de la organización se tenga conocimiento de los procesos que se deben llevar a cabo para garantizar la seguridad de la información, lo cual no solamente constituye una buena práctica en materia de protección de datos personales, sino que responde al cumplimiento de las obligaciones impuestas en la CUITF.
- En lo respectivo a la **Organización de Seguridad de la Información** la CUITF en el artículo 65 de la misma, establece que "las instituciones de financiamiento colectivo deberán contar con una persona que, entre sus funciones, se desempeñe como oficial en jefe de seguridad de la información" mientras que el artículo 66 de las citadas disposiciones establecen la responsabilidad del oficial en jefe de seguridad de la información de "Participar en la definición y verificar la implementación y continuo cumplimiento de las políticas y procedimientos de seguridad señalados en el artículo 63 de las presentes disposiciones." por lo que las propias disposiciones contemplan la existencia de al menos un responsable dedicado a iniciar y controlar la implementación de las iniciativas y políticas de operación de la seguridad de la información.
- Asimismo, a lo largo del presente estudio se identificaron riesgos de **Seguridad de Recursos Humanos** dado que ciertos colaboradores dentro de la ITF pueden tener acceso a todos los datos de identificación, ubicación, así como biométricos de los Clientes, por lo que el mismo artículo 72 de la CUITF insta a las Instituciones de financiamiento colectivo para que utilicen factores de autenticación para identificar a sus Clientes especificando que los mismos tendrán como requisito el "No ser conocida con anterioridad a su generación y a su uso por los funcionarios, empleados, representantes de la institución de financiamiento colectivo o por terceros." y, de acuerdo con el artículo 81 del mismo ordenamiento, las IFC "tendrán prohibido solicitar a sus Clientes, a través de sus funcionarios, empleados o representantes, la información parcial o completa, de los Factores de Autenticación a que se refiere el artículo 72 de las disposiciones".
- En lo relativo a la **Gestión de Activos** se identificó que las organizaciones deben llevar un adecuado control y tener un conocimiento preciso de la información que está bajo su gestión con la finalidad de que se implementen los controles adecuados al tipo de información que se maneja, por lo que, aunado a la clasificación del tipo de datos que contempla la LFPDPPP, la CUITF en su artículo 63 establece la obligación de clasificar la información considerando al menos una categoría referente a la información crítica en la cual se deberán incluir como mínimo la Información Sensible y las imágenes de identificaciones oficiales e información biométrica de los Clientes, así como cualquier otra que determinen de acuerdo con sus políticas las IFC.
- No obstante que en el contexto de una institución financiera parecería evidente la existencia de **Controles de Acceso** que restrinjan la visibilidad que tienen tanto los funcionarios de la institución como los terceros ajenos a la misma, la CUITF no escatima en especificar las políticas que se deben seguir para limitar o controlar el acceso a la información ya que, de lo contrario, tanto la ITF como los Clientes podrían sufrir pérdidas económicas o ver sus identidades afectadas, por lo que dicho ordenamiento considera como incidentes de seguridad de la información a cualquier pérdida por accesos no autorizados que deriven en el uso indebido de la información o de los sistemas e insta a las IFC en el artículo 63 fracción VI, inciso a establecer mecanismos de identificación y Autenticación de todos y cada uno de los Usuarios de la Infraestructura Tecnológica (funcionarios o no de la ITF), que permitan reconocerlos de forma inequívoca y aseguren el acceso únicamente a las personas autorizadas expresamente para ello, bajo el principio de mínimo privilegio.

- Se identificó también como riesgo de las ITF el que cualquier vulneración de seguridad en la que exista fuga de información podría exponer los datos y datos sensibles de los Clientes, por lo que deben existir lineamientos para la protección de la información por **medios criptográficos** lo cual retoma la multicitada CUITF en el artículo 63 fracción VI, inciso b donde se establece la obligación de las IFC de llevar a cabo el cifrado de la información conforme al grado de sensibilidad o clasificación de la información que la institución de financiamiento colectivo determine y obliga a cifrar al menos, la información que hayan clasificado como crítica, misma que, como ya vimos, incluye a la información sensible.
- Asimismo, se identificaron riesgos relativos a la **Seguridad Física y del Entorno** en el que la falta de perímetros de seguridad para proteger las áreas que contienen información sensible, así como las áreas en las que se lleva a cabo el tratamiento de la información podría traer como consecuencia el acceso físico no autorizado, los daños e interferencia a la información de la organización por parte de terceros no autorizados o colaboradores por mala fe o negligencia. Al respecto, la CUITF en el multicitado artículo 63 fracción VI, inciso e) se estipula que se deben implementar "Mecanismos de seguridad, tanto de acceso físico, como de controles ambientales y de energía eléctrica, que protejan la Infraestructura Tecnológica y permitan la operación".
- Se identificó que las ITF están expuestas los riesgos inherentes a las operaciones que se llevan a cabo a través de medios digitales por lo que identificamos que la falta de medidas adecuadas para la elaboración de copias de respaldo, mantenimiento de los equipos, gestión de soportes, gestión del correo, y seguridad de la infraestructura tecnológica puede traer como consecuencia la pérdida o destrucción de la información biométrica, de identificación y financiera de los Clientes, por lo que la CUITF, para mantener la **Seguridad en las Operaciones y Seguridad en las Comunicaciones,** regula en los artículos 63 la obligación de contar con un plan de continuidad de negocio en el que se cuente con mecanismos de respaldo y procedimientos de recuperación de la información que mitiguen el riesgo de interrupción de la operación, mientras que el artículo 68 establece que los Eventos de Seguridad de la Información calificados como relevantes e Incidentes de Seguridad de la Información a que se refiere el presente artículo deberá estar respaldada y conservada durante 10 años y finalmente, conforme al artículo 83 fracción I, cuando las IFC cuenten con canales remotos tales como centros de atención telefónica o canales electrónicos de mensajería deberán "mantener controles de seguridad física o lógica o ambas según sea el caso en la Infraestructura Tecnológica de los canales remotos, incluyendo los dispositivos de grabación de las comunicaciones y los medios de almacenamiento y respaldo de estas, que protejan en todo momento la confidencialidad e integridad de la información proporcionada por sus Clientes".
- En línea con lo anterior, atendiendo a que las operaciones de las ITF se llevan a cabo de manera 100% digital a través de medios electrónicos, existen riesgos que se pueden materializar en la **adquisición, desarrollo y mantenimiento de sistemas**, por lo que se deben considerar los requisitos de seguridad de la información desde la etapa de diseño de los sistemas, de lo contrario existe el riesgo de pérdida o acceso no autorizado a la información de los Clientes. Esto se refleja en el artículo 63 fracción CUITF en la cual se establece la obligación de que las IFC "en sus fases de estrategia, diseño, transición, operación y mejora continua, se proteja la integridad de la Infraestructura Tecnológica, así como la integridad, confidencialidad y disponibilidad de la información recibida, generada, procesada, almacenada y transmitida por esta". Y en la fracción III del mismo artículo se establece la obligación de "Que se hayan considerado aspectos de seguridad de la información en la definición de proyectos para adquirir o desarrollar cada uno de sus componentes, debiendo incluirlos durante las diversas etapas del ciclo de vida. Este comprenderá la elaboración de requerimientos, diseño, desarrollo o adquisición, pruebas de implementación, pruebas de aceptación por parte de los Usuarios de la Infraestructura Tecnológica, procesos de liberación incluyendo pruebas de vulnerabilidades y análisis de código previos a su puesta en producción, pruebas periódicas, gestión de cambios, reemplazo y destrucción de información. "
- Otro de los riesgos identificados en la operación de las ITF recae en la interacción que estas puedan tener en su **Relacionamiento con los Proveedores** ya que las entidades pueden contratar a terceros proveedores que lleven a cabo cualquier proceso que se desarrolle dentro

de la ITF por lo que la falta de identificación y los controles de seguridad de información para abordar específicamente el acceso de los proveedores a la información de la organización así como de implementación de seguridad en contratos con terceros puede conllevar riesgos en materia de seguridad de la información, por lo que los artículos 85 a 88 de la CUITF regulan los requisitos que debe cumplir una ITF para poder contratar ciertos servicios con terceros así como los pasos que se deben seguir para obtener la autorización por parte de las Autoridades Financieras para llevar a cabo dichas contrataciones.

- Respecto a la **Gestión de Incidentes de Seguridad de la Información** se reconoce el riesgo al cual las ITF, al igual que el resto de las instituciones financieras, están expuestas constantemente expuestas a tener eventos o Incidentes de Seguridad de la Información dada la conectividad que tienen y la cantidad de información valiosa que almacenan. La CUITF define como Incidente de Seguridad de la Información a cualquier Evento de Seguridad de la Información en que una IFC "(i) Haya comprometido la confidencialidad, integridad o disponibilidad de un componente o la totalidad de la Infraestructura Tecnológica con un efecto adverso para la institución de financiamiento colectivo, sus Clientes, terceros, proveedores o contrapartes, entre otros. (ii) Vulnere la Infraestructura Tecnológica comprometiendo la información que procesa, almacena o transmite. (iii) Constituya una violación de las políticas y procedimientos de seguridad de la información. o (iv) Represente la materialización de una pérdida, ya sea por extracción, alteración o extravío de la información; por fallas derivadas del uso del hardware, software, sistemas, aplicaciones, redes y cualquier otro canal de transmisión de información; por accesos no autorizados que deriven en el uso indebido de la información o de los sistemas; por fraude, robo, o en interrupción de los servicios, atentados contra las infraestructuras interconectadas, conocidos como ciberataques, entre otros." Al efecto, el artículo 67 de la CUITF establece la obligación de las ITF de hacer del conocimiento de la CNBV de forma inmediata los Incidentes de Seguridad de la Información.
- Por otro lado, como se mencionó la CUITF regula en los artículos 63 la obligación de contar con un plan de continuidad de negocio en el que se cuente con mecanismos de respaldo y procedimientos de recuperación de la información que mitiguen el riesgo de interrupción de la operación, por lo que se reconoce la importancia de contar con **aspectos de Seguridad de la Información de la Gestión de la Continuidad Negocios** y destina el capítulo V de la misma CUITF para establecer la obligación de contar con procedimientos de continuidad de la operación que aseguren el pronto restablecimiento de las operaciones y las obligaciones a cargo de las personas responsables del establecimiento y ejecución de dicho proceso, mientras que el anexo 10 establece los requerimientos mínimos para desarrollar el Plan de Continuidad de Negocio
- Por último, sin importar cuántas políticas regulen la seguridad de la información al interior de las ITF, existe el riesgo de que las mismas carezcan de efectividad si no hay una persona encargada, por lo que en el artículo 65 de la CUITF se establece la obligación de contar con un Oficial de Seguridad de la información quien se encargará del debido **Cumplimiento** por lo que se deberá asegurar de que se cumpla con las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información.

3.2. Riesgos relacionados con el incumplimiento del marco jurídico aplicable a las ITF

Como resultado de la identificación de los tratamientos de datos personales realizada en la Parte 2 del Entregable 2, se elaboraron una serie de tablas con la descripción concreta de los riesgos relacionados con el posible incumplimiento a la normatividad en materia de protección de datos personales aplicable a las ITF como es la LFPDPPP, su Reglamento y su normatividad de desarrollo. Asimismo, como parte de los riesgos relacionados con el incumplimiento al marco normativo se identificaron las distintas disposiciones legales aplicables al entorno ITF que podrían incumplirse, tales como la LRITG, la CUITF, las DCGA58, las DCGCONDUSEF, las DCGMP, entre otras.

Respecto los riesgos relacionados con el posible incumplimiento del marco normativo se identificó lo siguiente en los distintos procesos y tratamientos relacionados con las operaciones de las ITF:

Riesgos relacionados con el incumplimiento del marco jurídico aplicable a las ITF

- **Alta del cliente (los cuales deberán dividirse por tipo de cliente).**
  - La debilidad en los controles para la adecuada identificación del cliente de acuerdo con información histórica o preexistente puede dar lugar al incumplimiento de los artículos 7, 11 y de la LFPDPPP y el Título Tercero Capítulo VII de la CUITF (artículos 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83 y 84).
  - La debilidad en los mecanismos de autenticación del cliente para la contratación de servicios y realización de operaciones en las ITF puede dar lugar al incumplimiento de lo previsto en los artículos 7, 8, 9, 10 y 12 y de la LFPDPPP, el Título Tercero Capítulo VII de la CUITF (artículos 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83 y 84) y el artículo 8 de las DCGCONDUSEF.
  - Acontecimientos consistentes en que terceros pueden tener acceso a datos personales sin otorgar las garantías de seguridad previstas en la normatividad, facilitar información que pueda estar desactualizada o no reflejar la situación real o actual del titular, incumplir la obligación de formalizar adecuadamente la relación jurídica conforme a lo que exige la LFPDPP (encargados) puede dar lugar al incumplimiento de lo previsto en los artículos 7, 8, 9, 10 y 12 y de la LFPDPPP y el Título Tercero Capítulo VII de la CUITF (artículos 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84 y 85)
  - El hecho de que terceros puedan tener acceso a datos personales mediante el uso de APIs sin otorgar las garantías de seguridad previstas en la normatividad puede representar un incumplimiento a lo previsto por artículos 7, 8, 9, 10, 12, 14,19, 20 y 21 de la LFPDPPP y el artículo 76 de la LRITF.
  - La elaboración de listas negras puede representar un incumplimiento a lo previsto en los artículos 7, 8, 9, 10, 12, 14,19, 20 y 21 de la LFPDPPP.
  - La debilidad en los controles y procedimientos para conocimiento del cliente puede dar lugar al incumplimiento de lo previsto en los artículos 11 y 14 de la LFPDPPP, así como a lo previsto en el artículo 58 de la LRITF.
  - La falta de garantías para la adecuada protección y seguridad de los datos personales en infraestructura de cómputo en la nube gestionada por terceros puede dar lugar al incumplimiento de lo previsto en los artículos 14, 19, 20 y 21 de la LFPDPPP, artículos 50, 51 y 52 del RLFPDPPP, al Capítulo III del RLFPDPPP (artículos 57 a 66 del RLFPDPPP) y al Título Tercero Capítulos VI y VIII de la CUITF.
  - El hecho de que se usen asesores robóticos cuya programación no sea adecuada y afecte la facultad del titular para decidir de manera libre sobre el uso de sus datos y se le podría inducir a tomar decisiones erradas puede dar lugar al incumplimiento de lo previsto en los artículos 7 y 14 de la LFPDPPP.
  - El hecho de que existan terceros que puedan tener acceso a datos personales sin otorgar las garantías de seguridad y confidencialidad previstas en la normatividad puede dar lugar al incumplimiento de lo previsto en los artículos 14, 19, 20 y 21 de la LFPDPPP, artículos 50, 51 y 52 del RLFPDPPP, el Capítulo III del RLFPDPPP (artículos 57 a 66 del RLFPDPPP) y el Título Tercero Capítulo VII (artículos 77 y 83) y Capítulo VIII de la CUITF (artículos 85, 86, 87 y 88).
  - La obtención ilícita de datos de redes sociales puede dar lugar al incumplimiento de lo previsto en los artículos 7, 8, 9, 10 y 12 y de la LFPDPPP.
  - La segmentación de bases de datos (incluso con datos sensibles) y la generación de nuevas bases de datos puede dar lugar al incumplimiento de lo previsto en los artículos 7, 13 y 14 y de la LFPDPPP.
  - La asignación de una calificación crediticia al cliente a partir de información desactualizada puede dar lugar al incumplimiento de lo previsto en los artículos 7, 13 y 14 de la LFPDPPP.

- La elaboración de perfiles mediante el uso de IA cuando dé lugar a percepciones erróneas en caso de que no exista una adecuada programación de algoritmos puede representar un incumplimiento a lo previsto en los artículos 7, 12, 13, 14 y 15 de la LFPDPPP.
- La realización de tratamientos no consentidos ni informados al titular de forma previa al uso de técnicas de IA puede dar lugar al incumplimiento de lo previsto en los artículos 7, 12, 13, 14 y 15 de la LFPDPPP.
- El uso de técnicas de *big data* cuando no se prevean las medidas adecuadas para cumplir los principios de la LFPDPPP puede dar lugar al incumplimiento de los artículos 7, 12, 13, 14 y 15 de la LFPDPPP.
- El uso no consentido de cookies, web beacons y tecnologías similares puede dar lugar al incumplimiento de lo previsto en los artículos 7, 8, 14 y 15 de la LFPDPPP y el artículo 52 de las DCGCONDUSEF.
- El hecho de que terceros puedan a tener acceso a datos personales mediante el uso de APIs sin otorgar las garantías de seguridad previstas en la normatividad puede representar un incumplimiento a lo previsto en los artículos 7, 8, 9, 10, 12, 14, 19, 20 y 21 de la LFPDPPP, el Capítulo III del RLFPDPPP (artículos 57 a 66 del RLFPDPPP) y el artículo 76 de la LRITF.

- **PLD/CFT**
  - La debilidad en los controles para la adecuada identificación del cliente de acuerdo con información histórica o preexistente puede dar lugar al incumplimiento de los artículos 7, 11 y de la LFPDPPP y el Título Tercero Capítulo VII de la CUITF (artículos 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83 y 84).
  - El hecho de que existan terceros que puedan tener acceso a datos personales del titular sin otorgar las garantías de seguridad previstas en la normatividad en servicios de verificación de la identidad puede representar un incumplimiento a lo previsto en los artículos 7, 8, 9, 10 y 12 y de la LFPDPPP y al Título Tercero Capítulo VII de la CUITF (artículos 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84 y 85).
  - La elaboración de listas negras puede representar un incumplimiento a lo previsto en los artículos 7, 8, 9, 10, 12, 14,19, 20 y 21 de la LFPDPPP.
  - La debilidad en los controles y procedimientos para conocimiento del cliente puede dar lugar al incumplimiento de lo previsto en los artículos 11 y 14 de la LFPDPPP, así como a lo previsto en el artículo 58 de la LRITF.
  - La falta de garantías para la adecuada protección y seguridad de los datos personales en infraestructura de cómputo en la nube gestionada por terceros puede dar lugar al incumplimiento de lo previsto en los artículos 14, 19, 20 y 21 de la LFPDPPP, los artículos 50, 51 y 52 del RLFPDPPP, el Capítulo III del RLFPDPPP (artículos 57 a 66 del RLFPDPPP) y al Título Tercero Capítulos VI y VIII de la CUITF.
  - La obtención ilícita de datos de redes sociales puede dar lugar al incumplimiento de lo previsto en los artículos 7, 8, 9, 10 y 12 y de la LFPDPPP.
  - La segmentación de bases de datos (incluso con datos sensibles) y la generación de nuevas bases de datos puede dar lugar al incumplimiento de lo previsto en los artículos 7, 13 y 14 y de la LFPDPPP.
  - La elaboración de perfiles mediante el uso de IA cuando dé lugar a percepciones erróneas en caso de que no exista una adecuada programación de algoritmos puede representar un incumplimiento a lo previsto en los artículos 7, 12, 13, 14 y 15 de la LFPDPPP.
  - La realización de tratamientos no consentidos ni informados al titular de forma previa al uso de técnicas de IA puede dar lugar al incumplimiento de lo previsto en los artículos 7, 12, 13, 14 y 15 de la LFPDPPP.

- El uso de técnicas de *big data* cuando no se prevean las medidas adecuadas para cumplir los principios de la LFPDPPP puede dar lugar al incumplimiento de los artículos 7, 12, 13, 14 y 15 de la LFPDPPP.
- El uso no consentido de cookies, web beacons y tecnologías similares puede dar lugar al incumplimiento de lo previsto en los artículos 7, 8, 14 y 15 de la LFPDPPP y el artículo 52 de las DCGCONDUSEF.
- El hecho de que terceros puedan a tener acceso a datos personales mediante el uso de APIs sin otorgar las garantías de seguridad previstas en la normatividad puede representar un incumplimiento a lo previsto en los artículos 7, 8, 9, 10, 12, 14, 19, 20 y 21 de la LFPDPPP, el Capítulo III del RLFPDPPP (artículos 57 a 66 del RLFPDPPP) y el artículo 76 de la LRITF.

- **Obligación de conservación de documentos.**
  - La debilidad en los controles para la adecuada identificación del cliente de acuerdo con información histórica o preexistente puede dar lugar al incumplimiento de los artículos 7, 11 y de la LFPDPPP y el Título Tercero Capítulo VII de la CUITF (artículos 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83 y 84).
  - El hecho de que existan terceros que puedan tener acceso a datos personales del titular sin otorgar las garantías de seguridad previstas en la normatividad en servicios de verificación de la identidad puede representar un incumplimiento a lo previsto en los artículos 7, 8, 9, 10 y 12 y de la LFPDPPP y al Título Tercero Capítulo VII de la CUITF (artículos 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84 y 85).
  - La elaboración de listas negras puede representar un incumplimiento a lo previsto en los artículos 7, 8, 9, 10, 12, 14,19, 20 y 21 de la LFPDPPP.
  - La debilidad en los controles y procedimientos para conocimiento del cliente puede dar lugar al incumplimiento de lo previsto en los artículos 11 y 14 de la LFPDPPP, así como a lo previsto en el artículo 58 de la LRITF.
  - La falta de garantías para la adecuada protección y seguridad de los datos personales en infraestructura de cómputo en la nube gestionada por terceros puede dar lugar al incumplimiento de lo previsto en los artículos 14, 19, 20 y 21 de la LFPDPPP, los artículos 50, 51 y 52 del RLFPDPPP, el Capítulo III del RLFPDPPP (artículos 57 a 66 del RLFPDPPP) y al Título Tercero Capítulos VI y VIII de la CUITF.
  - En servicios de atención a clientes, el hecho de que puedan existir terceros que puedan tener acceso a datos personales sin otorgar las garantías de seguridad y confidencialidad previstas en la normatividad puede representar un incumplimiento a lo previsto en los artículos 50, 51 y 52 del RLFPDPPP, el Capítulo III del RLFPDPPP (artículos 57 a 66 del RLFPDPPP) y el Título Tercero Capítulo VII (artículos 77 y 83) y Capítulo VIII de la CUITF (artículos 85, 86, 87 y 88).
  - La segmentación de bases de datos (incluso con datos sensibles) y la generación de nuevas bases de datos puede dar lugar al incumplimiento de lo previsto en los artículos 7, 13 y 14 y de la LFPDPPP.
  - La asignación de una calificación crediticia al cliente a partir de información desactualizada puede dar lugar al incumplimiento de lo previsto en los artículos 7, 13 y 14 de la LFPDPPP.
  - La elaboración de perfiles mediante el uso de IA cuando dé lugar a percepciones erróneas en caso de que no exista una adecuada programación de algoritmos puede representar un incumplimiento a lo previsto en los artículos 7, 12, 13, 14 y 15 de la LFPDPPP.
  - La realización de tratamientos no consentidos ni informados al titular de forma previa al uso de técnicas de IA puede dar lugar al incumplimiento de lo previsto en los artículos 7, 12, 13, 14 y 15 de la LFPDPPP.

- El uso de técnicas de *big data* cuando no se prevean las medidas adecuadas para cumplir los principios de la LFPDPPP puede dar lugar al incumplimiento de los artículos 7, 12, 13, 14 y 15 de la LFPDPPP.
- El uso no consentido de cookies, web beacons y tecnologías similares puede dar lugar al incumplimiento de lo previsto en los artículos 7, 8, 14 y 15 de la LFPDPPP y el artículo 52 de las DCGCONDUSEF.
- El hecho de que terceros puedan a tener acceso a datos personales mediante el uso de APIs sin otorgar las garantías de seguridad previstas en la normatividad puede representar un incumplimiento a lo previsto en los artículos 7, 8, 9, 10, 12, 14, 19, 20 y 21 de la LFPDPPP, el Capítulo III del RLFPDPPP (artículos 57 a 66 del RLFPDPPP) y el artículo 76 de la LRITF.

- **Mecanismos de seguimiento y agrupaciones de operaciones.**
  - La debilidad en los controles para la adecuada identificación del cliente de acuerdo con información histórica o preexistente puede dar lugar al incumplimiento de los artículos 7, 11 y de la LFPDPPP y el Título Tercero Capítulo VII de la CUITF (artículos 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83 y 84).
  - La debilidad en los controles y procedimientos para conocimiento del cliente puede dar lugar al incumplimiento de lo previsto en los artículos 11 y 14 de la LFPDPPP, así como a lo previsto en el artículo 58 de la LRITF.
  - La falta de garantías para la adecuada protección y seguridad de los datos personales en infraestructura de cómputo en la nube gestionada por terceros puede dar lugar al incumplimiento de lo previsto en los artículos 14, 19, 20 y 21 de la LFPDPPP, artículos 50, 51 y 52 del RLFPDPPP, al Capítulo III del RLFPDPPP (artículos 57 a 66 del RLFPDPPP) y al Título Tercero Capítulos VI y VIII de la CUITF.
  - El hecho de que se usen asesores robóticos cuya programación no sea adecuada y afecte la facultad del titular para decidir de manera libre sobre el uso de sus datos y se le podría inducir a tomar decisiones erradas puede dar lugar al incumplimiento de lo previsto en los artículos 7 y 14 de la LFPDPPP.
  - La segmentación de bases de datos (incluso con datos sensibles) y la generación de nuevas bases de datos puede dar lugar al incumplimiento de lo previsto en los artículos 7, 13 y 14 y de la LFPDPPP.
  - La elaboración de perfiles mediante el uso de IA cuando dé lugar a percepciones erróneas en caso de que no exista una adecuada programación de algoritmos puede representar un incumplimiento a lo previsto en los artículos 7, 12, 13, 14 y 15 de la LFPDPPP.
  - La realización de tratamientos no consentidos ni informados al titular de forma previa al uso de técnicas de IA puede dar lugar al incumplimiento de lo previsto en los artículos 7, 12, 13, 14 y 15 de la LFPDPPP.
  - El uso de técnicas de *big data* cuando no se prevean las medidas adecuadas para cumplir los principios de la LFPDPPP puede dar lugar al incumplimiento de los artículos 7, 12, 13, 14 y 15 de la LFPDPPP.
  - El hecho de que terceros puedan a tener acceso a datos personales mediante el uso de APIs sin otorgar las garantías de seguridad previstas en la normatividad puede representar un incumplimiento a lo previsto en los artículos 7, 8, 9, 10, 12, 14, 19, 20 y 21 de la LFPDPPP, el Capítulo III del RLFPDPPP (artículos 57 a 66 del RLFPDPPP) y el artículo 76 de la LRITF.

- **Procesos que involucran el tratamiento de datos personales en las IFPE**
  - **Operaciones que realizan las IFPE (operaciones en moneda nacional, en moneda extranjera y sus características).**
    - La debilidad en los controles para la adecuada identificación del cliente de acuerdo con información histórica o preexistente puede dar lugar al incumplimiento de los

artículos 7, 11 y de la LFPDPPP y el Título Tercero Capítulo VII de la CUITF (artículos 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83 y 84).

- La elaboración de listas negras puede representar un incumplimiento a lo previsto en los artículos 7, 8, 9, 10, 12, 14,19, 20 y 21 de la LFPDPPP.
- La debilidad en los controles y procedimientos para conocimiento del cliente puede dar lugar al incumplimiento de lo previsto en los artículos 11 y 14 de la LFPDPPP, así como a lo previsto en el artículo 58 de la LRITF.
- La falta de garantías para la adecuada protección y seguridad de los datos personales en infraestructura de cómputo en la nube gestionada por terceros puede dar lugar al incumplimiento de lo previsto en los artículos 14, 19, 20 y 21 de la LFPDPPP, artículos 50, 51 y 52 del RLFPDPPP, al Capítulo III del RLFPDPPP (artículos 57 a 66 del RLFPDPPP) y al Título Tercero Capítulos VI y VIII de la CUITF.
- La segmentación de bases de datos (incluso con datos sensibles) y la generación de nuevas bases de datos puede dar lugar al incumplimiento de lo previsto en los artículos 7, 13 y 14 y de la LFPDPPP.
- El uso de tecnologías basadas en IoT en incumplimiento a los principios y deberes de la Ley puede representar un incumplimiento a los artículos 7, 12, 13, 14, 15, 19, 20 y 21 de la LFPDPPP, Capítulo III del RLFPDPPP (artículos 57 a 66 del RLFPDPPP) y al Título Tercero, Capítulo VI de la CUITF.
- El hecho de que terceros puedan a tener acceso a datos personales mediante el uso de APIs sin otorgar las garantías de seguridad previstas en la normatividad puede representar un incumplimiento a lo previsto en los artículos 7, 8, 9, 10, 12, 14, 19, 20 y 21 de la LFPDPPP, el Capítulo III del RLFPDPPP (artículos 57 a 66 del RLFPDPPP) y el artículo 76 de la LRITF.

- **Cierres de cuentas**
  - La debilidad en los controles para la adecuada identificación del cliente de acuerdo con información histórica o preexistente puede dar lugar al incumplimiento de los artículos 7, 11 y de la LFPDPPP y el Título Tercero Capítulo VII de la CUITF (artículos 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83 y 84).
  - La debilidad en los mecanismos de autenticación del cliente para la contratación de servicios y realización de operaciones en las ITF puede dar lugar al incumplimiento de lo previsto en los artículos 7, 8, 9, 10 y 12 y de la LFPDPPP, el Título Tercero Capítulo VII de la CUITF (artículos 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83 y 84) y el artículo 8 de las DCGCONDUSEF.
  - El hecho de que existan terceros que puedan tener acceso a datos personales del titular sin otorgar las garantías de seguridad previstas en la normatividad en servicios de verificación de la identidad puede representar un incumplimiento a lo previsto en los artículos 7, 8, 9, 10 y 12 y de la LFPDPPP y al Título Tercero Capítulo VII de la CUITF (artículos 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84 y 85).
  - La elaboración de listas negras puede representar un incumplimiento a lo previsto en los artículos 7, 8, 9, 10, 12, 14,19, 20 y 21 de la LFPDPPP.
  - La debilidad en los controles y procedimientos para conocimiento del cliente puede dar lugar al incumplimiento de lo previsto en los artículos 11 y 14 de la LFPDPPP, así como a lo previsto en el artículo 58 de la LRITF.
  - La falta de garantías para la adecuada protección y seguridad de los datos personales en infraestructura de cómputo en la nube gestionada por terceros puede dar lugar al incumplimiento de lo previsto en los artículos 14, 19, 20 y 21 de la LFPDPPP, artículos 50, 51 y 52 del RLFPDPPP, al Capítulo III del RLFPDPPP (artículos 57 a 66 del RLFPDPPP) y al Título Tercero Capítulos VI y VIII de la CUITF.
  - En los servicios de atención a clientes, el hecho de que existan terceros que puedan tener acceso a datos personales sin otorgar las garantías de seguridad y confidencialidad previstas en la normatividad puede dar lugar al incumplimiento

de lo previsto en los artículos 14, 19, 20 y 21 de la LFPDPPP, artículos 50, 51 y 52 del RLFPDPPP, el Capítulo III del RLFPDPPP (artículos 57 a 66 del RLFPDPPP) y el Título Tercero Capítulo VII (artículos 77 y 83) y Capítulo VIII de la CUITF (artículos 85, 86, 87 y 88).

- La obtención ilícita de datos de redes sociales puede dar lugar al incumplimiento de lo previsto en los artículos 7, 8, 9, 10 y 12 y de la LFPDPPP.
- El envío de publicidad no autorizada podría dar lugar al incumplimiento de lo previsto en los artículos 7, 8, 9 y 10 de la LFPDPPP.
- La segmentación de bases de datos (incluso con datos sensibles) y la generación de nuevas bases de datos puede dar lugar al incumplimiento de lo previsto en los artículos 7, 13 y 14 y de la LFPDPPP.
- La asignación de una calificación crediticia al cliente a partir de información desactualizada puede dar lugar al incumplimiento de lo previsto en los artículos 7, 13 y 14 de la LFPDPPP.
- La elaboración de perfiles mediante el uso de IA cuando dé lugar a percepciones erróneas en caso de que no exista una adecuada programación de algoritmos puede representar un incumplimiento a lo previsto en los artículos 7, 12, 13, 14 y 15 de la LFPDPPP.
- La realización de tratamientos no consentidos ni informados al titular de forma previa al uso de técnicas de IA puede dar lugar al incumplimiento de lo previsto en los artículos 7, 12, 13, 14 y 15 de la LFPDPPP.
- El uso de técnicas de *big data* cuando no se prevean las medidas adecuadas para cumplir los principios de la LFPDPPP puede dar lugar al incumplimiento de los artículos 7, 12, 13, 14 y 15 de la LFPDPPP.
- El uso no consentido de cookies, web beacons y tecnologías similares puede dar lugar al incumplimiento de lo previsto en los artículos 7, 8, 14 y 15 de la LFPDPPP y el artículo 52 de las DCGCONDUSEF.
- El hecho de que terceros puedan a tener acceso a datos personales mediante el uso de APIs sin otorgar las garantías de seguridad previstas en la normatividad puede representar un incumplimiento a lo previsto en los artículos 7, 8, 9, 10, 12, 14, 19, 20 y 21 de la LFPDPPP, el Capítulo III del RLFPDPPP (artículos 57 a 66 del RLFPDPPP) y el artículo 76 de la LRITF.

- **Requerimientos de información Banxico.**
  - La debilidad en los controles para la adecuada identificación del cliente de acuerdo con información histórica o preexistente puede dar lugar al incumplimiento de los artículos 7, 11 y de la LFPDPPP y el Título Tercero Capítulo VII de la CUITF (artículos 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83 y 84).
  - La elaboración de listas negras puede representar un incumplimiento a lo previsto en los artículos 7, 8, 9, 10, 12, 14,19, 20 y 21 de la LFPDPPP.
  - La debilidad en los controles y procedimientos para conocimiento del cliente puede dar lugar al incumplimiento de lo previsto en los artículos 11 y 14 de la LFPDPPP, así como a lo previsto en el artículo 58 de la LRITF.
  - La falta de garantías para la adecuada protección y seguridad de los datos personales en infraestructura de cómputo en la nube gestionada por terceros puede dar lugar al incumplimiento de lo previsto en los artículos 14, 19, 20 y 21 de la LFPDPPP, artículos 50, 51 y 52 del RLFPDPPP, al Capítulo III del RLFPDPPP (artículos 57 a 66 del RLFPDPPP) y al Título Tercero Capítulos VI y VIII de la CUITF.
  - La segmentación de bases de datos (incluso con datos sensibles) y la generación de nuevas bases de datos puede dar lugar al incumplimiento de lo previsto en los artículos 7, 13 y 14 y de la LFPDPPP.
  - La elaboración de perfiles mediante el uso de IA cuando dé lugar a percepciones erróneas en caso de que no exista una adecuada programación de algoritmos puede representar un incumplimiento a lo previsto en los artículos 7, 12, 13, 14 y 15 de la LFPDPPP.

- La realización de tratamientos no consentidos ni informados al titular de forma previa al uso de técnicas de IA puede dar lugar al incumplimiento de lo previsto en los artículos 7, 12, 13, 14 y 15 de la LFPDPPP.
- El uso de técnicas de *big data* cuando no se prevean las medidas adecuadas para cumplir los principios de la LFPDPPP puede dar lugar al incumplimiento de los artículos 7, 12, 13, 14 y 15 de la LFPDPPP.
- El hecho de que terceros puedan a tener acceso a datos personales mediante el uso de APIs sin otorgar las garantías de seguridad previstas en la normatividad puede representar un incumplimiento a lo previsto en los artículos 7, 8, 9, 10, 12, 14, 19, 20 y 21 de la LFPDPPP, el Capítulo III del RLFPDPPP (artículos 57 a 66 del RLFPDPPP) y el artículo 76 de la LRITF.

- **Procesos que involucran el tratamiento de datos personales en las IFC**
  - **Aspectos generales de las IFC**
    - La debilidad en los controles para la adecuada identificación del cliente de acuerdo con información histórica o preexistente puede dar lugar al incumplimiento de los artículos 7, 11 y de la LFPDPPP y el Título Tercero Capítulo VII de la CUITF (artículos 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83 y 84).
    - La debilidad en los mecanismos de autenticación del cliente para la contratación de servicios y realización de operaciones en las ITF puede dar lugar al incumplimiento de lo previsto en los artículos 7, 8, 9, 10 y 12 y de la LFPDPPP, el Título Tercero Capítulo VII de la CUITF (artículos 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83 y 84) y el artículo 8 de las DCGCONDUSEF.
    - La debilidad en los controles y procedimientos para conocimiento del cliente puede dar lugar al incumplimiento de lo previsto en los artículos 11 y 14 de la LFPDPPP, así como a lo previsto en el artículo 58 de la LRITF.
    - La falta de garantías para la adecuada protección y seguridad de los datos personales en infraestructura de cómputo en la nube gestionada por terceros puede dar lugar al incumplimiento de lo previsto en los artículos 14, 19, 20 y 21 de la LFPDPPP, artículos 50, 51 y 52 del RLFPDPPP, al Capítulo III del RLFPDPPP (artículos 57 a 66 del RLFPDPPP) y al Título Tercero Capítulos VI y VIII de la CUITF.
    - El hecho de que se usen asesores robóticos cuya programación no sea adecuada y afecte la facultad del titular para decidir de manera libre sobre el uso de sus datos y se le podría inducir a tomar decisiones erradas puede dar lugar al incumplimiento de lo previsto en los artículos 7 y 14 de la LFPDPPP.
    - En los servicios de atención a clientes, el hecho de que existan terceros que puedan tener acceso a datos personales sin otorgar las garantías de seguridad y confidencialidad previstas en la normatividad puede dar lugar al incumplimiento de lo previsto en los artículos 14, 19, 20 y 21 de la LFPDPPP, artículos 50, 51 y 52 del RLFPDPPP, el Capítulo III del RLFPDPPP (artículos 57 a 66 del RLFPDPPP) y el Título Tercero Capítulo VII (artículos 77 y 83) y Capítulo VIII de la CUITF (artículos 85, 86, 87 y 88).
    - El uso no consentido de cookies, web beacons y tecnologías similares puede dar lugar al incumplimiento de lo previsto en los artículos 7, 8, 14 y 15 de la LFPDPPP y el artículo 52 de las DCGCONDUSEF.

  - **Operaciones de las IFC**
    - La debilidad en los controles para la adecuada identificación del cliente de acuerdo con información histórica o preexistente puede dar lugar al incumplimiento de los artículos 7, 11 y de la LFPDPPP y el Título Tercero Capítulo VII de la CUITF (artículos 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83 y 84).

- La debilidad en los mecanismos de autenticación del cliente para la contratación de servicios y realización de operaciones en las ITF puede dar lugar al incumplimiento de lo previsto en los artículos 7, 8, 9, 10 y 12 y de la LFPDPPP, el Título Tercero Capítulo VII de la CUITF (artículos 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83 y 84) y el artículo 8 de las DCGCONDUSEF.
- El uso de servicios de verificación de identidad en los que terceros pueden tener acceso a datos personales sin otorgar las garantías de seguridad previstas en la normatividad, facilitar información que pueda estar desactualizada o no reflejar la situación real o actual del titular, incumplir la obligación de formalizar adecuadamente la relación jurídica conforme a lo que exige la LFPDPP (encargados) puede dar lugar al incumplimiento de lo previsto en los artículos 7, 8, 9, 10 y 12 y de la LFPDPPP y el Título Tercero Capítulo VII de la CUITF (artículos 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84 y 85)
- La elaboración de listas negras puede representar un incumplimiento a lo previsto en los artículos 7, 8, 9, 10, 12, 14,19, 20 y 21 de la LFPDPPP.
- La debilidad en los controles y procedimientos para conocimiento del cliente puede dar lugar al incumplimiento de lo previsto en los artículos 11 y 14 de la LFPDPPP, así como a lo previsto en el artículo 58 de la LRITF.
- La falta de garantías para la adecuada protección y seguridad de los datos personales en infraestructura de cómputo en la nube gestionada por terceros puede dar lugar al incumplimiento de lo previsto en los artículos 14, 19, 20 y 21 de la LFPDPPP, artículos 50, 51 y 52 del RLFPDPPP, al Capítulo III del RLFPDPPP (artículos 57 a 66 del RLFPDPPP) y al Título Tercero Capítulos VI y VIII de la CUITF.
- El uso de servicios de atención a clientes en los que terceros pueden tener acceso a datos personales sin otorgar las garantías de seguridad previstas en la normatividad, facilitar información que pueda estar desactualizada o no reflejar la situación real o actual del titular, incumplir la obligación de formalizar adecuadamente la relación jurídica conforme a lo que exige la LFPDPP (encargados) puede dar lugar al incumplimiento de lo previsto en los artículos 7, 8, 9, 10 y 12 y de la LFPDPPP y el Título Tercero Capítulo VII de la CUITF (artículos 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84 y 85)
- La obtención ilícita de datos de redes sociales puede dar lugar al incumplimiento de lo previsto en los artículos 7, 8, 9, 10 y 12 y de la LFPDPPP.
- La segmentación de bases de datos (incluso con datos sensibles) y la generación de nuevas bases de datos puede dar lugar al incumplimiento de lo previsto en los artículos 7, 13 y 14 y de la LFPDPPP.
- La asignación de una calificación crediticia al cliente a partir de información desactualizada puede dar lugar al incumplimiento de lo previsto en los artículos 7, 13 y 14 de la LFPDPPP.
- La elaboración de perfiles mediante el uso de IA cuando dé lugar a percepciones erróneas en caso de que no exista una adecuada programación de algoritmos puede representar un incumplimiento a lo previsto en los artículos 7, 12, 13, 14 y 15 de la LFPDPPP.
- La realización de tratamientos no consentidos ni informados al titular de forma previa al uso de técnicas de IA puede dar lugar al incumplimiento de lo previsto en los artículos 7, 12, 13, 14 y 15 de la LFPDPPP.
- El uso de técnicas de *big data* cuando no se prevean las medidas adecuadas para cumplir los principios de la LFPDPPP puede dar lugar al incumplimiento de los artículos 7, 12, 13, 14 y 15 de la LFPDPPP.
- El uso no consentido de cookies, web beacons y tecnologías similares puede dar lugar al incumplimiento de lo previsto en los artículos 7, 8, 14 y 15 de la LFPDPPP y el artículo 52 de las DCGCONDUSEF.
- El hecho de que terceros puedan a tener acceso a datos personales mediante el uso de APIs sin otorgar las garantías de seguridad previstas en la normatividad

puede representar un incumplimiento a lo previsto en los artículos 7, 8, 9, 10, 12, 14, 19, 20 y 21 de la LFPDPPP, el Capítulo III del RLFPDPPP (artículos 57 a 66 del RLFPDPPP) y el artículo 76 de la LRITF.

- **Procesos que involucran el tratamiento de datos personales en Open Banking**
  - La debilidad en los controles para la adecuada identificación del cliente de acuerdo con información histórica o preexistente puede dar lugar al incumplimiento de los artículos 7, 11 y de la LFPDPPP y el Título Tercero Capítulo VII de la CUITF (artículos 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83 y 84).
  - El uso de servicios de verificación de identidad en los que terceros pueden tener acceso a datos personales sin otorgar las garantías de seguridad previstas en la normatividad, facilitar información que pueda estar desactualizada o no reflejar la situación real o actual del titular, incumplir la obligación de formalizar adecuadamente la relación jurídica conforme a lo que exige la LFPDPP (encargados) puede dar lugar al incumplimiento de lo previsto en los artículos 7, 8, 9, 10 y 12 y de la LFPDPPP y el Título Tercero Capítulo VII de la CUITF (artículos 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84 y 85)
  - La elaboración de listas negras puede representar un incumplimiento a lo previsto en los artículos 7, 8, 9, 10, 12, 14,19, 20 y 21 de la LFPDPPP.
  - La debilidad en los controles y procedimientos para conocimiento del cliente puede dar lugar al incumplimiento de lo previsto en los artículos 11 y 14 de la LFPDPPP, así como a lo previsto en el artículo 58 de la LRITF.
  - La falta de garantías para la adecuada protección y seguridad de los datos personales en infraestructura de cómputo en la nube gestionada por terceros puede dar lugar al incumplimiento de lo previsto en los artículos 14, 19, 20 y 21 de la LFPDPPP, artículos 50, 51 y 52 del RLFPDPPP, al Capítulo III del RLFPDPPP (artículos 57 a 66 del RLFPDPPP) y al Título Tercero Capítulos VI y VIII de la CUITF.
  - La obtención ilícita de datos de redes sociales puede dar lugar al incumplimiento de lo previsto en los artículos 7, 8, 9, 10 y 12 y de la LFPDPPP.
  - El envío de publicidad no consentida puede significar un incumplimiento a los artículos 7, 8, 9 y 10 de la LFPDPPP, artículo 4 de las DCGMP y los artículos 11 y 44 de las DCGCONDUSEF.
  - La segmentación de bases de datos (incluso con datos sensibles) y la generación de nuevas bases de datos puede dar lugar al incumplimiento de lo previsto en los artículos 7, 13 y 14 y de la LFPDPPP.
  - La asignación de una calificación crediticia al cliente a partir de información desactualizada puede dar lugar al incumplimiento de lo previsto en los artículos 7, 13 y 14 de la LFPDPPP.
  - La elaboración de perfiles mediante el uso de IA cuando dé lugar a percepciones erróneas en caso de que no exista una adecuada programación de algoritmos puede representar un incumplimiento a lo previsto en los artículos 7, 12, 13, 14 y 15 de la LFPDPPP.
  - La realización de tratamientos no consentidos ni informados al titular de forma previa al uso de técnicas de IA puede dar lugar al incumplimiento de lo previsto en los artículos 7, 12, 13, 14 y 15 de la LFPDPPP.
  - El uso de técnicas de *big data* cuando no se prevean las medidas adecuadas para cumplir los principios de la LFPDPPP puede dar lugar al incumplimiento de los artículos 7, 12, 13, 14 y 15 de la LFPDPPP.
  - El uso no consentido de cookies, web beacons y tecnologías similares puede dar lugar al incumplimiento de lo previsto en los artículos 7, 8, 14 y 15 de la LFPDPPP y el artículo 52 de las DCGCONDUSEF.
  - El hecho de que terceros puedan a tener acceso a datos personales mediante el uso de APIs sin otorgar las garantías de seguridad previstas en la normatividad puede representar un incumplimiento a lo previsto en los artículos 7, 8, 9, 10, 12,

14, 19, 20 y 21 de la LFPDPPP, el Capítulo III del RLFPDPPP (artículos 57 a 66 del RLFPDPPP) y el artículo 76 de la LRITF.

IX. Conclusiones del Estudio

Como resultado de la elaboración del Entregable 1 se pueden sostener las siguientes conclusiones:

- Los datos personales son un activo imprescindible para el desarrollo de las actividades de las ITF.
- En este sentido, se identifican procesos que involucran el tratamiento de datos personales los cuales se dividen en cuatro rubros:
    - Procesos que involucran el tratamiento de datos personales de las IFPE.
    - Procesos que involucran el tratamiento de datos personales de las IFC.
- Respecto a los procesos generales que involucran el tratamiento de datos personales de las ITF (tanto IFC como IFPE), se identificaron los siguientes:
    - Alta de cliente.
    - PLD/CFT.
    - Obligación de conservar documentos.
    - Mecanismos de seguimiento y agrupaciones de operaciones.
    - *Open banking*
- Respecto a los procesos que involucran el tratamiento de datos personales de las IFPE, se identificaron los siguientes:
    - Operaciones que realizan las IFPE.
    - Cierre de cuentas.
    - Requerimientos de información Banxico.
- Respecto a los procesos que involucran el tratamiento de datos personales de las IFC, se identificaron los siguientes:
    - Aspectos generales de las IFC.
    - Operaciones de las IFC.

Como resultado de la elaboración del Entregable 2 se pueden sostener las siguientes conclusiones:

- Respecto a la parte dos del segundo entregable: "Identificación de tratamientos de datos personales" se dio continuación al entregable 1 identificando los tratamientos de datos personales de las ITF, considerando el ciclo de vida de aquellos proceso y subprocesos del entregable 1.
- Derivado del análisis se realizaron tablas analíticas que identificaban: el tipo de titular, los datos personales, la forma de obtención, almacenamiento, usos, tratamientos (identificando las finalidades primarias y secundarias), tipo de consentimiento, divulgación/otros sujetos intervinientes, bloqueo, supresión y actores involucrados.
- Respecto a lo anterior se identificó en algunos tratamientos de datos personales el uso de tecnologías de análisis masivo de datos (*big data*) e inteligencia artificial (*machine learning y deep learning*) y los resultantes de la combinación de dichas tecnologías y datos. En particular, se identificó el tratamiento de Big Data para mejorar los productos y/o servicios ofrecidos y/o conocer necesidades del cliente.
- Asimismo, se identificó que en varios tratamientos de datos personales aplicaba la excepción del artículo 10, fracción I, de la LFPDPPP. Esto debido a que las ITF en cumplimiento a la LRITF y disposiciones secundarias actualizan dicha disposición normativa. Sin embargo, para el tratamiento de datos personales para la publicidad, mercadotecnia, elaboración de perfiles, monetización de datos personales, comercialización de espacios digitales, elaboración de estadísticas, entre otros identificados será necesario que la ITF obtenga el consentimiento expreso del titular.
- Existen múltiples tratamientos de datos personales en las ITF relacionados con los distintos procesos y subprocesos en los que se produce el tratamiento de datos personales.

- Existen diversos tratamientos de alto riesgo relacionados con el uso de datos sensibles, elaboración de perfiles, conocimiento del cliente y uso de tecnologías de IA y big data.
- Existen diversos tratamientos de datos que pueden dar lugar al incumplimiento de la normatividad aplicable en materia de protección de datos personales, así como a aquella específica aplicable a las ITF.

X. Glosario

Activos Virtuales. Representación del valor registrada electrónicamente y utilizada entre el público como medio de pago para todo tipo de actos jurídicos y cuya transferencia únicamente pueda llevarse a cabo a través de Medios Electrónicos. En ningún caso se entenderá como activo virtual la moneda de curso legal en territorio nacional, las divisas, ni cualquier otro activo denominado en moneda de curso legal o en divisas. Solo se considerarán Activos Virtuales aquellos que sean determinados por el BANXICO conforme a lo dispuesto por el artículo 30 de la LRITF.

Archivo o Registro. Conjunto de datos y documentos que se conserven o almacenen en formato impreso o en medios electrónicos, ópticos o de cualquier otra tecnología, siempre y cuando, en estos últimos medios, se asegure que la información se haya mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta, teniendo como fin integrar, conservar y evidenciar las Operaciones, actividades y servicios de las ITF.

Autoridad Financiera. cualquiera de las Comisiones Supervisoras, al BANXICO o a la SHCP, según sus ámbitos de competencia.

Beneficiario. Persona designada por el Cliente de la ITF, para que, en caso de fallecimiento de dicho Cliente, tal persona ejerza ante la ITF los derechos derivados de la cuenta, contrato u Operación, de acuerdo con lo dispuesto por la LRITF.

Cliente. Persona física o moral que contrata o realiza alguna Operación con una ITF, así como la que contrata o utiliza los servicios de Entidades Financieras previstos en esta Ley o de sociedades autorizadas para operar con Modelos Novedosos.

CNBV. Comisión Nacional Bancaria y de Valores.

CNSF. Comisión Nacional de Seguros y Fianzas.

Comisiones Supervisoras. CNBV, CONSAR, CNSF y CONDUSEF, respecto a sus ámbitos de competencia.

Comité Interinstitucional. Instancia colegiada integrada por servidores públicos de la SHCP, del BANXICO y de la CNBV a que se refiere la LRITF.

CONDUSEF. Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros.

CONSAR. Comisión Nacional del Sistema de Ahorro para el Retiro.

Consorcio. Conjunto de personas morales vinculadas entre sí por una o más personas físicas que integrando un Grupo de Personas, tengan el Control de las primeras.

Control. La capacidad de imponer, directa o indirectamente, decisiones en las asambleas generales de accionistas, de socios u órganos equivalentes, o nombrar o destituir a la mayoría de los consejeros, administradores o sus equivalentes de una persona moral; o el mantener la titularidad de derechos que permitan, directa o indirectamente, ejercer el voto respecto de más del cincuenta por ciento del capital social de la sociedad, o el dirigir, directa o indirectamente, la administración, la estrategia o las principales políticas de la sociedad, ya sea a través de la propiedad de Valores o por cualquier otro acto jurídico.

Directivo Relevante. Director General de las ITF, así como a las personas físicas que, ocupando un empleo, cargo o comisión en aquellas o en las personas morales que tengan el Control de dichas ITF o que sean controladas por estas últimas, adopten decisiones que trasciendan de forma significativa en la situación administrativa, financiera, operacional o jurídica de la propia ITF o del Grupo Empresarial al que esta pertenezca, sin que queden comprendidos dentro de esta definición los consejeros de las ITF.

Entidades Financieras. Las sociedades controladoras y subcontroladoras de grupos financieros, instituciones de crédito, casas de bolsa, bolsas de valores, sociedades operadoras de fondos de inversión, sociedades distribuidoras de acciones de fondos de inversión, uniones de crédito, organizaciones auxiliares del crédito, casas de cambio, sociedades financieras de objeto múltiple, sociedades financieras populares, sociedades financieras comunitarias con niveles de operaciones I a IV, organismos de integración financiera rural, sociedades cooperativas de ahorro y préstamo con niveles de operación I a IV, instituciones para el depósito de valores, contrapartes centrales de valores, instituciones calificadoras de valores, sociedades de información crediticia, instituciones de seguros, instituciones de fianzas, sociedades mutualistas de seguros, administradoras de fondos para el retiro, así como otras instituciones y fideicomisos públicos que realicen actividades respecto de las cuales la CNBV, la CNSF o la CONSAR ejerzan facultades de supervisión.

Estado de Cuenta o Estado de Operación. Estado de Cuenta es el documento emitido por las ITF que informa sobre el estado que guardan las operaciones y servicios contratados por los Usuarios con las mismas.

Estado de Operación. Es el documento que las IFC entreguen a los inversionistas.

Financiamiento Colectivo de Capital. La operación de financiamiento colectivo mediante la cual los Solicitantes obtienen recursos por parte de los Inversionistas a cambio de títulos representativos de su capital social.

Financiamiento Colectivo de Copropiedad o Regalías. La operación de financiamiento colectivo mediante la cual los Inversionistas y Solicitantes celebran entre ellos asociaciones en participación o cualquier otro tipo de convenio por el cual los Inversionistas adquieren una parte alícuota o participación en un bien presente o futuro, o en los ingresos, utilidades, regalías o pérdidas que se obtengan de la realización de una o más actividades o de los proyectos de los Solicitantes.

Financiamiento Colectivo de Deuda de Préstamos Empresariales entre Personas. La operación de financiamiento colectivo, en la que los Solicitantes son personas morales o personas físicas con actividad empresarial y los Inversionistas realizan aportaciones: a) Con el fin de que los Solicitantes reciban un préstamo o crédito para financiar sus actividades, quedando obligados al pago del principal y, en su caso, accesorios a cada uno de los Inversionistas en proporción a sus aportaciones en la Operación; b) Con el objeto de efectuar una operación de arrendamiento financiero, en la que se adquiere un activo a nombre de los Inversionistas o de las instituciones de financiamiento colectivo a nombre propio, pero en representación de estos, y se da en arrendamiento financiero al Solicitante. Para efectos de la operación de arrendamiento financiero, se estará a lo dispuesto por la Ley General de Títulos y Operaciones de Crédito; c) Con el fin de celebrar una operación de factoraje financiero, en la que adquieren parte de algún derecho de crédito que el Solicitante tenga a su favor, quedando el Solicitante como obligado solidario de su deudor, sin que dicho derecho derive de préstamos, créditos o mutuos que el Solicitante previamente haya otorgado. Para efectos de la operación de factoraje financiero, se estará a lo dispuesto por la Ley General de Títulos y Operaciones de Crédito.

Financiamiento Colectivo de Deuda de Préstamos Personales entre Personas. La operación de financiamiento colectivo en la que el Solicitante es una persona física que obtiene en préstamo los recursos aportados por los Inversionistas, quedando obligado al pago del principal, y en su caso accesorios, a cada uno de los Inversionistas en proporción a sus aportaciones en la Operación.

Financiamiento Colectivo de Deuda para el Desarrollo Inmobiliario. La operación de financiamiento colectivo que tiene por objeto que los Inversionistas otorguen un préstamo o crédito a los Solicitantes destinado al financiamiento de actividades de desarrollo inmobiliario quedando obligados al pago del principal y, en su caso, accesorios a cada uno de los Inversionistas en proporción a sus aportaciones en la Operación.

Firma Autógrafa Digitalizada. Los rasgos o datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al suscriptor u originador de la instrucción de alguna Operación o servicio financiero e indicar que el firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa.

Firma Electrónica Avanzada. Certificado digital con el que deben contar las personas físicas y morales, conforme a lo dispuesto por el artículo 17-D del Código Fiscal de la Federación.

Fondo de Capital Privado. Vehículo de inversión, fideicomiso, mandato, comisión o figuras similares constituidos bajo las leyes mexicanas o extranjeras, cuyo fin sea invertir en el capital de sociedades no listadas en las bolsas de valores al momento de la inversión para promover su desarrollo y otorgarles financiamiento.

Grado de Riesgo. Clasificación que la ITF otorgue a sus Clientes con base en la evaluación de su Riesgo conforme al Capítulo II del Título Tercero de las DCGA58.

Grupo de Personas. Personas que tengan acuerdos, de cualquier naturaleza, para tomar decisiones en un mismo sentido. Se presume, salvo prueba en contrario, que constituyen un Grupo de Personas: a) Las personas que tengan parentesco por consanguinidad, afinidad o civil hasta el cuarto grado, los cónyuges, la concubina y el concubinario, y b) Las sociedades que formen parte de un mismo Consorcio o Grupo Empresarial y la persona o conjunto de personas que tengan el Control de dichas sociedades.

Grupo Empresarial. Conjunto de personas morales organizadas bajo esquemas de participación directa o indirecta del capital social, en las que una misma sociedad mantiene el Control de dichas personas morales, incluyendo a los grupos financieros constituidos conforme a la Ley para Regular las Agrupaciones Financieras.

Infraestructura Tecnológica. Infraestructura de cómputo, redes de telecomunicaciones, sistemas operativos, bases de datos, software y aplicaciones que utilizan las ITF, las sociedades autorizadas para operar con Modelos Novedosos y las entidades financieras para soportar sus operaciones;

Institución de Financiamiento Colectivo. Aquella persona moral autorizada por la CNBV que, de manera habitual y profesional, lleve a cabo actividades destinadas a poner en contacto a personas del público en general, con el fin de que entre ellas se otorguen financiamientos mediante alguna de las Operaciones a que se refiere el artículo 16 de la LRITF, a través de aplicaciones informáticas, interfaces, páginas de Internet o cualquier otro medio de comunicación electrónica o digital.

Institución de Fondos de Pago Electrónico. Aquella persona moral autorizada por la CNBV que, de manera habitual y profesional, preste los servicios de emisión, administración, redención y transmisión de fondos de pago electrónico, por medio de cualquiera de los actos a que hace referencia el artículo 22 de la LRITF, a través de aplicaciones informáticas, interfaces, páginas de Internet o cualquier otro medio de comunicación electrónica o digital.

ITF. Las instituciones de tecnología financiera reguladas en la LRITF, las cuales son las instituciones de financiamiento colectivo y las instituciones de fondos de pago electrónico;

Lista de Personas Bloqueadas. Lista a que se refiere el artículo 58, párrafo séptimo de la LRITF.

Manual de Cumplimiento. Documento a que se refiere el artículo 82 de las DCGA58.

Medio de Disposición. Los que se refiere la fracción XII del artículo 3 de la LTOSF.

Medios Electrónicos. Los dispositivos tecnológicos para el procesamiento, impresión, despliegue, conservación y, en su caso, modificación de información.

Modelo Novedoso. Aquel que para la prestación de servicios financieros utilice herramientas o medios tecnológicos con modalidades distintas a las existentes en el mercado al momento en que se otorgue la autorización temporal en términos de la LRITF,

Obtener los datos personales de forma directa de su titular. Acto en el cual el propio titular proporciona los datos personales por algún medio que permite su entrega directa al responsable, entre ellos, medios electrónicos, ópticos, sonoros, visuales o cualquier otra tecnología, como correo postal, internet o vía telefónica, entre otros.

Obtener los datos personales de forma indirecta. Acto en el cual el responsable obtiene los datos personales sin que el titular se los haya proporcionado de forma personal o directa, como por ejemplo a través de una fuente de acceso público o una transferencia.

Obtener los datos personales de forma personal de su titular. Acto en el cual el titular proporciona los datos personales al responsable o a la persona física designada por el responsable, con la presencia física de ambos.

Operación Interna Preocupante. La Operación, actividad, conducta o comportamiento de cualquiera de los miembros del consejo de administración, administrador único, accionistas, socios, propietarios o dueños, directivos, funcionarios, apoderados y empleados de la ITF de que se trate con independencia del régimen o instrumento legal utilizado para contratar sus servicios, que, por sus características, pudiera contravenir, vulnerar o evadir la aplicación de lo dispuesto por la LRITF o las DCGA58, o aquella que, por cualquier otra causa, resulte dubitativa para las ITF por considerar que pudiese favorecer o no alertar sobre la actualización de los supuestos previstos en los artículos 139 Quáter o 400 Bis del CPF.

Operación Inusual. La Operación, actividad, conducta o comportamiento de un Cliente que no concuerde con los antecedentes o actividad conocida por la ITF o declarada a esta, o con el perfil transaccional inicial o habitual de dicho Cliente, en función al origen o destino de los recursos, así como al monto, frecuencia, tipo o naturaleza de la Operación de que se trate, sin que exista una justificación razonable para dicha Operación, actividad, conducta o comportamiento, o bien, aquella Operación, actividad, conducta o comportamiento que un Cliente realice o pretenda realizar con la ITF de que se trate en la que, por cualquier causa, esta considere que los recursos correspondientes pudieran ubicarse en alguno de los supuestos previstos en los artículos 139 Quáter o 400 Bis del CPF.

Operación Relevante. La Operación que se realice con los billetes y las monedas metálicas de curso legal en los Estados Unidos Mexicanos o en cualquier otro país, por un monto igual o superior al equivalente en moneda nacional a cinco mil dólares de los Estados Unidos de América. Para efectos del cálculo del importe de las Operaciones a su equivalente en moneda nacional, se considerará el tipo de cambio para solventar obligaciones denominadas en moneda extranjera pagaderas en la República Mexicana, que publique el BANXICO en el DOF, el día hábil bancario inmediato anterior a la fecha en que se realice la Operación.

Operaciones. Los actos de carácter financiero o de pagos a que se refiere la LRITF, que una ITF puede ofrecer o realizar con el público o, que a través de ellas se realizan entre Clientes, en términos de la LRITF.

Persona Políticamente Expuesta. Aquel individuo que desempeña o ha desempeñado funciones públicas destacadas en un país extranjero o en territorio nacional. Se considerarán como Personas

Políticamente Expuestas, entre otras, a los jefes de estado o de gobierno, líderes políticos, funcionarios gubernamentales, judiciales o militares de alta jerarquía, altos ejecutivos de empresas estatales, funcionarios o miembros importantes de partidos políticos y organizaciones internacionales.

Personas Relacionadas. Las personas que respecto de una ITF, se ubiquen en alguno de los supuestos siguientes: a) Las personas físicas o morales que mantengan, directa o indirectamente, la propiedad del uno por ciento o más de los títulos representativos del capital de una ITF, de acuerdo con el registro de socios más reciente que lleve la ITF respectiva; b) El administrador único o los miembros del consejo de administración de la ITF, así como los auditores o comisarios, sus funcionarios o empleados o las personas distintas a estos que con su firma puedan obligar a la ITF de que se trate; c) Los cónyuges y las personas que tengan parentesco hasta el segundo grado con las personas señaladas en los incisos anteriores; d) Las personas morales, así como sus consejeros y funcionarios, respecto de las cuales la ITF mantenga, directa o indirectamente, la propiedad del diez por ciento o más de los títulos representativos de su capital; e) Las personas morales en las que cualquiera de las personas señaladas en los incisos anteriores, así como los funcionarios, empleados, auditores externos y comisarios de la ITF, los ascendientes y descendientes en primer grado, así como sus cónyuges, mantengan, directa o indirectamente, la propiedad del diez por ciento o más de los títulos representativos de su capital, y f) Las personas morales respecto de las cuales los funcionarios, auditores externos, miembros del comité de auditoría y comisarios de las ITF sean consejeros o administradores u ocupen cualquiera de los tres primeros niveles jerárquicos en dichas personas morales.

Plataforma: Las aplicaciones informáticas, interfaces páginas de Internet o cualquier otro medio de comunicación electrónica o digital que las ITF utilicen para operar con sus Usuarios.

Poder de Mando. La capacidad de hecho de influir de manera decisiva en los acuerdos adoptados en las asambleas de accionistas o socios o sesiones del consejo de administración o de directores o en la gestión, conducción y ejecución de los negocios de la ITF o de las personas morales que esta tenga el Control. Se presume que tienen Poder de Mando en una ITF, salvo prueba en contrario, las personas que se ubiquen en cualquiera de los supuestos siguientes: a) Los accionistas que tengan el Control; b) Las personas físicas que tengan vínculos con la ITF o las personas morales que integran el Grupo Empresarial o Consorcio al que aquélla pertenezca, a través de cargos vitalicios, honoríficos o con cualquier otro título análogo o semejante a los anteriores; c) Las personas que hayan transmitido el Control de la ITF bajo cualquier título y de manera gratuita o a un valor inferior al de mercado o contable, en favor de personas con las que tengan parentesco por consanguinidad, afinidad o civil hasta el cuarto grado, el cónyuge, la concubina o el concubinario, y d) Las personas que instruyan a consejeros o Directivos Relevantes de la ITF, la toma de decisiones o la ejecución de operaciones en la propia ITF o en las personas morales que esta tenga el Control.

Riesgo. La probabilidad de que las ITF puedan ser utilizadas por sus Clientes para realizar actos u Operaciones a través de los cuales se pudiesen actualizar los supuestos previstos en los artículos 139 Quáter o 400 Bis del CPF.

UMA. Unidad de Medida y Actualización cuyo valor equivalente en pesos se determina de conformidad con la Ley para Determinar el Valor de la Unidad de Medida y Actualización.

Valores. Las acciones, partes sociales, obligaciones, bonos, títulos opcionales, certificados, pagarés, letras de cambio y demás títulos de crédito, nominados o innominados, que se emitan en serie o en masa y representen el capital social de una persona moral o una parte de este, una parte alícuota de un bien o la participación en un crédito colectivo o cualquier derecho de crédito individual, en los términos de las leyes nacionales o extranjeras aplicables.