RECOMENDACIONES PARA EL TRATAMIENTO DE DATOS PERSONALES Y CUMPLIR CON EL DEBER DE SEGURIDAD PARA INSTITUCIONES DE TECNOLOGÍA FINANCIERA (ITF)

inai

DIRECTORIO

Blanca Lilia Ibarra Cadena
Comisionada Presidente

Francisco Javier Acuña Llamas
Comisionado

Adrián Alcalá Méndez
Comisionado

Norma Julieta Del Rio Venegas
Comisionada

Oscar Mauricio Guerra Ford
Comisionado

Rosendoevgeni Monterrey Chepov
Comisionado

Josefina Román Vergara
Comisionada

Av. Insurgentes Sur 3211, Col. Insurgentes Cuicuilco, C.P. 04530, Alcaldía Coyoacán, Ciudad de México.

Edición Febrero 2021.

CONTENIDO

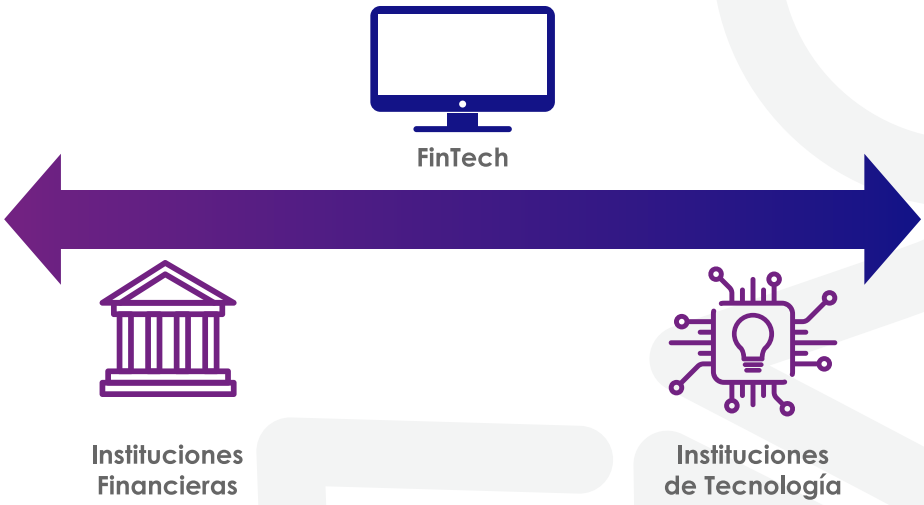
IR AL CONTENIDO

ANTECEDENTES

¿QUÉ ES FINTECH?

La palabra FinTech es un término compuesto que surge de la contracción de las primeras silabas de las palabras en inglés.

FINance + TECHnology = FinTech



FinTech hace referencia a una industria conformada por empresas que usan tecnologías como: internet, teléfonos inteligentes, algoritmos inteligentes, Big Data, inteligencia artificial (IA), interfaces de programación de aplicaciones y aplicaciones móviles, para ofrecer servicios financieros a un menor costo de manera eficiente, ágil, cómoda y confiable.

IR AL CONTENIDO

De acuerdo con la Comisión Nacional Bancaria y de Valores,[1] FinTech es la innovación tecnológica aplicada a los servicios financieros que busca ofrecer servicios de manera eficiente, ágil y cómoda mediante plataformas como aplicaciones, páginas web y redes sociales.

¿Qué es FinTech?

CONTEXTO FINTECH

1. FinTech nace como una combinación de tecnología y servicios financieros con el fin de aportar nuevas soluciones en ese campo (servicios financieros).
2. Este concepto implica la innovación tecnológica en los servicios financieros.
3. Se utiliza para referirse a los servicios que otorgan las instituciones financieras, ya sean productos o servicios que operan y se desarrollan a través de la tecnología.
4. Se compone de compañías que utilizan la tecnología que hacen la operación de los sistemas financieros más eficientes.
5. Se relaciona con las pequeñas empresas del sector tecnológico que generan una disrupción en los sectores de transmisores de pago, otorgamiento de créditos, financiamiento y el manejo de activos, en contraste con el sector financiero.

1 https://www.gob.mx/cnbv/acciones-y-programas/sector-fintech

IR AL CONTENIDO

En América Latina los nuevos actores en el mercado de servicios financieros están innovando los modelos tradicionales y han traído cambios en la regulación de otros países, como se puede ver en México, Brasil y Colombia. Fuera del contexto de las actualizaciones legales para la operación de servicios financieros a través de empresas FinTech, emprendedores de la región latinoamericana están aprovechando su capacidad de llevar al mercado productos y servicios, para satisfacer la creciente demanda de servicios financieros que se ha detonado por el incremento de usuarios con acceso a equipos Smartphone. De acuerdo al Banco Mundial, se estima que el 81,6%[2] de la población adulta en 18 países de América Latina y el Caribe tiene acceso a un Smartphone, mientras que solo el 53,5%[3] de la población adulta tiene acceso a una cuenta bancaria en una institución financiera.

La oportunidad que representa la brecha entre estos dos indicadores, el cada vez más fácil acceso a tecnologías disruptivas sobre las tecnologías utilizadas en el sector y el surgimiento de una cultura emprendedora y experta en el uso de las tecnologías, han convertido a América Latina en un semillero de emprendimientos.

ES	
Analítica de Datos y Big Data	19.14 %
Cómputo en la nube	8.56%
Blockchain y Criptoactivos	6.30%
Hardware	0.25%
Internet de las Cosas	1.26%
Inteligencia Artificial	8.06%
Tecnología Movil y apps	20.65%
APIs y código abierto	16.62%
Otro	8.82%
Sharing Economy	10.33%
TOTAL	100%

2 World Bank (2017). The Global Findex Database 2017. https://globalfindex.worldbank.org/#data_sec_focus

3 World Bank (2018). The Little Data Book on Financial Inclusion 2018. https://openknowledge.worldbank.org/handle/10986/29654

IR AL CONTENIDO

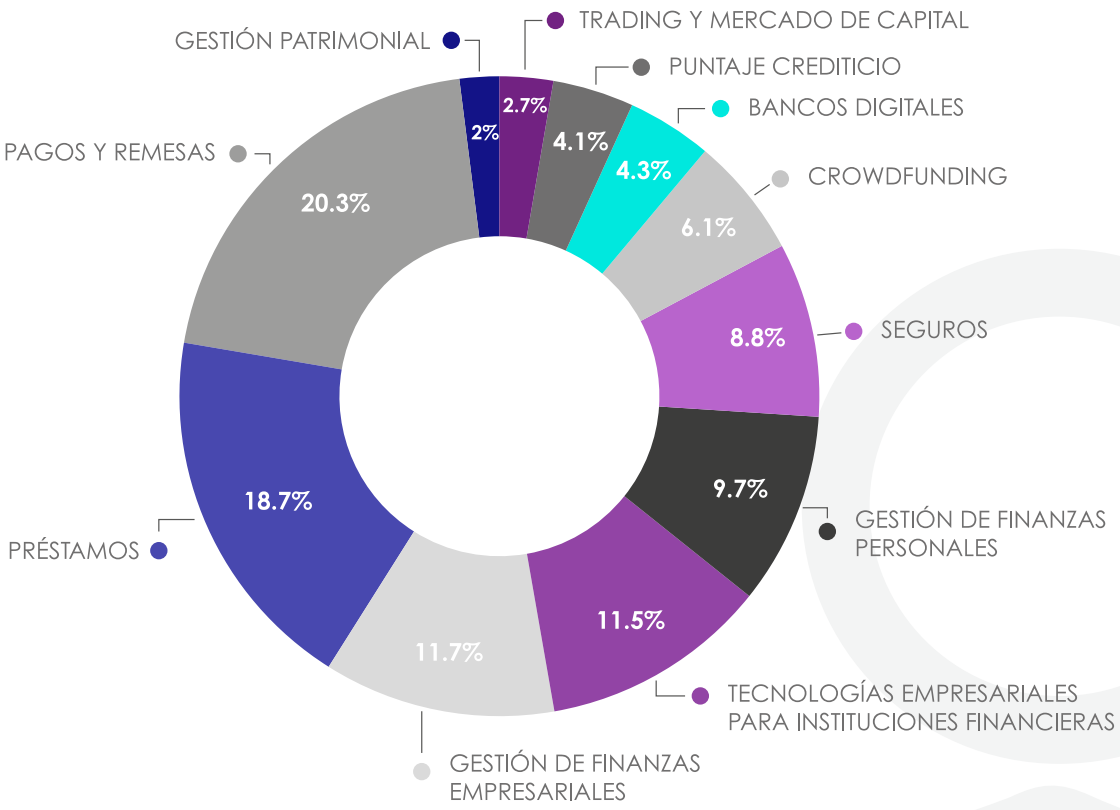
México es el segundo país que registra más emprendimientos FinTech en la región, solo por detrás de Brasil. Sin embargo, el reto de inclusión financiera es claro y se ve aún más acentuado en México, debido a la baja tasa de penetración que tienen los productos y servicios ofrecidos por la banca tradicional.

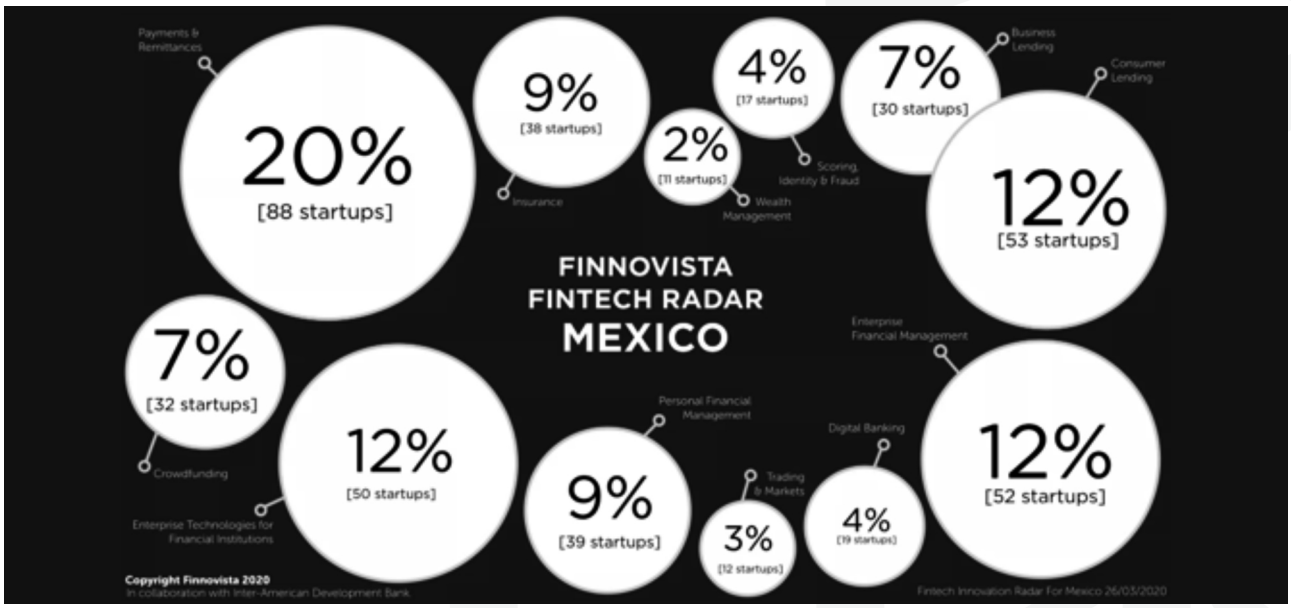
Las razones son diversas y muy debatidas en el ecosistema financiero, pero basta observar el elevado costo del capital y las altas comisiones de servicios financieros básicos para entender que la banca tradicional no había tenido suficientes incentivos para competir en el segmento de población no-bancarizada, sobre todo por cargar con costos unitarios de infraestructura tecnológica y financiera que no justificaban la creación de productos y servicios financieros para la base de la pirámide.

Esto cambió con la llegada de las soluciones FinTech al mercado, pues el bajo costo de adquisición de clientes y el incremento en la eficiencia de procesos bancarios a través de plataformas digitales reveló el potencial de la inclusión financiera. Según los datos del recientemente publicado Finnovista FinTech Radar México edición 2020[4], en México únicamente se han identificado 441 Startups FinTech, de las cuales el 24,4% ofrecen soluciones de pagos digitales (wallets, agregadores de pagos digitales, puntos de venta móviles, etc.) y un 17,8% satisfacen la demanda de crédito digital a usuarios (11%) y pymes (6,8%).

4 Finnovista Fintech Radar México edición 2020. https://www.finnovista.com/el-numero-de-startups-FinTech-en-mexico-crecio-mas-de-un-14-en-un-ano-hasta-las-441/

IR AL CONTENIDO





IR AL CONTENIDO

De acuerdo con el mapeo del ecosistema FinTech que hace Finnovista desde 2016, en México se ha producido un incremento medio anual del número de startups FinTech del 23% año con año. Esto contrasta significativamente con las perspectivas macroeconómicas negativas que aquejan a otros sectores de la economía. La ventaja competitiva de las unidades económicas del sector FinTech es saber adaptarse a los cambios usando la tecnología para generar valor al cliente final, así como la cultura de confianza y colaboración que se ha forjado en los últimos años en el ecosistema.

De acuerdo con la Asociación FinTech México, las empresas de dicho segmento ofrecen distintos tipos de servicios financieros y operan dentro de mercados variados; considerándose como servicios más relevantes los siguientes:

- **Medios de pago y transferencias.** Las plataformas de pagos, comercio electrónico y transferencias internacionales.
- **Infraestructura para servicios financieros.** Evaluación de clientes y perfiles de riesgo, prevención de fraudes, verificación de identidades, APIs bancarias, agregadores de medios de pago, big data & analytics, inteligencia de negocios, ciberseguridad y contratación electrónica.
- **Originación digital de créditos.** Son empresas que ofrecen productos de crédito a través de plataformas electrónicas.
- **Soluciones financieras para empresas.** Software para contabilidad e infraestructuras de facturación y gestión financiera.
- **Finanzas personales y asesoría financiera.** Administración de finanzas personales, comparadores y distribuidores de productos financieros, educación financiera, asesores automatizados y planeación financiera.
- **Mercados financieros.** Servicios digitales de intermediación de valores, instrumentos financieros y divisas.
- **Crowdfunding.** La Asociación de Plataformas de Fondeo Colectivo de México (AFICO) refiere que se trata de un modelo de formación de capital y participación de mercado, en el que las necesidades de financiamiento de proyectos se transmiten a una comunidad a través de una plataforma digital y se obtiene apoyo de inversionistas, fondeadores y donantes.
- **InsurTech.** Tecnología aplicada a la prestación de servicios en el sector asegurador.

IR AL CONTENIDO

- **Criptomonedas y blockchain.** Desarrolladores de soluciones basadas en el blockchain, intermediarios y mercados de activos digitales.
- **Entidades financieras disruptivas.** Bancos u otras entidades financieras 100% digitales.

Además, se pueden distinguir los siguientes segmentos de aplicación de la tecnología al sector financiero: el de FinTech en general ya mencionado, el regulatorio ("RegTech", con soluciones tecnológicas —cómputo en la nube o big data— que facilitan el cumplimiento de la regulación), y el de seguros ("InsurTech", con soluciones tecnológicas especializadas y enfocadas al sector asegurador).

IR AL CONTENIDO

MARCO NORMATIVO PARA FINTECH EN MÉXICO

En México, a fin de regular este tipo de Instituciones de Tecnología Financiera, el 9 de marzo de 2018, se publicó en el Diario Oficial de la Federación (DOF) la Ley para Regular las Instituciones de Tecnología Financiera (ITF);[5] Ley conocida como "Ley FinTech", la cual regula un nuevo tipo de entidad financiera en el sistema financiero mexicano.

FinTech implica tecnología y servicios financieros por lo que No debe confundirse FinTech con ITF.

Toda ITF es FinTech, pero no todo FinTech es ITF, salvo que se determine que le ampara un modelo novedoso y posteriormente se constituya como ITF.

Respecto al marco normativo que regula la operación de las ITF, a fin de fortalecerse, se publicaron los siguientes instrumentos normativos para dicho sector:

Las ***Disposiciones de carácter general aplicables a las Instituciones de Tecnología Financiera***[6] publicadas en el DOF el 10 de septiembre de 2018, modificadas el 25 de marzo de 2019, las ***Disposiciones de carácter general de la CONDUSEF en materia de transparencia y sanas practicas a las Instituciones de Tecnología Financiera***[7] publicadas en el DOF el 9 de julio de 2019 y finalmente, la ***Circular 2/2020 dirigida a las Sociedades de Información Crediticia y Cámaras de Compensación, relativa a las disposiciones de carácter general a que se refiere el artículo 76 de la Ley para Regular Instituciones de Tecnología Financiera, aplicables a las sociedades***

5 https://www.dof.gob.mx/nota_detalle.php?codigo=5515623&fecha=09/03/2018

6 https://www.cnbv.gob.mx/Normatividad/Disposiciones%20de%20carácter%20general%20aplicables%20a%20las%20instituciones%20de%20tecnolog%C3%ADa%20financiera.pdf

7 http://www.dof.gob.mx/nota_detalle.php?codigo=5565233&fecha=09/07/2019

IR AL CONTENIDO

de información crediticia y cámaras de compensación en materia de interfaces de programación de aplicaciones informáticas estandarizadas[8] publicada en el DOF el 10 de marzo de 2020.

De esta manera, respecto al marco normativo para las ITF en México, podemos mencionar que se cuenta con una regulación robusta que permite identificar las actividades de las ITF. Para estas Recomendaciones, se realizó un análisis exhaustivo de los documentos antes mencionados a fin de identificar puntualmente aquellas actividades que conlleven un tratamiento de datos personales.

Como se mencionó, conforme a la normativa mexicana se instituye el término de Instituciones de Tecnología Financiera, término que será utilizado para el presente documento, abordando las definiciones reguladas en la Ley comentada.

Primero, debemos tener identificadas a las Autoridades Financieras que participan en el ecosistema de las Instituciones de Tecnología Financiera:

Autoridades Financieras

- Banco de México.
- Comisión Nacional Bancaria y de Valores (CNBV).
- Comisión Nacional de Seguros y Fianzas (CNSF).
- Comisión Nacional del Sistema de Ahorro para el Retiro (CONSAR).
- Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF).
- Secretaria de Hacienda y Crédito Público (SHCP).

Con la Ley FinTech el Gobierno Federal no garantiza ni respalda el dinero de los clientes de las FinTech, aunque si autoriza el funcionamiento y supervisa a aquellas FinTech que en sus actividades realicen servicios financieros.

8 https://www.dof.gob.mx/nota_detalle.php?codigo=5588824&fecha=10/03/2020

IR AL CONTENIDO

Es así que, de acuerdo a la Ley FinTech existen dos tipos de Instituciones las cuales serán autorizadas, reguladas y supervisadas por la SHCP, el Banco de México y la CNBV, buscando que las ITF cuenten con un buen funcionamiento; seguridad de la información; protección de los intereses del público, y de prevención de lavado de dinero (PLD) y financiamiento al terrorismo (FT).

LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES

Con la entrada en vigor de la normativa para regular las Instituciones de Tecnología Financiera (Ley FinTech o LRITF), las Instituciones de Financiamiento Colectivo (IFC) y de Fondos de Pago Electrónico (IFPE) son reconocidas como personas físicas o morales de carácter privado, las cuales llevan a cabo diversos tratamientos de datos personales; por lo cual, son sujetos obligados a cumplir con la normativa en protección de datos personales conforme a lo que se establece en la Ley Federal de Protección de Datos Personales en Posesión de Particulares y su Reglamento.

En este contexto, las personas físicas o morales privadas, que traten datos personales en sus actividades, deberán cumplir una serie de obligaciones con objeto de garantizar a los titulares el derecho a la protección de su información personal.

IR AL CONTENIDO

INSTITUCIONES DE FONDO DE PAGO ELECTRÓNICO (IFPE)

¿QUÉ SON LAS IFPE?

Se refiere a aquellas instituciones (personas morales autorizadas por la CNBV) que presten servicios al público de manera habitual y profesional, consistentes en la emisión, administración, redención y transmisión de fondos de pago electrónico, por medio de los actos señalados en el artículo 22, de la Ley FinTech, a través de aplicaciones informáticas, interfaces, páginas de internet o cualquier otro medio de comunicación electrónica o digital.

Es decir, las IFPE son todas aquellas instituciones que llevan a cabo servicios consistentes en la emisión, administración, rendición y transmisión de fondos de pago electrónico (e-money) a través de cualquier medio de comunicación electrónica o digital, mediante cuentas a nombre de los usuarios que mantiene la propia Institución en su plataforma, así como entregar por instrucciones de sus clientes, cantidades de dinero o de activos virtuales equivalentes al saldo del monedero respectivo. La Institución tiene la obligación de reconocer los cargos y abonos que se hagan a dichas cuentas por instrucciones de sus clientes.

TIPOS DE CLIENTES DE UNA IFPE

- **Usuario**, para las IFPE solo se puede identificar a los usuarios, los cuales son aquellas personas que se registren a una plataforma IFPE y realicen alguna de las operaciones aprobadas para este tipo de instituciones.

IR AL CONTENIDO

ACTIVIDADES DE LA IFPE

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

- Emitir, comercializar o administrar instrumentos para la disposición de fondos de pago electrónico.
- Prestar el servicio de transmisión de dinero.
- Prestar servicios relacionados con las redes de medios de disposición.
- Procesar la información relacionada con los servicios de pago correspondientes a los fondos de pago electrónico o a cualquier otro medio de pago.
- 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.
- Realizar operaciones con activos virtuales, en términos de lo dispuesto en la LRITF.
- 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.
- Emitir valores por cuenta propia.
- Constituir depósitos a la vista o a plazo en entidades financieras autorizadas para recibirlos.
- Adquirir o arrendar los bienes muebles e inmuebles necesarios para la realización de su objeto y enajenarlos cuando corresponda.
- 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.
- Comprar, vender o, en general, transmitir activos virtuales por cuenta propia o de sus Clientes.
- Realizar los actos necesarios para la consecución de su objeto social.

IR AL CONTENIDO

TIPOS DE SERVICIOS REALIZADOS

- Abrir y llevar cuentas de fondos de pago electrónico por cada cliente. [MXN, moneda extranjera o Activos Virtuales (AV)]
- Transferencias de fondos de pago electrónico entre sus clientes. Transferencias de dinero en MXN, moneda extranjera o AV.
- Entregar una cantidad de dinero o AV equivalente a la misma cantidad de fondos de pago electrónico.
- Mantener actualizado el registro de cuentas de fondos de pago electrónico por cada cliente.

PROCESOS PROPIOS DE LAS IFPE

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 de los clientes.
3. Realizar transferencias de dinero en moneda nacional o, sujeto a la previa autorización del Banco de México, en moneda extranjera o de activos virtuales, mediante los respectivos abonos y cargos entre cuentas de sus propios clientes o 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 los clientes, así como modificarlo en relación con el ingreso, transferencia y retiro de fondos de pago electrónico.

IR AL CONTENIDO

INSTITUCIONES DE FINANCIAMIENTO COLECTIVO O CROWDFUNDING FINANCIERO (IFC)

¿QUÉ SON LAS IFC?

Se refiere a aquellas instituciones (personas morales autorizadas por la CNBV) que lleven 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 las operaciones de financiamiento colectivo de deuda, de capital o 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.

Es decir, aquellas Instituciones que realizan actividades consistentes en el desarrollo y operación de plataformas que permiten poner en contacto a personas del público en general con el fin de que entre ellas se otorguen financiamientos, a través de cualquier medio de comunicación electrónica o digital, a fin de que los solicitantes se alleguen de recursos para realizar un proyecto, y los inversionistas obtengan, a través de la plataforma, ya sea (i) acciones de la empresa que lleva a cabo el proyecto (capital), (ii) los rendimientos que resulten del préstamo (deuda) o bien y (iii) una participación en las ganancias o pérdidas del proyecto (copropiedad o regalías).

TIPOS DE CLIENTES DE UNA IFC

- **Inversionistas,** se consideran inversionistas a las personas físicas o morales que aporten recursos a los solicitantes.[9]
- **Solicitantes,** se consideran solicitantes a las personas físicas o morales que hubieren requerido tales recursos a través de la IFC.[10]

9 Art. 16 Ley para Regular las Instituciones de Tecnología Financiera

10 Art. 16 Ley para Regular las Instituciones de Tecnología Financiera

IR AL CONTENIDO

ACTIVIDADES QUE PUEDE REALIZAR UN CLIENTE DE UNA IFC

- **Financiamiento colectivo de deuda,** con el fin de que los inversionistas otorguen prestamos, 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.
- **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 perdidas que se obtengan de la realización de una o más actividades o de los proyectos de un solicitante.

TIPOS DE FINANCIAMIENTOS COLECTIVOS

- **Deuda:** Inversionistas otorgan préstamos, créditos, mutuos o cualquier tipo de financiamiento causante de un pasivo directo o contingente a los solicitantes.
- **Capital:** Inversionistas compran o adquieren títulos representativos del capital social de las personas morales solicitantes.
- **Copropiedad o regalía:** Inversionistas y solicitantes celebran entre ellos asociaciones en participación o cualquier convenio por el cual el inversionista adquiere 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.

ACTIVIDADES PROPIAS DE LAS IFC

De acuerdo con la Ley FinTech, 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 dicha Ley:

IR AL CONTENIDO

- 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.

IR AL CONTENIDO

PROCESOS DE LAS IFC

1. **Recibir, procesar y publicar las solicitudes de Operaciones de Financiamiento Colectivo.**
   Para realizar la publicación de las solicitudes de Operaciones de Financiamiento Colectivo las IFC deberán indicar en sus plataformas la información y documentación soporte necesaria para que los interesados se den de alta ya sea como inversionistas o como solicitantes.

2. **Establecer y dar a conocer a los posibles inversionistas de forma clara e indubitable a través de los medios que son utilizados para operar.**
   Una vez que la Institución ha detectado si se trata de un usuario solicitante o un usuario inversionista, deberá indicar las actividades que se realizan para contar con los siguientes elementos:
   a. Criterios de selección de solicitantes.
   b. Criterios de selección de los proyectos objeto de financiamiento.
   c. Información y documentación a analizar.
   d. Mecanismos de verificación de la veracidad de la información y documentación.
   e. El riesgo de los solicitantes.
   f. El riesgo de los proyectos.
   g. Incluir indicadores generales sobre el comportamiento de pago y desempeño de los solicitantes.
   h. Presentar una metodología de evaluación y calificación de los solicitantes y proyectos.

3. **Obtener de los inversionistas una constancia electrónica de que conocen los riesgos a que esta sujeta su inversión en la Institución.**
   Las Instituciones deberán contar con una constancia electrónica en la que el inversionista es consiente sobre los riesgos a los que se sujeta su inversión.

4. **Habilitar canales de comunicación electrónicos.**
   La Institución deberá proporcionar canales de comunicación electrónicos para que inversionistas y solicitantes puedan relacionarse.

IR AL CONTENIDO

5. **Proporcionar medios necesarios para formalizar operaciones entre solicitantes e inversionistas.**
   Finalmente, la Institución debe formalizar los contratos entre los inversionistas y solicitantes mediante su plataforma, en la cual se indicará la manera en la que se realizaran los pagos y depósitos derivados del financiamiento.

IR AL CONTENIDO

MODELOS NOVEDOSOS

Adicionalmente, la Ley FinTech contempla la figura conocida como Modelos novedosos.

Esta figura se refiere a 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 establecida en el Título IV de la Ley FinTech.

Un modelo novedoso permite que cualquier sociedad de nacionalidad mexicana, o en su caso, cualquier entidad financiera, pueda estar en condiciones de solicitar una autorización temporal para ofrecer servicios financieros usando medios tecnológicos y otros modelos innovadores que no existan en el mercado cuando la sociedad considere que la regulación financiera existente crea un impedimento para la prestación de estos servicios.

Las sociedades autorizadas como Modelos Novedosos podrán operar de forma condicionada durante un plazo limitado (máximo: dos años para empresas, y un año para entidades financieras, en ambos casos con posibilidad de una prórroga).

La autorización temporal se otorga a:

- **Entidades reguladas.**
  Por alguna Comisión o Banco de México, que pretendan llevar a cabo temporalmente operaciones o actividades de su objeto social a través de Modelos Novedosos cuando en su realización se requiera de excepciones o condicionantes a lo contenido en la regulación secundaria, por un plazo de un año, prorrogable a un año más.

- **Personas morales distintas a las entidades reguladas.**
  Autorizada temporalmente para que mediante un Modelo Novedoso lleve a cabo alguna actividad cuya realización requiere de un autorización, registro o concesión de conformidad con las leyes financieras, por un plazo no mayor a dos años, prorrogable a un año más.

IR AL CONTENIDO

Las Sociedades Autorizadas deberán:

- Identificar y evaluar el Riesgo al que están expuestas, previo al lanzamiento del producto o servicio de que se trate a través de Modelos Novedosos.
- Presentar el resultado de la mencionada evaluación a la Comisión Supervisora competente junto con su solicitud de autorización.

Adicionalmente, deberán ajustarse a las Disposiciones, conforme a los casos, forma, términos, plazos, condiciones y excepciones que en la autorización respectiva señale la Comisión Supervisora o el Banco de México, previa opinión de la SHCP.

IR AL CONTENIDO

ASPECTOS GENERALES RESPECTO AL TRATAMIENTO DE DATOS PERSONALES

Antes de comenzar con recomendaciones generales dirigidas a las ITF respecto al tratamiento de datos personales, es necesario definir algunos conceptos en materia de protección de datos personales.

¿QUÉ SON LOS DATOS PERSONALES?

Es cualquier información concerniente a una persona física identificada o identificable, como puede ser el nombre, los apellidos, la dirección postal, el número de teléfono, la dirección de correo electrónico, el número de pasaporte, una fotografía, la Clave Única de Registro de Población (CURP) o cualquier otra información que permita identificar o haga identificable al titular de los datos.

Los datos personales pueden estar expresados en forma numérica, alfabética, gráfica, fotográfica, acústica o en cualquier otra modalidad.

Se considera que una persona es identificable cuando su identidad puede determinarse mediante los datos personales de que se traten.

Es importante considerar que si los datos personales son objeto del procedimiento de disociación, ya no es posible asociarlos a su titular, ni permitir su identificación.

¿QUÉ SON LOS DATOS PERSONALES SENSIBLES?

Son datos personales que afectan la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen o conlleve un riesgo grave para éste, como, por ejemplo, el origen racial o étnico; estado de salud (pasado, presente y futuro); información genética; creencias religiosas, filosóficas y morales; afiliación sindical; opiniones políticas y preferencia sexual.

IR AL CONTENIDO

¿QUÉ ES EL TRATAMIENTO DE DATOS PERSONALES?

Tratar datos personales es un concepto amplio, ya que incluye la obtención, uso, almacenamiento y divulgación de los datos personales.

El uso de los datos personales abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

Por ejemplo, un responsable del tratamiento puede obtener datos personales de una persona física, a través de un formulario en papel, almacenarlos en el disco duro de una máquina o en la nube, utilizarlos para sus actividades cotidianas, comunicarlos con el encargado que le brinda un servicio y suprimirlos cuando haya concluido la finalidad para la cual los obtuvo. Todas estas acciones se consideran tratamiento de datos personales.

¿QUIÉN ES EL TITULAR DE LOS DATOS PERSONALES?

Es la persona física a quien corresponden y pertenecen los datos personales que son objeto de tratamiento. Por tanto, es el dueño de los datos personales, aunque éstos estén en posesión de un tercero para su tratamiento. Por ejemplo, el titular de los datos personales contenidos en un expediente laboral, es el trabajador a quien refieren esos datos.

¿QUIÉN ES EL RESPONSABLE?

Es la persona física o moral de carácter privado que decide sobre el tratamiento de los datos personales, es decir, la que establece las finalidades del tratamiento o el uso que se le dará a los datos personales, el tipo de datos que se requieren, a quién y para qué se comparten, cómo se obtienen, almacenan y suprimen los datos personales, y en qué casos se divulgarán, entre otros factores de decisión.

El responsable del tratamiento puede ser, por ejemplo, una empresa o persona moral, un emprendedor, un doctor, un abogado, un contador, una organización de la sociedad civil, una escuela o colegio, el patronato de un museo, una universidad

IR AL CONTENIDO

privada o una fundación, o cualquier otra persona física o moral que decida sobre el tratamiento de los datos personales para el desarrollo de su actividad.

¿QUIÉN ES EL ENCARGADO?

Es la persona física o moral, ajena a la organización del responsable del tratamiento, que trata los datos personales a nombre y por cuenta del responsable. A diferencia de este último, el encargado no decide sobre el tratamiento de los datos personales, sino que lo realiza siguiendo las instrucciones del responsable.

Por ejemplo, se considera encargado a la empresa que fue contratada por el responsable para administrar su nómina o prestarle el servicio de call center. También sería encargada del tratamiento una empresa que ofrece servicios de cómputo en la nube y que almacena bases de datos de un responsable, o bien, aquélla que contrató el responsable para la destrucción de sus documentos.

Si el encargado tratara los datos personales para finalidades propias, de forma tal que decidiera sobre dicho tratamiento, se convertiría en un responsable, con todas sus obligaciones, y estaría sujeto a las sanciones previstas por la LFPDPPP, en caso de incumplimiento.

CUMPLIMIENTO DEL MARCO NORMATIVO EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

El objeto de la LFPDPPP es la protección de los datos personales en posesión de los particulares con la finalidad de regular el tratamiento legítimo, controlado e informado de los datos personales, para garantizar así la privacidad de las personas y la protección de su información personal.

Este tratamiento legítimo, controlado e informado de los datos personales se basa en principios y deberes que los responsables deben observar en el tratamiento de los datos personales. En concreto, los principios y los deberes de seguridad y confidencialidad se convierten en obligaciones concretas para el responsable, que tiene que cumplir, así como hacer cumplir, en cada una de las fases del tratamiento.

IR AL CONTENIDO

Ahora bien, para cumplir con estas obligaciones, en primer lugar, resulta importante que el responsable conozca cómo se lleva a cabo el tratamiento de datos personales dentro de su organización. Para ello, es necesario que realice un diagnóstico que le permita identificar cuál es el flujo que, al interior de su organización, se sigue con respecto al tratamiento de los datos personales, desde que éstos se recaban hasta que los mismos se eliminan de sus bases de datos.

En específico, para las ITF, se realizan las siguientes recomendaciones agrupadas por actividades.

IR AL CONTENIDO

RECOMENDACIONES RESPECTO AL TRATAMIENTO DE DATOS PERSONALES QUE REALIZAN LAS ITF POR PROCESOS IDENTIFICADOS

Como se mencionó, la Ley FinTech al regular las IFC involucra directamente a las IFPE y a las IFC, por lo que, hay actividades que realizan dichas Instituciones que son generales y que involucran un tratamiento de datos personales, así mismo, cada tipo de Institución cuenta con tratamientos particulares para ofrecer sus servicios, al respecto, conforme a lo dispuesto en la Ley y al seguimiento de tramites de clientes ante una ITF se pueden agrupar en actividades para su análisis particular.

De acuerdo con cada actividad que se ha identificado, es posible observar que existe un tratamiento continuo de datos personales, los cuales deben ser comunicados a quienes utilizan ITF para realizar cualquier actividad de las que se han enlistado anteriormente. Para tal efecto, se enlistan las actividades y se acompañan de una serie de recomendaciones que las ITF deberán observar a fin de proteger la información personal de sus clientes.

ALTA DE CLIENTES

Descripción del proceso.
El proceso de alta de cliente inicia cuando una persona quiere acceder a uno de los productos que ofrecen las ITF, es así que cualquier usuario al contratar cualquier tipo de servicio que ofrece una ITF debe de considerar que el primer paso que va a realizar es el de darse de alta a una plataforma, en dicha plataforma cada prestador de servicios puede solicitar diversos datos personales para atender la solicitud de un servicio, dependiendo del servicio que el cliente quiera contratar, por lo que, los usuarios al darse de alta deberán de llenar un expediente que contempla al menos los siguientes datos:

IR AL CONTENIDO

- Nombre, apellidos, género, fecha de nacimiento, entidad y país de nacimiento, nacionalidad, clave de elector, domicilio actualizado, ocupación, CURP, firma autógrafa digitalizada, teléfono, correo, CLABE bancaria.

Adicionalmente, la plataforma a utilizar le solicitara fotografías de documentos oficiales que permitan cotejar que la información proporcionada en el registro es correspondiente a la que aparece en el documento oficial.

Por lo que, se entiende que las ITF implementan mediante aplicaciones web plataformas que permiten al cliente potencial introducir directamente sus datos personales mediante un formulario, además de incluir la opción de cargar imágenes o archivos en diversos formatos directamente desde el dispositivo en el que se esta registrando el usuario, por lo que la ITF, deberá observar las siguientes recomendaciones para un tratamiento legitimo de los datos personales que recaba.

Recomendación.
Primero, las ITF deberán de contar con un inventario de datos personales por actividad o producto ofrecido, dicho inventario de datos personales le permitirá identificar que datos personales son necesarios para prestar sus servicios, de esta manera, estará observando el **principio de proporcionalidad**, es decir tratar sólo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron.

Respecto al mecanismo de obtención de los datos personales, las ITF deberán atender al **deber de seguridad**, es decir, deberán implementar medidas de seguridad físicas, tecnológicas y administrativas que permitan al usuario entablar una comunicación segura o cifrada a través del dispositivo con el que se conecta con la plataforma que la ITF le facilita sus productos.

IDENTIFICACIÓN DE CLIENTES

Descripción del proceso.
Una vez que un cliente ingreso su información y anexó los documentos solicitados por la ITF a fin de comprobar que los datos proporcionados se encuentran legitimados en un documento oficial, las ITF, comienzan a realizar un perfila-

IR AL CONTENIDO

miento de usuario, es decir, dependiendo del servicio que se vaya a contratar, las ITF realizan un proceso en el que verifican el historial crediticio del usuario que se registro y hacen un perfil para dar a conocer, en caso de que el usuario solicite un financiamiento, el comportamiento crediticio de los solicitantes.

Recomendación.
La identificación de clientes se refiere en si misma a una tratamiento de datos personales, ya que, partir de los datos recolectados, las ITF aplican algoritmos que buscan categorizar a los clientes y determinar si son candidatos para otorgarles alguno de los diversos servicios que ofrecen, es por eso, que en este paso, las ITF deberán realizar un tratamiento prudente de la información de sus clientes a fin de no causar algún tipo de discriminación sobre sus condiciones financieras de sus clientes, o bien, generar nuevos mecanismos en los que se soliciten más datos personales de los que fueron solicitados de inicio para pasar por un nuevo tratamiento que pretenda garantizar el acceso al servicio solicitado por el cliente.

TRANSFERENCIAS DE DATOS PERSONALES PARA EL OTORGAMIENTO DE UN SERVICIO

Descripción del proceso.
Como se ha mencionado, las ITF ofrecen servicios en los cuales fungen como canales de comunicación para diversos usuarios a través de sus plataformas, derivado de esta actividad, las ITF deberán informar puntualmente a sus clientes sobre las transferencias de datos personales realizadas por el cumplimiento de las actividades por la cuales fueron contratadas, particularmente las IFC son las que deben observar lo correspondiente a las transferencias de datos personales ya que, de acuerdo a la naturaleza de sus funciones, este tipo de instituciones envían datos personales que han aceptado a posibles inversores, por lo que, esta información que se comparte debe de observar lo que corresponde a las comunicaciones de datos personales, específicamente a las transferencias de datos.

IR AL CONTENIDO

iNTERCAMBIO DE INFORMACIÓN EN ITF

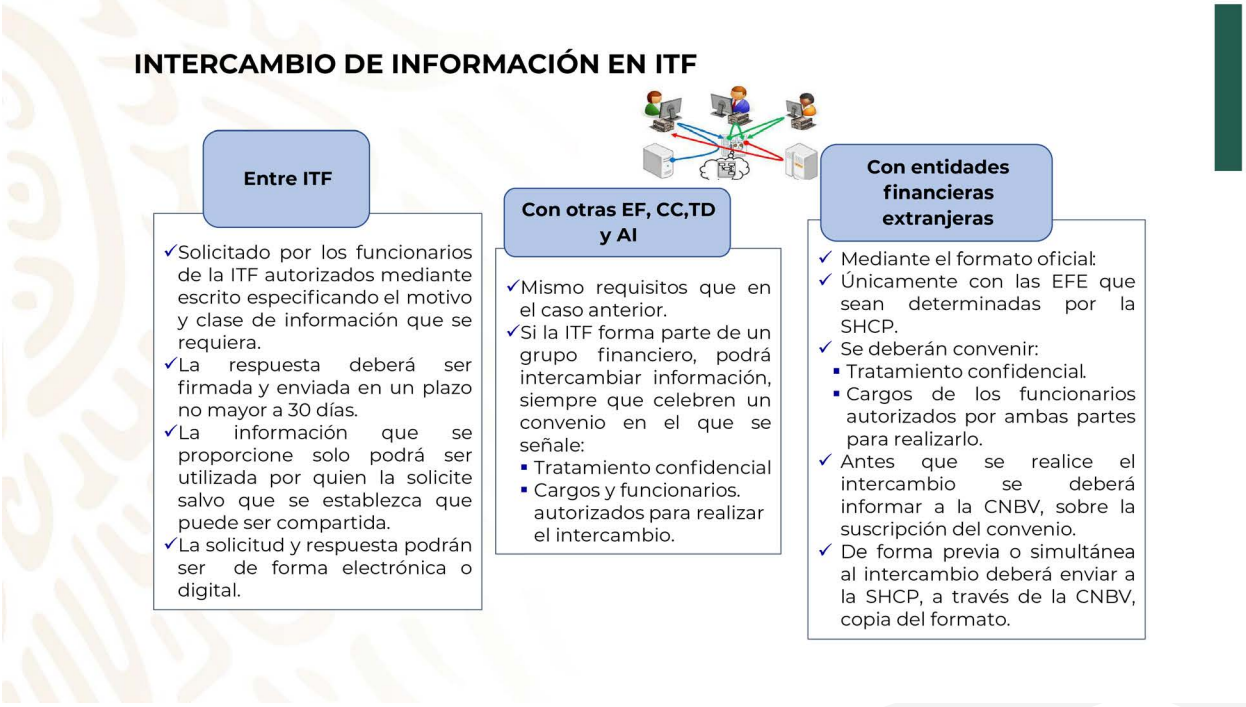


Imagen obtenida de: https://www.cnbv.gob.mx/PrevencionDeLavadoDeDinero/Documents/2-1_Conocimientos_tecnicos_en_PLD-FT_Leyes_y_disposiciones.pdf

Recomendación.

Como recomendación principal se considera que cualquier comunicación que pueda darse entre los diversos clientes de las Instituciones sea realizada únicamente mediante la plataforma de la ITF, por lo que, las ITF deberán de habilitar canales de comunicación para actividades específicas derivadas de sus servicios y que involucren la atención personalizada con sus clientes.

Adicionalmente, las ITF deben de analizar las transferencias de datos personales que realizan en el cumplimento de sus funciones, tomando en cuenta lo siguiente.

IR AL CONTENIDO

¿Qué son las transferencias de datos personales?
Se denomina transferencia de datos personales a la comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento, (por ejemplo las comunicaciones al interior de la organización del responsable, como las que se realizan entre el personal) o del encargado.

La comunicación puede producirse, entre otros actos, por el envío de los datos al tercero, por el hecho de mostrarlos en una pantalla o permitirle el acceso a los mismos.

La transferencia de datos personales puede ser nacional o internacional, según el destino de los datos personales.

¿A quién corresponde acreditar que se cumplió con las obligaciones en materia de transferencia?
Para poder demostrar que la transferencia de datos personales, sea nacional o internacional, se realizó conforme a lo que establece la normativa en materia de protección de datos personales, la carga de la prueba recae tanto en el responsable que transfiere como en el receptor de los datos personales.

Obligaciones ligadas a las transferencias.
El responsable tiene las siguientes obligaciones en torno a las transferencias de datos personales:

1. El consentimiento del titular para las transferencias, salvo en el caso de que aplique algunas de las excepciones previstas en el artículo 37 de la LFPDPPP.
2. Informar las transferencias en el aviso de privacidad y, en su caso, incluir la cláusula correspondiente.
3. Limitar las transferencias a las finalidades y condiciones establecidas en el aviso de privacidad y que, en su caso, hayan sido consentidas por el titular.
4. Comunicar a los terceros receptores de los datos personales el aviso de privacidad, con las finalidades a las que el titular sujetó su tratamiento.
5. Demostrar que la trasferencia se hizo conforme a la normativa en materia de protección de datos personales.

IR AL CONTENIDO

6. Cuando la transferencia sea nacional, formalizarla mediante instrumento jurídico que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.
7. Cuando el responsable recibe los datos personales, tratarlo exclusivamente para las finalidades y bajo las condiciones informadas en el aviso de privacidad y, en su caso, consentidas por el titular.
8. Cuando se trate de transferencias internacionales, transferir los datos exclusivamente cuando el tercero receptor asuma las mismas obligaciones a las que se encuentra sujeto el responsable que transfiere los datos personales.
9. Cuando se trate de transferencias internacionales, formalizar la transferencia mediante instrumento jurídico que prevea al menos las mismas obligaciones para el tercero receptor, a las que se encuentra sujeto el responsable que transfiere los datos personales, así como las condiciones en las que el titular consintió el tratamiento de sus datos personales.

¿Cuáles son las condiciones generales para las transferencias?
Para que un responsable pueda transferir los datos personales, dentro o fuera de México, es necesario que:

- Se informe al titular en el aviso de privacidad correspondiente lo siguiente: que la transferencia se podrá realizar, a quién se transferirán los datos y para qué fines. Asimismo, en caso de requerirse, el aviso de privacidad deberá contener una cláusula para que el titular consienta o no la transferencia.
- El titular haya otorgado su consentimiento para que la transferencia se realice, salvo los casos de excepción previstos en el artículo 37 de la LFPDPPP.
- El objeto de la transferencia se deberá limitar a la finalidad y condiciones informadas en el aviso de privacidad, y que hayan sido consentidas por el titular, en su caso.

Finalmente, es necesario que las ITF cuenten con mecanismos que permitan garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, el presente Reglamento y demás normativa aplicable, podrá ser la exis-

IR AL CONTENIDO

tencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la LFPDPPP, su Reglamento y demás normativa aplicable.

MONITOREO DE LAS OPERACIONES DE SUS CLIENTES

Descripción del proceso.
Esta actividad se refiere a que las ITF deberán crear un seguimiento de cualquier acción que realicen sus clientes en sus plataformas, estas actividades pueden incluir metadatos y datos de otros usuarios que no necesariamente corresponden a clientes de una ITF, por lo que, se recomienda que se revisen los datos necesarios, solicitados en los reportes que deben presentar las ITF a la autoridad bancaria, a fin de identificar los datos personales de los clientes y terceros que se involucran por cada operación que se realiza, misma que quedara documentada y en su momento será reportada a las autoridades financieras correspondientes.

Recomendaciones.
Respecto al monitoreo de operaciones de clientes, las ITF deberán conservar y reportar solo aquellos datos que por ley están obligados a presentar a las autoridades correspondientes, asimismo, se recomienda evitar realizar tratamientos de datos personales adicionales a los datos que se generan del monitoreo de operaciones con fines comerciales o de cualquier tratamiento adicional no reportado u ofrecido desde la contratación del servicio que da origen al tratamiento de los datos del cliente y que se encuentre debidamente reportado en el aviso de privacidad correspondiente.

CLASIFICACIÓN DE CLIENTES POR GRADO DE RIESGO

Descripción del proceso.
Para establecer el Grado de Riesgo, las ITF 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.

IR AL CONTENIDO

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.[11]

Recomendación.
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 ITF 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.[12]

Las ITF 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 ITF, deberán modificar las políticas, criterios, medidas y procedimientos correspondientes. Las modificaciones serán revisadas por las ITF en un plazo no mayor a 12 meses contados a partir de que la propia ITF cuente con los resultados de su implementación.[13]

11 Art. 3 de las 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 https://www.dof.gob.mx/nota_detalle.php?codigo=5537449&fecha=10/09/2018. (DCGA58).

12 Art. 4 de las 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 https://www.dof.gob.mx/nota_detalle.php?codigo=5537449&fecha=10/09/20188.

13 Art. 5 de las 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 https://www.dof.gob.mx/nota_detalle.php?codigo=5537449&fecha=10/09/2018.

IR AL CONTENIDO

De la clasificación del Grado de Riesgo del Cliente.

El modelo de evaluación de Riesgo con el que deberán contar las ITF, 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.[14]

Las ITF 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 riesgo es diferente al establecido en un inicio. Entre mas alto sea el grado del riesgo, la frecuencia de evaluación incrementa.[15]

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.
   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.

14 Art. 29 de las 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 https://www.dof.gob.mx/nota_detalle.php?codigo=5537449&fecha=10/09/2018.

15 Art. 30 de las 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 https://www.dof.gob.mx/nota_detalle.php?codigo=5537449&fecha=10/09/2018.

IR AL CONTENIDO

II. Características transaccionales:
   a. Tipo y numero de productos y servicios contratados.
   b. Volumen en número y monto de Operaciones.
   c. Frecuencia de Operaciones.
   e. Número de contrapartes.
   f. Origen y destino de los recursos.
   g. Instrumento monetario.
   h. Tipo de moneda.[16]

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.
   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. (art 70)
c. Personas políticamente expuestas extranjeras.[17]

Las ITF, 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.

16 Art. 31 de las 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 https://www.dof.gob.mx/nota_detalle.php?codigo=5537449&fecha=10/09/2018.

17 Art. 33 de las 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 https://www.dof.gob.mx/nota_detalle.php?codigo=5537449&fecha=10/09/2018.

IR AL CONTENIDO

b. Obtener, en su caso, los datos señalados en el Título Tercero, Capítulo I de las 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[18] (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.

Personas Políticamente Expuestas extranjeras.
Obtener, además de los datos exigidos para las personas físicas y morales, la documentación señalada en el Título Tercero, Capítulo I de las DCGA58, que refiere a la política de identificación del cliente.[19]

PREVENCIÓN DE LAVADO DE DINERO Y FINANCIAMIENTO AL TERRORISMO

Descripción del proceso.
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).

18 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 https://www.dof.gob.mx/nota_detalle.php?codigo=5537449&fecha=10/09/2018.

19 Art. 38 de las 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 https://www.dof.gob.mx/nota_detalle.php?codigo=5537449&fecha=10/09/2018.

IR AL CONTENIDO

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."[20] 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."[21] 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.

Recomendación.
Para esta actividad, las ITF deberán atender los elementos contenidos en las siguientes actividades que son derivadas de la ejecución de medidas para prevenir el lavado de dinero y el financiamiento al terrorismo.

20 https://www.gob.mx/cms/uploads/attachment/file/71151/VSPP_Lavado_de_Dinero___130701.pdf

21 https://www.cnbv.gob.mx/CNBV/Documents/VSPP_Financiamiento%20al%20Terrorismo.pdf

IR AL CONTENIDO

INSPECCIÓN, VIGILANCIA E INTERCAMBIO DE INFORMACIÓN

Descripción del proceso.
Las ITF están obligadas a proporcionar a la CNBV y al Banco de México información sobre las operaciones propias y operaciones realizadas entre sus clientes.

Al ser sujetos obligados como parte de una infraestructura tecnológica, deberán contar con sistemas automatizados en materia de PLD/FT que desarrollen entre otras, las siguientes funciones:

- Conservar y actualizar, así como permitir la consulta de los datos relativos a los registros de la información de expedientes de identificación de cada cliente y usuario.
- Generar, y transmitir de forma segura a la SHCP, por conducto de la CNBV, la información relativa a los reportes de operaciones.
- Clasificar los tipos de operaciones o productos financieros que ofrezcan a sus clientes y usuarios a fin de detectar posibles operaciones inusuales.
- Detectar y monitorear las operaciones realizadas en una misma cuenta o por un mismo cliente o usuario.
- Ejecutar un sistema de alertas.
- Contribuir a la detección, seguimiento y análisis de las posibles operaciones inusuales y operaciones internas preocupantes, considerando al menos, la información que haya sido proporcionada por el cliente o usuario al inicio de la relación comercial, los registros históricos de las operaciones realizadas por este, el comportamiento transaccional, los saldos promedio y cualquier otro parámetro que pueda aportar mayores elementos para el análisis de este tipo de operaciones.
- Agrupar en una base consolidada los diferentes contratos de un mismo cliente y las operaciones de un mismo usuario, a efecto de controlar y dar seguimiento integral a sus saldos y operaciones.
- Conservar registros históricos de las posibles operaciones inusuales y operaciones internas preocupantes.
- Mantener esquemas de seguridad de la información procesada, que garanticen la integridad, disponibilidad, auditabilidad y confidencialidad de la misma.

IR AL CONTENIDO

- Proveer la información que los sujetos obligados incluirán en la metodología de enfoque basado en riesgos que deben elaborar conforme a lo establecido en las Disposiciones.
- Facilitar la verificación de los datos y documentos proporcionados por el cliente o usuario.

Recomendación.
Las ITF deberán crear sistemas informáticos que permitan monitorear de manera no invasiva la información guardada y generada por sus clientes, cuidando las medidas de seguridad necesarias que resguarden los datos que intervienen en cada etapa de un proceso realizado a través de sus plataformas, asimismo, garantizar que los datos que serán incluidos en los reportes, sean correctos y correspondan al cliente que los realizó.

PRESENTACIÓN DE REPORTES A LA SHCP POR CONDUCTO DE LA CNBV

Descripción del proceso.
En el momento en el que se emite un reporte, es importante tener en cuenta 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 ITF son los siguientes:

I. *Reportes de Operaciones Relevantes*, los cuales deberán realizarse dentro de los 10 primeros días hábiles de los meses de enero, abril, julio y octubre.[22]

22 Art. 66 de las 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 https://www.dof.gob.mx/nota_detalle.php?codigo=5537449&fecha=10/09/2018.

IR AL CONTENIDO

II. *Reportes de operaciones en efectivo en moneda extranjera,* los cuales deberán realizarse dentro de los 10 primeros días hábiles[23] 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 los 10 primeros días hábiles de los meses de enero, abril, julio y octubre. Dicho reporte deberá incluir la compra o venta de Activos Virtuales.[24]
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.[25]

23 Art. 67 de las 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 https://www.dof.gob.mx/nota_detalle.php?codigo=5537449&fecha=10/09/2018.

24 Art. 74 de las 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 https://www.dof.gob.mx/nota_detalle.php?codigo=5537449&fecha=10/09/2018.

25 Art. 58 de la LRITF

IR AL CONTENIDO

Recomendación.
Respecto a este tipo de transferencias de datos personales, se recomienda informarles a los titulares que las comunicaciones de su información personal, será realizada dentro del marco normativo que regula a las ITF. Y como tal no es necesario requerir su consentimiento.

Las transferencias que no requieren del consentimiento del titular son las que ocurren en alguno de los siguientes casos (artículo 37 de la LFPDPPP):

I. Cuando la transferencia esté prevista en una ley o tratado en los que México sea parte;
II. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;
III. Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;
IV. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;
V. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;
VI. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y
VII. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.

CONSERVACIÓN DE ARCHIVOS

Descripción del proceso.
Se identificó la Ley FinTech obliga a las IFT 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

IR AL CONTENIDO

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.[26]

En este sentido, los datos que se encuentran en documentos deben cumplir con diversas obligaciones y están sujetas a los siguientes periodos de conservación:

- **Reportes de operaciones.**
  Copia de los reportes de actividades, deberá conservarse por un periodo no menor a diez años contado a partir de su ejecución.
  I. Original, copia o registro contable o financiero de toda la documentación soporte de las operaciones realizadas, deberá conservarse por un periodo no menor a diez años contado a partir de su ejecución.
  II. Resultados de la dictaminarían de posibles operaciones inusuales, deberán conservarse por un periodo no menor a diez años contado a partir de su ejecución.
- **Expedientes de identificación.**
  Datos y documentos que integran los expedientes, deberán conservarse durante toda la vigencia del contrato y, una vez que este concluya, por un periodo no menor a diez años contado a partir de dicha conclusión, o a partir de que se lleve a cabo la operación de que se trate en el caso de los usuarios.
- **Informes de auditorias.**
  Resultados de la revisión realizada por el área de auditoria o por un auditor externo independiente, deberá conservarse por un plazo no menor a cinco años.

26 Art. 58 de la LRITF

- **Metodologías de enfoque basado en riesgos.**
  Conservación de la información generada por la metodología de la evaluación de riesgos, deberá conservarse por un plazo no menor a cinco años.

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.

Recomendación.
Respecto a este tema, las ITF deberán cumplir con los periodos de conservación establecidos y una vez que hayan pasado los plazos de tiempo mencionados, deberán contar con mecanismos de borrado seguro de la información de sus usuarios, la información que otorgaron los usuarios y la referente a las actividades realizadas derivadas de la contratación de un servicio.

IR AL CONTENIDO

SEGURIDAD DE LA INFORMACIÓN COMO PARTE DEL PLAN DIRECTOR DE SEGURIDAD

De acuerdo con lo dispuesto en las Disposiciones de carácter general aplicables a las Instituciones de Tecnología Financiera (ITF)[27] 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, las ITF deben contar con un Plan Director de Seguridad.

El Plan Director de Seguridad es el documento que establece la estrategia de seguridad de una institución de financiamiento colectivo a corto, mediano y largo plazo para procurar una correcta gestión de la seguridad de la información y evitar que los Eventos de Seguridad de la Información se materialicen en Incidentes de Seguridad de la Información.

Las ITF deberán implementar controles internos en materia de seguridad de la información que procuren la confidencialidad, integridad y disponibilidad de la información. El marco de gestión a que se refiere este párrafo, deberá asegurar que la Infraestructura Tecnológica de dicha Institución, ya sea propia o provista por terceros, se apegue a los requerimientos siguientes:

1. Que cada uno de sus componentes realice las funciones para las que fue diseñado, desarrollado o adquirido.

2. Que sus procesos, funcionalidades y configuraciones, incluyendo su metodología de desarrollo o adquisición, así como el registro de sus cambios, actualizaciones y el inventario detallado de cada componente de la Infraestructura Tecnológica, estén documentados.

27 https://www.cnbv.gob.mx/Normatividad/Disposiciones%20de%20carácter%20general%20aplicables%20a%20las%20instituciones%20de%20tecnolog%C3%ADa%20financiera.pdf

IR AL CONTENIDO

3. 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. Tratándose de componentes de comunicaciones y de computo, los aspectos de seguridad deberán incluir, al menos, lo siguiente:

a. Segregación lógica, o lógica y física de las diferentes redes en distintos dominios y subredes, dependiendo de la función que desarrollen o el tipo de datos que se transmitan, incluyendo segregación de los ambientes productivos de los de desarrollo y pruebas, así como componentes de seguridad perimetral y de redes que aseguren que solamente el trafico autorizado es permitido. En particular, en aquellos segmentos con enlaces al exterior, tales como Internet, proveedores, autoridades, otras redes de la institución de financiamiento colectivo o matriz y otros terceros, todo ello referido a aquellos servicios definidos como críticos por la propia institución, ya sean sistemas de pagos, equipos de Cifrado, autorizadores de Operaciones, entre otros, deberán considerar zonas seguras, incluyendo las denominadas zonas desmilitarizadas (DMZ por sus siglas en inglés).
b. Configuración segura de acuerdo con el tipo de componente, considerando al menos, puertos y servicios, permisos otorgados bajo el principio de mínimo privilegio, uso de medios extraíbles de almacenamiento, listas de acceso, actualizaciones del fabricante y reconfiguración de parámetros de fábrica. Se entenderá como principio de mínimo privilegio a la habilitación del acceso únicamente a la información y recursos necesarios para el desarrollo de las funciones propias de cada Usuario de la Infraestructura Tecnológica.
c. Mecanismos de seguridad en las aplicaciones que procuren que, durante su ejecución se protejan de ataques o intrusiones, tales como inyección de código, manipulación de la sesión, fuga de información,

IR AL CONTENIDO

alteración de privilegios de acceso, entre otros. Dichos mecanismos deberán de ser implementados tanto para las aplicaciones proporcionadas por terceros como para las aplicaciones desarrolladas, implementadas y mantenidas por la propia institución de financiamiento colectivo.

4. Que cada uno de sus componentes sea probado antes de ser implementado o modificado, utilizando mecanismos de control de calidad que eviten que en dichas pruebas se utilicen datos reales del ambiente de producción, se revele información confidencial o de seguridad o se introduzca cualquier funcionalidad no reconocida para dicho componente.

5. Que cuente con las licencias o autorizaciones de uso, en su caso.

6. Que cuente con medidas de seguridad para su protección, así como para el acceso y uso de la información que sea recibida, generada, transmitida, almacenada y procesada en la propia Infraestructura Tecnológica contando, al menos, con lo siguiente:

a) Mecanismos de identificación y Autenticación de todos y cada uno de los Usuarios de la Infraestructura Tecnológica, que permitan reconocerlos de forma inequívoca y aseguren el acceso únicamente a las personas autorizadas expresamente para ello, bajo el principio de mínimo privilegio.
   Para lo anterior, se deberán incluir controles pertinentes para aquellos Usuarios de la Infraestructura Tecnológica con mayores privilegios, derivados de sus funciones, tales como la de administración de bases de datos, sistemas operativos y aplicativos.
   Asimismo, se deberán prever en manuales las políticas y procedimientos para las autorizaciones de accesos por excepción, tales como usuarios de ambientes de desarrollo con acceso a ambientes de producción y con accesos por eventos de contingencia, entre otros. Dichas políticas y procedimientos deberán ser aprobados por el oficial en jefe de seguridad de la información.
b) Cifrado de la información conforme al grado de sensibilidad o clasificación de la información que la institución de financiamiento colectivo

IR AL CONTENIDO

determine y establezca en sus políticas, cuando dicha información sea transmitida, intercambiada y comunicada entre componentes o almacenada en la Infraestructura Tecnológica o se acceda de forma remota.

Las instituciones de financiamiento colectivo deberán cifrar al menos, la información que hayan clasificado como critica en términos de estas disposiciones.

c) Claves de acceso con características de composición que eviten accesos no autorizados, considerando procesos que aseguren que solo el Usuario de la Infraestructura Tecnológica sea quien las conozca, así como medidas de seguridad, Cifrado en su almacenamiento y mecanismos para solicitar el cambio de claves de acceso cada noventa días o menos. Tratándose de Clientes, el plazo referido será el definido por las propias instituciones de financiamiento colectivo en los manuales a que alude el último párrafo de este artículo. En el caso de los Usuarios de la Infraestructura Tecnológica asignados a aplicativos o componentes para autenticarse entre ellos, el cambio a que alude este inciso deberá realizarse, al menos, una vez al año. En el evento de que algún Usuario de la Infraestructura Tecnológica tenga conocimiento de las claves de acceso y deje de prestar sus servicios a la institución de financiamiento colectivo, estas deberán inhabilitarse de manera inmediata.
d) Controles para terminar automáticamente sesiones no atendidas, así como para evitar sesiones simultáneas no permitidas con un mismo identificador de Usuario de la Infraestructura Tecnológica.
e) Mecanismos de seguridad, tanto de acceso físico, como de controles ambientales y de energía eléctrica, que protejan la Infraestructura Tecnológica y permitan la operación conforme a las especificaciones del proveedor, fabricante o desarrollador.
f) Medidas de validación para garantizar la autenticidad de las transacciones ejecutadas por los diferentes componentes de la Infraestructura Tecnológica considerando, al menos, lo siguiente:

    a. La veracidad e integridad de la información.
    b. La Autenticación entre componentes de la Infraestructura Tecnológica, que aseguren que se ejecutan solo las solicitudes de servicio legítimas desde su origen y hasta su ejecución y registro.

IR AL CONTENIDO

c. Los protocolos de mensajería, comunicaciones y Cifrado, los cuales deben procurar la integridad y confidencialidad de la información.
d. La identificación de transacciones atípicas, previendo que se cuenten con herramientas de monitoreo o medidas de alerta automática para su atención por las áreas operativas correspondientes.
e. La actualización y mantenimiento de certificados digitales y componentes proporcionados por proveedores de servicios que estén integrados al proceso de ejecución de transacciones. Las medidas a que alude este inciso deberán establecerse acorde con el grado de riesgo que las instituciones de financiamiento colectivo definan para cada tipo de transacción.

Las instituciones de financiamiento colectivo, en la clasificación de la información a que alude el inciso b) de esta fracción, deberán considerar al menos una categoría referente a la información critica. En dicha categoría 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.

7. Que cuente con mecanismos de respaldo y procedimientos de recuperación de la información que mitiguen el riesgo de interrupción de la operación, en concordancia con lo estipulado en su Plan de Continuidad de Negocio a que alude el Capítulo V del Título Tercero de las presentes disposiciones.

8. Que mantenga registros de auditoría íntegros, incluyendo la información detallada de los accesos o intentos de acceso y la operación o actividad efectuada por los Usuarios de la Infraestructura Tecnológica, lo anterior con independencia del nivel de privilegios con el que estos cuenten para el acceso, generación o modificación de la información que reciban, generen, almacenen o transmitan en cada componente de la Infraestructura Tecnológica, incluyendo actividad de procesos automatizados, así como los procedimientos para la revisión periódica de dichos registros.

IR AL CONTENIDO

Las instituciones de financiamiento colectivo deberán conservar los registros de auditoría a que se refiere esta fracción, por un periodo de tres años cuando dichos registros se refieran a actividades realizadas sobre componentes que procesen o almacenen información considerada como critica de conformidad con la clasificación que determine la institución de financiamiento colectivo. En caso contrario, el periodo de conservación de los registros será mínimo de seis meses.

9. Que para la atención de los Eventos de Seguridad de la Información e Incidentes de Seguridad de la Información se cuente con procesos de gestión que aseguren la detección, clasificación, atención y contención, investigación y, en su caso, análisis forense digital, diagnóstico, reporte a áreas competentes, solución, seguimiento y comunicación a autoridades, Clientes y contrapartes.
Para la detección y respuesta de Incidentes de Seguridad de la Información a que hace referencia el párrafo anterior, el director general o, en su caso, el administrador único deberá designar un equipo que incorpore al personal de las diferentes áreas de la institución de financiamiento colectivo para participar en cada actividad del proceso de gestión antes señalado del que, en todo caso, deberá formar parte el oficial en jefe de seguridad de la información de conformidad con el artículo 66 de las presentes disposiciones.
En caso de que se detecte la existencia de vulnerabilidades y deficiencias en la Infraestructura Tecnológica, deberán tomarse las acciones correctivas o controles compensatorios de acuerdo con el nivel de riesgo de que se trate, previniendo que los Usuarios de la Infraestructura Tecnológica o la institución de financiamiento colectivo puedan verse afectados.

10. Que sea sometida a la realización de ejercicios de planeación y revisión anuales que permitan medir su capacidad para soportar su operación, garantizando que se atiendan oportunamente las necesidades de incremento de capacidad detectadas como resultado de dichos ejercicios.
Asimismo, la institución de financiamiento colectivo deberá evaluar la obsolescencia de los componentes de la Infraestructura Tecnológica, debiendo contar con un plan para su actualización.

IR AL CONTENIDO

11. Que cuente con controles automatizados o, en ausencia de estos, que se realicen controles compensatorios, tales como doble verificación y conciliación que, previo o posteriormente a la realización de la operación de que se trate, minimicen el riesgo de eliminación, exposición, alteración o modificación de información, que se deriven de procesos manuales o semiautomatizados realizados por el personal de la institución de financiamiento colectivo, con el objetivo de prevenir errores, omisiones, sustracción o manipulación de información.

12. Que tenga controles que permitan detectar la alteración o falsificación de libros, registros y documentos digitales relativos a las Operaciones.

13. Que cuente con procesos para medir y asegurar los niveles de disponibilidad y tiempos de respuesta, que garanticen la ejecución de las Operaciones realizadas; lo anterior, incluyendo los supuestos en que las instituciones de financiamiento colectivo contraten la prestación de servicios por parte de terceros para el procesamiento y almacenamiento de información.

14. Que cuente con dispositivos o mecanismos automatizados para detectar y prevenir Eventos de Seguridad de la Información e Incidentes de Seguridad de la Información, así como para evitar conexiones y flujos de datos entrantes o salientes no autorizados y fuga de información considerando, entre otros, medios de almacenamiento removibles.

Las instituciones de financiamiento colectivo deberán correlacionar los datos obtenidos de los dispositivos o mecanismos automatizados a que alude el párrafo anterior con los datos de otras fuentes, tales como registros de actividad de Eventos de Seguridad de la Información o de Incidentes de Seguridad de la Información.

Adicionalmente, las instituciones de financiamiento colectivo deberán mantener controles que eviten la filtración de la información correspondiente a la configuración de la Infraestructura Tecnológica, tales como direcciones IP, reglas de los cortafuegos, así como versiones de hardware y software.

IR AL CONTENIDO

15. Que, para la prestación de servicios de tecnologías de información a los Usuarios de la Infraestructura Tecnológica, 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. El director general o, en su caso, el administrador único de la institución de financiamiento colectivo será responsable de documentar en manuales las políticas y procedimientos previstas en este artículo.

El director general o, en su caso, el administrador único de la institución de financiamiento colectivo será responsable de documentar en manuales las políticas y procedimientos previstas en este artículo.

IR AL CONTENIDO

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