Grañén
Porrúa
Grupo Editorial

El futuro llegó:

bases y condiciones de la transformación del sistema financiero

José Antonio
Quesada Palacios

El futuro llegó:
bases y condiciones de la transformación del sistema financiero

El futuro llegó:
bases y condiciones de la transformación del sistema financiero

José Antonio
Quesada Palacios

EGADE Business School
Tecnológico de Monterrey
HLB MAAT ASESORES
LITO-GRAPO S.A. de C.V.
Grañén Porrúa

MÉXICO, 2020

IMPRESO EN MÉXICO
PRINTED IN MEXICO

Colima 35, Tizapán,
01080 Ciudad de México.

Primera edición, mayo de 2020

© 2020 Por características tipográficas y de diseño editorial
Lito-Grapo S.A. de C.V.

Editora: Adriana Reyes Urrutia

Impreso en los talleres de Lito-Grapo, S.A. de C.V.

Derechos reservados conforme a la ley
ISBN 978-607-8341-97-9

Queda prohibida la reproducción parcial o total, directa o indirecta del contenido de la presente obra, sin contar previamente con la autorización expresa y por escrito de los editores, en términos de lo así previsto por la *Ley Federal del Derecho de Autor* y, en su caso, por los tratados internacionales aplicables.

Contenido

Introducción 9
Prólogo 11
Presentación 13
Preámbulo 15
Liminar 17
Nota del editor 21

Primera parte
Tecnología, factor de cambio

Capítulo 1. Recuento imprescindible 25
Nuevas realidades implican nuevas visiones del negocio financiero 25

Capítulo 2. Desregulación: se abre la puerta a la innovación 27
La regulación después de 1970 28
Consecuencias 32
Desregulación y crisis 33

Capítulo 3. Se aprende del pasado:
nuevo escenario para la innovación tecnológica 34
Nuevos jugadores: American BigTechs (Google, Amazon y Apple), AsianTechs, Neo y Challengers Banks y fintechs 36
Llegaron las grandes: American BigTechs y/o GAFP 36
Del otro lado del mundo: AsianTechs 37
Totalmente digitales: Neo y Challenger Banks 39
Crecen las pequeñas: Fintech 39
BigTech, ¿Competencia o alianza? 41
Banca Abierta: colaboración inminente 43
Recuadro. Open Banking, perspectiva internacional 44
Recuadro. API. Los datos en primer plano 48
Transición: de la Banca Abierta al Open X 51
Qué pasa con la Banca Abierta 51
Regulación: ¿motivación o desencanto? 53

Segunda parte
Factores entrelazados. El cambio implica consecuencias

Capítulo 4. Riesgos en escenarios cambiantes 59
Recuadro. Crisis: México 1994-1995 59
Cambian los riesgos 65
Recuadro. Tipo de riesgos asociados al sistema bancario 66
Supervisión 68
Preocupación explícita 69

Capítulo 5. La gestión de riesgos se abre a nuevos actores 70

Capítulo 6. Ciberseguridad: riesgos al acecho 71
Esfuerzos conjuntos 75
¿Cómo pinta México? 78
Radiografía: situación, alcances y respuesta 80

Capítulo 7. Prácticas regulatorias de seguridad cibernética 80

Capítulo 8. Tecnología y después qué 91
Blockchain, inicia la revolución 93
Significado y proceso 93
Del internet de la información al internet del valor 95
Lo ya cuantificable 97
Disrupción en la disrupción 98
Inteligencia Artificial 98
Recuadro. Blockchain / *IA* 100
Complementarias y sinérgicas 100
Internet de las Cosas 101
Big Data 104
Generación de valor 105
Comprender y aplicar 106
En el sector financiero 108
Barreras y soluciones 108

Capítulo 9. Seguimos mirando a futuro 109

Tercera parte
Nuevos componentes para un desarrollo incluyente

Capítulo 10. Evolución de la arquitectura del sistema financiero 113

Capítulo 11. Fintech: Incorporación, marco, avance, expectativas 117
Estructura y alcance 119
Recuadro. Reformas al iniciar el Siglo XXI 120
¿En el camino correcto? 121
Capítulo 12. Contexto: antes y después de la Ley Fintech 123
Inclusión financiera 123
Protección al consumidor 128
Estabilidad financiera 130
Sana competencia 132
Prevención y mitigación del riesgo de lavado de dinero y financiamiento al terrorismo 135
Razón de ser 137
Recuadro. Crowdfunding 139

Capítulo 13. Reconocimiento: Las bases del cambio 141
Activos virtuales 141
Crecimiento y respuesta 142
Una vuelta atrás 147
Definiciones pertinentes 147
API, el panorama 150
Proyecto de disposiciones relativas a las API 150
Instituciones de Fondos de Pago Electrónico 155
La única constante es el cambio 157

Anexo 1
Panorama de la Ley para Regular las Instituciones de Tecnología Financiera 159
Leyes modificadas para hacer realidad la Ley Fintech 164

Anexo 2
Borrador de las disposiciones aplicables a las Instituciones de Fondos de Pago Electrónico 173

Anexo 3
Disposiciones de carácter general para regular las Instituciones de Tecnología Financiera, aplicables a las Sociedades de Información Crediticia y Cámaras de Compensación en materia de interfaces de programación de aplicaciones informáticas estandarizadas 259

Fuentes consultadas 275

Semblanza 279

Introducción

En las últimas décadas, en el Sistema Financiero mexicano los consumidores se convirtieron en el eje de la acción. Dichos usuarios son cada vez más exigentes, tienen más recursos y mayor acceso a la información del mercado por lo que, de la mano de la tecnología, están cambiando a patrones en los que se busca una experiencia personalizada e inmediata en la que las entidades financieras (como las conocimos hasta hace poco, antes de iniciar el nuevo siglo), si desean mantenerse vivas, deben adelantarse a sus necesidades y adaptar su modelo de negocio bajo un contexto que cambia constantemente.

Esta transformación que viene de la mano de la innovación de productos y servicios, así como de la *forma de hacer las cosas,* requiere nuevos marcos para establecer las interrelaciones, aunque es un hecho que no podemos mirar hacia delante si no echamos una mirada atrás.

Recordar el pasado nos puede ayudar a planear el futuro. Partimos de esta consigna para que el lector –el que ha pasado de la ventanilla física y del escritorio del ejecutivo bancario al teclado de una computadora y luego a la pantalla táctil de su teléfono inteligente; y el que directamente se ha sumado a los servicios financieros usando su dispositivo móvil— recuerde o conozca que la innovación requiere un compromiso, estrategia y visión pero, sobre todo, conocimiento del 'qué' y 'cómo' para entender el 'para qué' y 'para quién'.

De ahí que en las siguientes páginas se plantee un recorrido por la regulación, la tecnología, los productos financieros, los participantes (los tradicionales y los nuevos; los que ofrecen y los que reciben los servicios financieros) y los vínculos que se establecen entre éstos y que están dando forma a un nuevo contexto o arquitectura.

¿Qué mueve a la regulación?, ¿la tecnología, los participantes del sistema financiero, los productos financieros o los consumidores? ¿Qué mueve a la tecnología?, ¿la regulación, los participantes, los productos financieros o los consumidores? ¿Qué mueve las preferencias del consumidor, la tecnología, la regulación, la oferta de productos? En general el 'qué mueve a qué' es la pregunta clave y el lector, a partir de la información reunida en las siguientes páginas y su experiencia, podrá responder y contar con elementos para entender el sentido del cambio, en el que, sin duda, él es el protagonista.

Ignacio de la Vega
Decano de la Escuela de Negocios y de EGADE *Business School del Tecnológico de Monterrey*

Prólogo

El futuro llegó: bases y condiciones de la transformación del sistema financiero es una mirada a través de cinco décadas del sistema financiero, tomando en cuenta cinco elementos fundamentales: tecnología, regulación, innovación, participantes y riesgos que han modificado a la ingeniería y a la arquitectura financieras, al establecer vínculos y oportunidades, pero también presentar vulnerabilidades.

Los cinco elementos se desarrollan en tres partes y catorce apartados. En cada uno el eje gira en torno a un elemento y su relación con los otros cuatro, lo que refuerza la visión de que los cinco elementos están estrechamente unidos.

El autor parte de la tecnología como factor de cambio y hace un recuento que considera imprescindible en el que nuevas realidades implican nuevas visiones del negocio financiero. Y en esas realidades está la regulación después la desregulación y nuevamente la regulación. Innovación y crisis son las dos aristas presentes en ese proceso que el autor plantea como marco para establecer que se aprende del pasado y que la nueva arquitectura con nuevos jugadores requiere colaboración, porque el cambio implica consecuencias y éstas tienen que ser a favor de los participantes, los que generan los productos y servicios, los que establecen las reglas y, sobre todo, los usuarios del sistema financiero.

De ahí que se aboque a los riesgos en escenarios cambiantes y aborde los contextos para dar paso a la gestión de riesgos abierta a nuevos contextos y actores, donde la ciberseguridad es considerada como un riesgo al acecho que amerita practicas regulatorias, las cuales expone para entender la magnitud de este riesgo del cual México ya tiene un panorama de su situación, alcances y respuesta, en el entendido de que la innovación tecnológica modificará el entorno y las respuestas porque, como dice el autor, "seguimos mirando a futuro" por lo que se detiene en cuatro tecnologías que, de una forma u otra, irrumpirán modificando lo que hoy existe y donde el usuario es quien marca la ruta: Blockchain, Inteligencia Artificial, Internet de las Cosas y Big Data

El futuro llegó, dice el autor, por lo tanto hay nuevos componentes para un desarrollo incluyente. En el décimo apartado el autor se concentra en México y presenta los elementos que han marcado la ruta de la evolución de la arquitectura del sistema financiero. Se detiene en las Fintech, su incorporación, marco, avance, expectativas y presenta el contexto antes y después de la Ley para Regular las Instituciones de Tecnología Financiera (Ley Fintech) a partir de inclusión financiera, protección al consumidor, estabilidad financiera, sana competencia,

así como prevención y mitigación del riesgo de lavado de dinero y financiamiento al terrorismo.

La razon es exponer como han sido abordados en el país los cinco elementos (tecnología, regulación, innovación, participantes y riesgos) factores del cambio, así como mostrar las Disposiciones de Carácter General en torno a elememtos de la Ley Fintech: Activos virtuales, Interfaces de Programación de Aplicaciones Informáticas (APIs) e Instituciones de Fondos de Pago Electrónico, con lo que el autor refrenda que la única constante es el cambio y que estos temas son parte de los cinco elementos.

El trabajo del autor demuestra que la interacción entre los elementos genera nuevas realidades que trascienden la acción de sumar los componentes. *El futuro llegó: bases y condiciones de la transformación del Sistema Financiero* es un trabajo para mostrar que se debe aprender del pasado para responder al futuro.

Salvador Villalobos Gómez
Presidente Ejecutivo Consejo de la Comunicación

Presentación

La transformación digital ha generado que las organizaciones asuman constantemente desafíos buscando la integración de la tecnología digital en todas las áreas del negocio y transformando la forma de operar y agregar valor a sus clientes quienes, por cierto, están marcando la agenda en muchos sectores, incluido el financiero.

Esta transformación está dando giros de 360 grados a los que se han subido todos los involucrados: instituciones publicas y privadas, autoridades financieras, así como usuarios y legislación, lo que ha dado lugar a nuevos participantes, productos, servicios y formas de interactuar. La nueva relación no deja de usar el adjetivo nueva porque la velocidad de los cambios no permite quitarlo. El cambio es constante.

Y es el cambio en el sector financiero, precisamente, el que da motivo a la obra que tienen en sus manos. El autor se remonta varias décadas atrás para sustentar las características del ecosistema, abordando los temas que han determinado la transformación.

Este libro es un ejercicio para entender "de donde venimos y hacia dónde vamos" en el sector financiero, dice el autor, quien considera importante establecer el vínculo entre tecnología y regulación, y partir de este binomio abordar otros como innovación y productos, servicios y usuarios, así como usuarios y regulación en un recorrido que comienza en los años 70 del siglo pasado y no tiene fecha de termino porque, como insiste el autor en el transcurso de estás páginas, el cambio es constate. Tanto que en la tercera parte de este trabajo da continuidad a la obra que presentó en 2019 en la que la Ley para Regular a las Instituciones de Tecnología Financiera (Ley Fintech) fue el eje principal.

La continuidad consiste no solo en sumar Disposiciones de Carácter General correspondientes a la Ley Fintech, sino en presentar los avances en los temas específicos motivo de la ley que se presentó en marzo de 2018; es decir el panorama después de Ley.

El futuro llegó: bases y condiciones de la transformación del Sistema Financiero se suma al giro de 360 grados presentando los cambios que la transformación digital ha motivado entre los involucrados: instituciones publicas y privadas, autoridades financieras, así como usuarios y legislación, e infiere —a partir de la información disponibles y realidad evidente— qué sigue en cuanto a productos, servicios y formas de interactuar de los involucrados.

Carlos Salazar Lomelí
Presidente Consejo Coordinador Empresarial

Preámbulo

Es una realidad incuestionable que el avance tecnológico ha representado beneficios en la mayoría de los procesos de producción: abarata costos, proporciona mejores experiencias de uso y, en general, ofrece soluciones óptimas. La prestación de servicios financieros no escapa de esta realidad, pues las entidades financieras no sólo se limitan al uso de las nuevas tecnologías, sino que también se han convertido en creadoras de procesos digitales que pretenden aportar múltiples beneficios como reducir costos, acelerar la producción, mejorar la oferta de servicios, anticipar las necesidades de los clientes, entre otros.

Sin embargo, el esfuerzo realizado por las entidades financieras es alto porque deben alinear todas las variables involucradas en la cadena de valor y hacer de la digitalización el hilo conductor de su estrategia debido a que deben considerar la necesidad que tienen sus clientes de acceder veinticuatro horas al día al gran escaparate de la red para obtener información transparente, completa y fidedigna en tiempo real.

Este nuevo escenario tecnológico, donde el *smartphone* es casi una extensión del consumidor y uno de los principales canales de comunicación entre la empresa y el cliente, plantea cómo las entidades financieras tradicionales, como los bancos, y las nuevas entidades, como las fintech, enfrentan este proceso de tecnificación que implica reacción, adaptación y posicionamiento, y para poder aportar una respuesta hay que considerar aspectos sobre tecnología, innovación, regulación, visión y estrategia.

Con esta nueva realidad, el futuro de las entidades financieras —las tradicionales y las que tienen como base a la tecnología, que no solo son las fintech, sino también los gigantes tecnológicos que han pasado de su negocio inicial a los servicios financieros— dependerá de su adaptación o reinvención porque no sólo están cambiando los participantes, también se están transformando los modelos; así, la banca tradicional ha dado paso a la banca abierta, que augura una nueva etapa: la del *Open X*. En ese sentido, es importante recalcar que la tecnología, el acceso y las opciones en productos y servicios tienen un papel preponderante, visto, analizado y regulado (ya en muchos casos) para cuidar las acciones e interacciones con el objetivo que deben cumplir los involucrados (las entidades públicas y las privadas): la estabilidad financiera en un contexto en el que los nuevos competidores surgen constantemente y van ocupando una posición que era, hasta hace algunos años, impensable.

Con la finalidad de ofrecer este amplio panorama, *El futuro llegó: bases y condiciones de la transformación del Sistema Financiero* expone los diferentes estadios por los que ha pasado el sistema financiero, tanto el nacional como el internacional, para incluir —a partir de nuestra visión y posición en el ecosistema— los nuevos elementos y condiciones en un marco de estabilidad en el que los riesgos, si bien no se pueden predecir, sí se pueden mitigar para seguir un camino del que no hay vuelta atrás. Así, el autor presenta un compendio de hechos, acciones y reacciones que hicieron, hacen y harán al sistema financiero.

Tomás Humberto Rubio Pérez
Director de la Facultad de Contaduría y Administración de la UNAM

Liminar

Con este libro José Antonio Quesada nos lleva por un viaje que va del pasado del sistema financiero hasta nuestros días, con la peculiaridad de que hace paradas para entender cada momento con sus razón y su contribución para establecer bases para el sistema financiero.

El autor parte de la tecnología como factor de cambio y a partir de ella hace un recuento imprescindible en el que nuevas realidades implican nuevas visiones del negocio financiero, por lo que dedica un apartado a la desregulación, que abre la puerta a la innovación financiera y tecnológica (¿o innovación tecnológica y financiera? Vale la pena plantear que ni una es primero ni la otra segunda; ambas interactúan para avanzar y establecer una simbiosis) en un entorno en el que es necesario conocer el contexto en el que se daba y se da la regulación.

El autor hace un recorrido en el tiempo y se detiene en los hitos como el fin de la era Bretton Woods, la desregulación del sistema financiero, la adopción de un modelo de banca universal y la libre movilidad de capitales, así como la caída de la Ley Glass Steagall a partir de la cual comenzaron las fusiones y la integración horizontal de la banca en los Estados Unidos. Los eventos internacionales sirven para contextualizar lo que pasó en México, un referente para el cambio.

Ese recorrido lleva al planteamiento de que con las medidas de desregulación y cambios generados en la economía, la industria financiera —con un rápido crecimiento— adquirió cada vez mayor relevancia en las economías a nivel local e internacional, pero también acentuó sus vulnerabilidades que culminan en la crisis desatada por las hipotecas subprime en 2007.

De este episodio el autor escribe: "La crisis financiera, que comenzó en el verano de 2007 y afectó, en mayor o menor medida, a la estabilidad financiera de todos los países cuestionó la ideología de los mercados libres y la liberalización financiera y llevó a la mesa la necesidad de una regulación financiera eficiente que actuase dentro de determinados parámetros de seguridad sistémica, y con una supervisión efectiva para prevenir los excesivos riesgos asumidos como práctica habitual por las instituciones financieras en los años recientes".

Su premisa, entonces, es que se aprende del pasado y de este pasado surge un nuevo escenario para la innovación tecnológica en el que con nuevos jugadores —American BigTechs (Google, Amazon y Apple), AsianTechs, Neo y Challengers Banks y Fintechs— se establece un nuevo modelo de banca, la Banca Abierta, y ésta camina aceleradamente de la mano de los nuevos actores apoyados en la tecnología, razón y motivo de la transformación digital, que está

cambiando la fisonomía del sector financiero. Por lo tanto se pregunta: Big Tech, Fintechs ¿Competencia o alianza?

Las páginas de este libro nos llevan a asumir que todos necesitan de todos, recordando que las vulnerabilidades han cambiado. Por lo tanto, la Banca Abierta tiene una consigna: colaboración inminente. "La Banca Abierta es un nuevo modelo bancario comparable al nacimiento de la banca telefónica u online. Para ello, las entidades deben activar un sistema tecnológico mediante API abiertas (enlaces tecnológicos que contienen información). De esta forma, terceras empresas pueden acceder a sus datos y obtener información sobre el comportamiento financiero de sus usuarios", dice el autor, lo que corrobora que tecnología, regulación, innovación y consumidores interactúan y, en ocasiones, se sobreponen.

El autor no se detiene en la Banca Abierta, avanza al Open X porque los cambios ya no duran, se suceden unos tras otros y continúan configurando y reconfigurando el sistema que siempre tiene una pregunta latente en todos los participantes: Regulación: ¿motivación o desencanto?

Por esa pregunta en la segunda parte del libro establece que hay factores entrelazados y que el cambio implica consecuencias, una de ellas son los *riesgos en escenarios cambiantes* porque la innovación financiera aportó un catálogo de productos, pero no la capacidad de medir mejor los riesgos financieros y en particular los riesgos sistémicos.

El autor argumenta que desde finales de los años 60 del siglo pasado ocurrieron diversos acontecimientos que han marcado en gran parte la evolución de las finanzas internacionales y, por ende, de la estructura del sistema financiero. Menciona los cambios relevantes en ámbitos como el tipo de instrumentos financieros negociados, la importancia y diversidad de los mercados financieros, las prácticas de gestión en las empresas, las retribuciones de los directivos, los sistemas de información y comunicación, las teorías financieras de valoración de los instrumentos financieros, la importancia de la política monetaria y las normas de regulación y supervisión financiera, dentro de un profundo proceso de globalización y de acumulación y concentración de la riqueza financiera, lo que trajo nuevos riesgos y la combinación de los riesgos tradicionales con los nuevos.

Por esta realidad el apartado seis lleva por título "La gestión de riesgos se abre a nuevos actores"; así que nuevos actores en nuevos escenarios implica detenerse en la ciberseguridad y considerar que hay riesgos al acecho por lo que se requieren esfuerzos conjuntos que conduzcan a prácticas regulatorias de seguridad cibernética.

"De acuerdo con el Instituto de Estabilidad Financiera del BIS, son pocas las economías a nivel mundial que cuentan con regulaciones explícitas y marcos o políticas en vigor para el riesgo cibernético. Dentro de este grupo de naciones se encuentran Estados Unidos, el Eurosistema, Hong Kong, México, Reino Unido y República Dominicana, por mencionar algunos (en un intento por plantear el nivel de desarrollo y la geografía)", apunta el autor para dar paso a esas prácticas regulatorias y su porqué en un contexto de riesgo determinado.

Por qué acotó que es en un contexto determinado, porque al autor sabe que nos hemos subido a un auto sin reversa. No hay marcha atrás: la tecnología evoluciona y debemos ser prospectivos por lo que es importante tener en el radar a la tecnología actual y a la que viene. Todos los sabemos. De hecho las regulaciones lo tienen presente porque como se señala en el apartado 10 "seguimos mirando a futuro".

La parte tres del libro nos dice que hay nuevos componentes para un desarrollo incluyente y en cada uno de sus apartados nos dice el por qué de esa aseveración: por la evolución de la arquitectura del sistema financiero y por las fintech, su incorporación, marco, avance y expectativas, lo que lleva a hacer una revisión del contexto antes y después de la Ley Fintech bajo los principios que le dieron origen: inclusión financiera, protección al consumidor, estabilidad financiera, sana competencia, así como prevención y mitigación del riesgo de lavado de dinero y financiamiento al terrorismo.

En ese antes y después de la Ley Fintech el autor hace un alto para detenerse en los activos virtuales, las APIs y las Instituciones de Fondos de Pago Electrónico; el primer tema un pendiente que se resolvió en marzo de 2019 con las Disposiciones emitidas por el Banco de México; los otros dos, un pendiente que se resuelve en 2020 para hacer camino al andar y dejar patente que "la única constante es el cambio" y que se cuenta con las bases y condiciones de la transformación del Sistema Financiero porque el futuro llegó.

Juan Alberto Adam Siade
Miembro de la Junta de Gobierno de la UNAM

Nota del Editor

La única constante es el cambio. Esta consigna se repite a lo largo de esta obra en la que el autor plantea un recorrido por la regulación, la tecnología, los productos financieros, los participantes y la relación que estos elementos tienen en diferentes momentos (de crisis y de crecimiento) hasta llegar al actual, así como su impacto en la sociedad y el mercado, que son finalmente el objetivo de la transformación.Y en función de esa consiga está página se suma de último momento para que el lector tenga un elemento más para responder unas de las preguntas que Ignacio de la Vega hace en la introducción de este libro: ¿Qué mueve a la regulación? ¿la tecnología, los participantes del sistema financiero, los productos financieros o los consumidores?

El objetivo de esta página también es apuntalar la visión del autor, que Juan Alberto Adam Siade retoma en su aportación al mencionar que "las páginas de este libro nos llevan a asumir que todos necesitan de todos, recordando que las vulnerabilidades han cambiado".

En este sentido el 25 de marzo la Comisión Nacional Bancaria y de Valores informó que con el objetivo de mitigar los efectos económicos derivados de la contingencia por el Covid-19, emitía, con carácter temporal, criterios contables especiales, aplicables a instituciones de crédito, respecto de los créditos al consumo, de vivienda y comerciales, para los clientes cuya fuente de pago se encuentre afectada por esta contingencia.

Las medidas relacionadas a los criterios contables especiales se dieron en respuesta a la solicitud de autorización de las instituciones de crédito del Sistema Financiero de México, para que éstas lleven a cabo la implementación de diversos programas dirigidos a los acreditados afectados.

En obras anteriores, y en la que tiene en sus manos, el autor hace énfasis en la inclusión financiera y lo que representa como posibilidad de desarrollo para la sociedad y como reto (que incluye cobertura y seguridad, entre otros elementos) para los integrantes del Sistema Financiero. La importancia que le da a la inclusión financiera, se suma a su interés de conocer el pasado para entender el presente y mirar al futuro, sabiendo que ese futuro, como lo indica el título, ya *llegó* y, por lo tanto, las *bases y condiciones de la transformación del Sistema Financiero* son dar respuesta inmediatas antes situaciones contundentes para evitar los errores del pasado y no retroceder del camino andado.

Adriana Reyes
Editora *El futuro llegó: bases y condiciones de la transformación del Sistema Financiero*
Ciudad de México, 25 de marzo de 2020

PRIMERA PARTE

Tecnología, factor de cambio

1. Recuento imprescindible

Desde finales de los años sesenta del siglo xx, ocurrieron diversos acontecimientos que han marcado la rápida evolución del sistema financiero. Esos eventos, que para algunos son la gestación de la metamorfosis, pueden ubicarse en dos grupos; en el primero se encuentran los propios de la ingeniería financiera y en el segundo, los factores relacionados con los medios y las herramientas que hacen posible la evolución e incorporación de nuevos elementos al primer grupo, como las Tecnologías de Información (TI).

Si bien en cierto momento algunos desestimaron el impacto de las TI por la lenta evolución y los altos costos, otros valoraron su impacto en el sistema financiero, viéndolas como uno de los elementos generadores de multitud de acontecimientos que comenzaban a redefinir las características de las empresas financieras, desde la extensión de la actividad de algunas de ellas hacia campos muy alejados de la naturaleza de su negocio típico hasta los intentos de interpenetración o dominio entre entidades pertenecientes a subsectores financieros tradicionalmente distantes, aprovechando las oportunidades del movimiento desregulador de la época.

Así, los dos grupos se mezclaban para cambiar los paradigmas y sumar cualidades a la implementación de las TI, como las reducciones en el costo de obtención, tratamiento y transmisión de la información, lo que provocó la redefinición de los productos y procesos financieros, y proporcionó nuevos elementos para generar una nueva competencia, con la creación de fuertes ventajas competitivas y sectores totalmente nuevos.

Es a partir de la década de los años setenta cuando la integración de las comunicaciones y el procesamiento de datos alcanzó un nivel que permitió mirar hacia delante con una perspectiva diferente. El desarrollo tecnológico a lo largo de los años setenta y ochenta contribuyó notablemente a la transformación del entorno financiero y, entre otras cosas, al estrechamiento de los márgenes asociados al negocio bancario tradicional.

Nuevas realidades implican nuevas visiones del negocio financiero

Al reducirse la complicación y el costo del tratamiento de la información, surgieron nuevas posibilidades de la mano de los procesos de desregulación, que dieron la posibilidad de decidir y competir respecto a variables fundamentales, como precio, cantidad de productos y cobertura geográfica.

La intensidad de la influencia del cambio tecnológico sobre la actividad financiera se convirtió en un componente esencial de las estrategias bancarias de éxito, lo que propició hacer una simbiosis que a la fecha continúa, y con más fuerza, pero que, además, se ha convertido en el elemento que identifica las prácticas financieras, por lo que el sistema financiero se ha transformado en uno de los sectores con mayores modificaciones estructurales registradas en el marco de una reconceptualización del sector, de sus fronteras y de su alcance.

Un dato del Banco Interamericano de Desarrollo (BID) es ejemplo de lo anterior: "entre 1996 y 2002, más de una cuarta parte de los bancos de Argentina, Brasil, Colombia, Costa Rica, El Salvador y Perú cerraron o se fusionaron [...] y en muchos países,

los bancos extranjeros se convirtieron en los principales componentes del sistema financiero interno, tanto así que en 2002, aun cuando se encontraba en la fase de profundización de los cambios, los bancos extranjeros controlaban más de 50 por ciento de los activos en Argentina, Chile, México y Perú, muy por encima del nivel de menos de 30 por ciento que controlaban en cualquiera de esos países en 1995".[1]

¿Por qué remontarnos a las últimas décadas del siglo pasado? Simplemente porque es la época de los cimientos para construir un nuevo sistema financiero abriendo las puertas, es decir, de cara a una apertura regulatoria que daría margen a la innovación, y porque en ese entonces la prospectiva planteaba acciones voluntarias en un nuevo mercado —caracterizado por sucesivas innovaciones en el sector financiero, como la introducción de las tarjetas de crédito en los sesenta, los cajeros automáticos en los setenta y ochenta, y los nuevos productos financieros tras la desregulación de los mercados de bonos y de capitales en los noventa, así como la banca electrónica al inicio del nuevo siglo, que permitió prescindir de las oficinas bancarias y realizar operaciones de manera remota—, en el que la visión de los especialistas era considerada, tal vez, como una profecía sin la seguridad de que se cumpliría, o al menos en qué tiempo y a qué ritmo.

En la última década del siglo pasado, Juan R. Quintas[2] analizó el sistema financiero ante el cambio tecnológico y, citando a Michel Porter, escribió que las TI inciden intensamente sobre cada una de las fuerzas cuya interacción constituye la estructura sectorial al:

1. Modificar las barreras de entrada al existir competidores enfocados hacia segmentos específicos y utilizadores intensivos de las nuevas TI, y realizar fuertes inversiones en equipo vinculadas a canales de distribución concretos.
2. Abrir las posibilidades de la sustitución de productos que pueden satisfacer idénticas necesidades en multitud de contextos.
3. Alterar el poder negociador del clientes y proveedores.
4. Cambiar el nivel de rivalidad interna por la utilización de las innovaciones técnicas como arma competitiva.

Si bien ésta era una visión de los años noventa, se ha retomado para efecto de este trabajo porque es, en esencia, el punto de partida para plantear los elementos que caracterizan actualmente el sistema financiero y que son el parteaguas de lo que será la actividad financiera que, si bien sigue teniendo como sustento las características de los dos grupos referidos, el de la ingeniería financiera y el de los medios y herramientas de las TI, suma elementos a cada uno de ellos para plantear un tercer grupo que, a la vez que cohesiona, diversifica el sistema financiero: los clientes o usuarios que están presentes en los cuatro puntos expresados y que por su interacción están modificando las situaciones convergentes, como los riesgos —los tradicionales y los propios de la evolución tecnológica— que se convierten en un actor prioritario que condiciona el marco legal donde habrán de moverse los viejos y nuevos actores en la nuevas circunstancias determinadas por la innovación tecnológica.

[1] Banco Mundial (2013), "Base de datos de desarrollo financiero DFDD", disponible en <http://databank.bancomundial.org/data/reports.aspx?source=desarrollo-financiero-mundial, > consultado en diciembre de 2019.

[2] Juan R. Quintas (1990), *El sistema financiero ante el cambio tecnológico*.

Si volteamos a ver las características de la época que estamos tomando como punto de partida: tecnología, condiciones del sistema financiero, estado de la regulación y contexto económico, podemos observar una evolución en calidad y cantidad que nos lleva al punto donde debemos aterrizar para plantear el nuevo panorama del sistema financiero: inclusión financiera, mayor competencia y nuevas reglas determinadas por el contexto económico (el histórico y el actual).

Es un hecho: la tecnología permite avanzar en la inclusión financiera con el consecuente abatimiento de costos en un entorno de competencia que ha permitido importantes ganancias para las grandes instituciones financieras. De acuerdo con la BBC, en medio de un estancamiento global, en 2016, el mundo estaba dominado por 28 grandes bancos internacionales —entre los que se encuentran cuatro con presencia en México: HSBC, Santander, BBVA y Citigroup, además de Bank of America, Deutsches Bank y Bank of China— que en conjunto controlan cinco mecanismos que permiten la hegemonía financiera, económica y política del mundo: 90 por ciento de los activos financieros (bienes, dinero, clientes, préstamos, etcétera), 90 por ciento de la creación de moneda, 51 por ciento del manejo del mercado cambiario; 11 de los 28, encabezados por Bank of America, BNP-Paribas, Barclays y Citigroup, manejan las tasas de interés y los productos derivados; de ellos, 14 producen derivados por 710 mil millones de dólares, es decir, el equivalente a 10 veces el Producto Interno Bruto mundial.[3]

No obstante, en el contexto anticipado de ese poder, en 2008 surgieron nuevas empresas para explotar los diversos avances tecnológicos y vincularlos a los servicios financieros para sectores o nichos específicos. Los nuevos desarrollos o fintechs generaron un cambio de fondo y marcaron la pauta para cambiar el sistema financiero, vinculándose a la industria financiera tradicional o generando nuevos sectores con nuevo y mayor potencial, y así ofrecer una oportunidad, como nunca, para abatir los rezagos, como el de la inclusión financiera.

En este nuevo contexto se aprende del pasado con una visión de futuro para enfrentar retos y oportunidades. El primer reto atañe a la estabilidad financiera, mientras que el segundo está relacionado con encontrar mejores usos y aplicaciones en los servicios financieros; la oportunidad que implican ambos es promover una mayor inclusión financiera y mayores oportunidades de desarrollo para la población.

Pero para ello es indispensable la estabilidad del sistema financiero y nuevas regulaciones con el fin de hacer frente a los riesgos potenciales que ahora son más difíciles de identificar, al tiempo que su impacto económico, operativo o reputacional es más complicado de cuantificar, porque el vínculo de contagio entre riesgos cambia el proceso de identificación de estos factores, alejándose de la típica medición de la probabilidad de ocurrencia e impacto individual, hacia un modelo que se centra en grupos de riesgos, entre los que está el de la ciberseguridad.

2. Desregulación: se abre la puerta a la innovación

La integración creciente de los mercados y las crisis financieras recurrentes han puesto

[3] "Cómo funcionan los 28 bancos que dominan la economía global", disponible en <https://www.bbc.com/mundo/noticias/2016/03/160325_economia_mecanismos_hidra_financiera_mundial_mj>, consultado el 23 de noviembre de 2019.

énfasis en la regulación en el marco de la nueva arquitectura financiera internacional, que ha ido desarrollando un complejo entramado de instituciones que regulan el sistema financiero internacional.

Para entender la situación actual de la regulación, debe considerarse la evolución de la banca después de la crisis de los años treinta y las fuertes regulaciones que se generaron hasta 1970, año en el que se inició un periodo caracterizado por una mayor liberalización y desregulación, y por las dificultades que se generaron a raíz de la crisis financiera de 2008, relacionadas con el poder de mercado ganado por los bancos más grandes del mundo y con la profundización de la concentración bancaria.

La tendencia de concentración se acentuó con la profundización y expansión del sector financiero a partir del año 2000, lo que puede ser explicado por la posibilidad que tienen los bancos universales de crear poder de mercado y sacar del mismo a bancos más débiles, generando menos competencia y acentuando el poder de monopolio.

El poder de los cinco mayores bancos del mundo se intensificó en el presente siglo, tanto en países ricos como en economías de medianos y bajos ingresos. Asimismo, pudo determinarse la disparidad existente entre el financiamiento obtenido por habitantes de países ricos y sus pares de países con ingresos medios y bajos, lo que permitió encontrar que el margen de intermediación, medido como el valor contable de los ingresos netos por intereses del banco como parte de la ganancia total de activos, muestra que son mayores para los países más pobres, lo que significa que los costos de estos sistemas bancarios resultan más de tres veces onerosos para los habitantes de los países de menores niveles de ingreso en comparación con sus pares que habitan en países ricos.

La regulación después de 1970

La crisis económica que estalló a partir de 1929, resultante de la eminente desaceleración de la economía mundial, la deflación en el precio de los productos agrícolas y de los insumos básicos —base del comercio internacional por esa época— y de la caída de la Bolsa de Nueva York, condujo a la economía mundial a una recesión profunda.

A raíz de lo ocurrido en 1929, se impulsaron cambios en la regulación bancaria, desde el establecimiento de restricciones al ingreso de nuevos bancos y la separación de las actividades de los bancos y de las instituciones del sector financiero no bancarias hasta medidas como la fijación y control de las tasas de interés; en términos generales, puede entenderse que fueron medidas producto de la crisis, así como de políticas intervencionistas del Estado en la vida económica.

En Estados Unidos, en el marco del programa económico New Deal, encaminado a la generación de empleo y al incremento de la demanda, se dio un mayor control de los bancos por parte del Estado. A través de la Ley de Bancos Glass-Steagall de 1933, se estableció:

- La separación de la actividad bancaria de la bursátil.
- La creación de un sistema bancario conformado por bancos nacionales, estatales y locales.
- La expedición de la Ley Antimonopolio (Sherman Act), que permitía sólo 18 por ciento de control por parte una institución financiera nacional, estatal o local, con el fin de evitar la competencia desleal entre entidades.
- La prohibición a los bancos de participar en el manejo de los fondos de pensiones.

- La negativa a los bancos de suscribir acciones conjuntas con otras empresas y de participar directamente del mercado bursátil.
- La creación de una comisión de vigilancia autónoma, la Securities and Exchange Commission, que fue autorizada para aplicar sanciones a bancos y casas de bolsa que se unieran para especular con los recursos públicos.
- La creación de la Federal Insurance Deposit Corporation (FDIC), un órgano autónomo e independiente que vigilaba el comportamiento de los depósitos públicos en los bancos.

El objetivo general de la Ley Glass-Steagall era evitar que los bancos se enfrascaran en actividades especulativas. De esta manera, no sólo en Estados Unidos, sino en la mayoría de las economías avanzadas, la competencia entre las instituciones financieras se mantuvo limitada, regulándose las tasas de interés y las operaciones de la banca universal. Además, se estableció el seguro de depósito y los bancos centrales comenzaron a actuar como prestamistas de última instancia.[4]

Durante la era de Bretton Woods[5] (1945-1971), las operaciones de la banca comercial estaban restringidas en la posibilidad de expansión a través de sucursales y de ser integradas con las actividades de inversión en títulos de valores. El control de capitales se daba como una forma de evitar las crisis monetarias bajo un sistema de tipo de cambio fijo (se estableció una equivalencia fija entre dólares y oro: una onza de este metal valdría siempre 35 dólares, con lo que la moneda estadounidense se convirtió en la divisa de referencia), adquiriendo el sistema financiero un carácter primordialmente nacional y favoreciendo la creación de bancos de desarrollo que apoyaran políticas de desarrollo industrial.

En este periodo se experimentó una gran expansión con leves recesiones, pero no crisis financieras. Sin embargo, este largo periodo de robusto crecimiento creó las condiciones necesarias para que las crisis financieras retornaran. Las innovaciones financieras eludieron la regulación, erosionando las regulaciones del New Deal, y el sistema transitó gradualmente hacia la fragilidad (Nersisyan y Wray, 2010: 5).[6]

En 1971 se rompió el acuerdo de Bretton Woods y en 1973 se presentó la crisis de precios del petróleo por el corte de suministro de los países de la OPEP, en la conocida como primera crisis del petróleo durante la guerra árabe-israelí del Yom Kippur, lo que provocó un incremento del precio del crudo de 2.50 a 11.50 dólares en 1974 y una fuerte crisis en los países más industrializados.

En los años ochenta, con el neoliberalismo, impulsado especialmente por Margaret Thatcher en Inglaterra y Ronald Reagan en Estados Unidos, se rescató el libre mercado y la exigencia de no intervención regulatoria del Estado en la economía.

En el ámbito financiero, a partir de 1971 se generó una ampliación y crecimiento de las masas financieras que condujo a la adopción de medidas de liberalización, permitiendo una rápida expansión en la inte-

[4] CEPAL (2011), "La inversión extranjera directa en América Latina y el Caribe", disponible en <http://www.cepal.org/publicaciones/xml/0/46570/LIE2011esp.pdf>, consultado en diciembre de 2019.

[5] En Bretton Woods, New Hampshire, se establecieron, hace 70 años, las nuevas reglas para las relaciones financieras entre los países industrializados y se trató de poner fin al proteccionismo.

[6] Y. Nersisyan y R. Wray (2010), *The Global Financial Crisis and the Shift to Shadow Banking*, Working Paper 587, Levy Institute Economics.

gración y en los volúmenes de operaciones de capital, lo cual estuvo acompañado de varios factores presentes en las economías desarrolladas, como bajos ritmos de crecimiento, bajo nivel en las tasas de interés y, principalmente, condiciones de abundante liquidez, generada por la emisión de bonos y, en general, de variados tipos de derivados financieros. Algunos autores señalan que los bancos comerciales comenzaron a convivir con el mercado de capitales.

En este contexto, se comenzó a exigir mayor flexibilización de los controles sobre las tasas de interés y se planteó que la desregulación del sistema financiero era necesaria como requisito para lograr un mayor crecimiento económico y mejor desempeño de las economías.

Asimismo, se empezaron a dar presiones por la flexibilización en las regulaciones, en la medida en que la ampliación de los mercados, con el establecimiento de sucursales bancarias y la participación de éstas en los mercados de valores, se convirtió en una alternativa atractiva para el incremento de utilidades del sector bancario. Aunque hasta ese entonces las regulaciones limitaban la participación de la banca en la suscripción de títulos valores, en el mercado se encontraban fuertes incentivos para proponer la libertad de integración de servicios.

Ya en los años noventa, la banca de los países industrializados enfrentaba un escenario marcado por el aumento de la competencia y por grandes excedentes de capital, pero comenzaba a evidenciar intensas presiones para abaratar costos y afrontar la reducción sostenida de los márgenes de rentabilidad. Además, sus mercados internos, que representaban la principal fuente de ingresos, alcanzaban altos niveles de madurez y presentaban escasas oportunidades.

Con el propósito de aprovechar economías de escala, las entidades bancarias aceleraron la adopción de un modelo de banca universal. No obstante, al operar en economías maduras se evidenciaron tensiones entre el gran tamaño que comenzaban a adquirir y la reducción de los márgenes de rentabilidad en las actividades tradicionales de intermediación. De este modo, muchas entidades bancarias comenzaron a buscar oportunidades fuera de sus mercados (CEPAL, 2011).

Todo este contexto, desde la teoría de que el control financiero desalienta el ahorro y contribuye a una mala asignación del crédito, favorecería la idea de desregulación para permitir la libre movilidad de capitales. Bajo ese argumento, en las décadas de los años ochenta y noventa, muchos países realizaron reformas a sus sistemas financieros para permitir la libre movilidad de capitales.

Desde la perspectiva teórica, en un entorno que favorecía y promulgaba la libertad de mercado, los argumentos mostraban las ventajas que podían atribuirse a la liberalización de capitales, y las decisiones de política económica adoptadas en la mayoría de países fueron en torno a adoptar las medidas tendientes a permitirla.

Dentro de las acciones de desregulación que permitieron que fueran configurándose los cambios en los sistemas financieros, está la eliminación de la regulación que impedía la integración de servicios. En Estados Unidos, los bancos lograron, en 1999, que se derogara la Ley Glass-Steagall; su eliminación permitió a los especuladores la integración de mercados de bancos, seguros e inversión, posibilitando una rápida recomposición de grupos financieros mediante procesos de fusiones y adquisiciones entre entidades, como fueron los casos de CitiGroup, HSBC y Deutsche Bank, entre otros. Estados Unidos y Alemania se esforzaron por desarrollar de diferentes maneras la banca universal con el fin de aumentar el poder de la competencia de sus bancos en el mercado

financiero internacional. Esta tendencia se extendió y fueron muy pocos los países que mantuvieron limitaciones en la realización de alguna actividad intersectorial. En 2002, según datos de *The Banker*, los 10 primeros bancos controlaban 8'136,937 millones de dólares, cuando, 12 años antes, la cifra era de 3'059,741 millones.

Con la caída de la Ley Glass-Steagall comenzaron las fusiones y la integración horizontal de la banca en Estados Unidos; un año más tarde se promulgaba la Ley de Modernización de Futuros de Productos Básicos (Commodity Futures Modernization Act), que limitaba el papel regulador y supervisor de las agencias federales sobre el mercado de derivados, como la SEC, lo que favorecía las prácticas financieras más riesgosas (CEPAL, 2011).

A su vez, esta dinámica de liberación del mercado de capitales fue acompañada de la privatización de las empresas públicas, lo cual permitió la expansión del capital trasnacional que se apoderó de bienes públicos a escala global y tomó funciones antes desempeñadas por el Estado.

En México, a principio de la década de 1990, el sistema financiero mexicano, al igual que la estructura macroeconómica del país, experimentó cambios profundos. Algunos de los más significativos, inducidos por la apertura y desregulación del sistema financiero, fueron la reprivatización de la banca comercial, la reducción y reestructuración de la banca pública, el crecimiento de los mercados de capital y de derivados, así como la expansión de las instituciones financieras no bancarias y de los inversionistas institucionales.

El objetivo de estos cambios era elevar la eficiencia macroeconómica del sistema financiero para que condujera a un patrón de financiamiento del desarrollo económico más funcional a la estructura del país; sin embargo, los principales indicadores macroeconómicos no reflejaban un crecimiento financieramente estable y sostenido.[7]

Para Ortiz,[8] el proceso de desregulación y liberalización del sistema financiero se divide en dos etapas. En la primera, 1988-1992, se consolida la constitución de la banca universal; en la segunda, 1993-2001, los cambios se dirigen a flexibilizar el marco regulatorio para estimular la entrada y expansión de nuevas instituciones extranjeras y nuevos agentes financieros en el mercado bursátil, particularmente, los bancos comerciales y de inversión. Los efectos de la primera etapa sólo modificaron las condiciones del crédito externo porque, a partir de 1990, los flujos voluntarios de capitales externos hacia México crecieron rápidamente. Esto provocó un incremento de las reservas de divisas que redujo las limitaciones de la balanza de pagos y creó las condiciones para sostener el programa de estabilidad de precios. En tanto, las modificaciones en el marco regulatorio crearon cambios radicales en el mecanismo de financiamiento-fondeo de la inversión.

Los bancos comerciales pudieron ampliar e integrar mejor la oferta de productos y servicios, así como su alcance en términos espaciales. Bajo una ideología de funcionamiento eficiente de mercados y con las reformas tendientes a la desregulación, fueron gestándose cambios en las estructuras financieras en los ámbitos nacionales e internacionales, dando paso a la integración de

[7] Luis Ángel Ortiz Palacios, "Desregulación financiera y transformación de los mecanismos de financiamiento y fondeo a la inversión en México", disponible en <http://www.economia.unam.mx/publicaciones/econinforma/pdfs/337/06luisnagelortizpalacios.pdf>, consultado el 23 de enero de 2020.

[8] *Idem*.

servicios financieros y a la conformación de conglomerados que posteriormente harían evidentes los problemas relacionados con la concentración de la propiedad financiera.[9]

En 1975 operaban 139 instituciones bancarias, siendo Bancomer uno de los grupos más integrados. Para 1977, de un total de 77 instituciones, las 10 más grandes concentraban 82 por ciento de la captación. Antes de 1982, se da un proceso de fusiones entre los recién constituidos bancos múltiples, de tal forma que antes de la nacionalización existían sólo 40 grupos bancarios privados y mixtos, de los cuales 27 eran bancos múltiples y concentraban 90 por ciento de los recursos totales.[10]

En un contexto de gran desregulación y de tendencia creciente de internacionalización del capital, fueron desarrollándose estructuras de grandes bancos con expansión a nivel mundial a través de la figura de sucursales y filiales con fondos centralizados y la oferta de actividades diversas, por ejemplo, la inversión en títulos, los valores y el corretaje de seguros. Puede decirse que los cambios en las estructuras financieras a partir de 1990 se caracterizaron principalmente por:

- Cambios en la propiedad de los bancos, siendo clara la tendencia de un aumento predominante de los grandes bancos extranjeros y un debilitamiento significativo de los bancos de propiedad pública.
- Cambios en la propiedad; un acelerado proceso de concentración de la industria fortalecido con la integración de operaciones y negocios financieros.
- Mayor integración de los mercados financieros a nivel global.
- Desarrollo de diversos y múltiples instrumentos financieros, producto de las innovaciones financieras.
- Ampliación de la especulación y los riesgos financieros.

Consecuencias

América Latina no fue la excepción y en la década de 1990, después de la crisis de la deuda de los años ochenta, bajo las directrices del denominado Consenso de Washington, se realizaron importantes reformas con el fin de profundizar y mejorar sus sistemas financieros. Estas reformas se basaron principalmente en liberalización de la tasa de interés, cambios en las normas de regulación y supervisión financiera, apertura a la banca extranjera y, en general, a los flujos de capitales provenientes del exterior, creación de nuevos instrumentos de financiamiento y desmantelamiento de la mayoría de instrumentos de crédito dirigido.[11]

En términos generales, aunque en los diseños de los sistemas financieros de cada país existen sus particularidades, puede decirse que esta tendencia de las estructuras financieras se extendió a nivel global, llevando a la consolidación de estructuras oligopólicas, lo que produjo a la vez un incremento significativo de riesgo sistémico en los mercados financieros, con el privilegio de la especulación financiera y en detrimento de la inversión de tipo productivo.

[9] F. E. Salazar y L. C. Guzmán (2015), "Globalización financiera y crisis bancaria ¿producto de los cambios en las estructuras bancarias a partir de 1980?", *Dimensión Empresarial*, vol. 13 (1), disponible en <http://dx.doi.org/10.15665/rde.v13i2.531>, consultado el 23 de enero de 2020.

[10] Ortiz Palacios, *op. cit*.

[11] D. Titelman (2003), "La banca de desarrollo y el financiamiento productivo", CEPAL, disponible en <http://www.cepal.org/publicaciones/xml/7/14027/lcl1980e.pdf>, consultado el 12 enero de 2020.

Con las medidas de desregulación y cambios generados en la economía, la industria financiera con un rápido crecimiento adquirió cada vez mayor relevancia en las economías a nivel local e internacional, pero también acentuó sus vulnerabilidades.

La tendencia a la concentración bancaria con la participación de pocos bancos y la extensión a través de sucursales se dio a partir de los años noventa, de acuerdo con la premisas del modelo neoliberal y especialmente después de la caída de la Ley Glass-Steagall, pero con una característica adicional: el volcamiento hacia estructuras con integración de servicios o banca universal, un sistema en el que los bancos proporcionan una amplia variedad de servicios financieros, incluidos los comerciales y de inversión.

Los bancos universales pueden ofrecer créditos, préstamos, depósitos, gestión de activos, asesoramiento en materia de inversiones, procesamiento de pagos, transacciones de valores, suscripción y análisis financiero. La banca universal combina los servicios de un banco comercial y los de un banco de inversiones, proporcionando todos los servicios desde una sola entidad.

Bajo este sistema, un banco puede elegir participar en cualquiera o en todas las actividades permitidas. Se espera que cumplan con todos los lineamientos que gobiernan o dirigen el manejo apropiado de activos y transacciones. Dado que no todas las instituciones participan en las mismas actividades, las regulaciones pueden variar de una institución a otra. Algunos de los bancos universales más notables son Deutsche Bank, HSBC e ING Bank, Bank of America, Wells Fargo y JPMorgan Chase.

Desregulación y crisis

Como hemos visto, dos periodos se distinguen en la historia reciente del sector financiero. El primero es de regulación estricta, intervencionismo y estabilidad desde los años cuarenta hasta los setenta; el segundo es un periodo de liberalización y mayor inestabilidad desde los años setenta, que culmina en la crisis desatada por las hipotecas *subprime* en 2007. La estabilidad del primero contrasta con el aumento considerable del número de quiebras y crisis del segundo, en el cual el sector fue liberalizado. El origen del aumento de la inestabilidad está en la liberalización acompañada de una inadecuada regulación, como muestran las crisis en Estados Unidos, Japón y Escandinavia. A pesar de estos episodios de crisis, la liberalización financiera ha contribuido al desarrollo financiero general y, por lo tanto, al crecimiento de la economía.[12]

La crisis financiera, que comenzó en el verano de 2007 y afectó, en mayor o menor medida, a la estabilidad financiera de todos los países, cuestionó la ideología de los mercados libres y la liberalización financiera, y llevó a la mesa la necesidad de una regulación financiera eficiente que actuase dentro de determinados parámetros de seguridad sistémica y con una supervisión efectiva para prevenir los excesivos riesgos asumidos como práctica habitual por las instituciones financieras en los años recientes. Además, se requirió de una coordinación regulatoria entre países desarrollados y en desarrollo para obtener soluciones globales a partir del diálogo entre bancos centrales, supervisores y reguladores.

Los cambios de la regulación financiera pueden organizarse en torno a dos grandes bloques: micro y macroprudenciales; los se-

[12] Xavier Vives, "La industria financiera y la crisis: el papel de la innovación" (2018), disponible en <https://www.bbvaopenmind.com/articulos/la-industria-financiera-y-la-crisis-el-papel-de-la-innovacion/>, consultado el 2 de enero de 2020.

gundos contemplan el sistema en su conjunto (riesgo sistémico) y giran fundamentalmente sobre los efectos del grado de interconexión de los diversos participantes en el mercado.

A raíz de la crisis de 2007-2008, el foco apuntó a reconducir ciertas actividades financieras dentro del escrutinio de la regulación —ya sea actuaciones fuera de balance o actividades desarrolladas a través de lo que se conoce como el *shadow system*— y a tener más y mejor capital alineado con los riesgos en los que las entidades incurren, entre otros factores que conducirían a reestructuraciones globales de ciertas entidades, demasiado grandes o demasiado interconectadas para dejarlas caer (*too big to fail*), de tal manera que, dado un proceso de liquidación, éste pueda resultar más fácil y previsto de antemano.

3. Se aprende del pasado: nuevo escenario para la innovación tecnológica

La ventaja sostenible no exige ni la utilización de tecnología sofisticada ni tampoco ser el primero en introducirla en un mercado; por el contrario, requiere la adopción en el momento más adecuado de las innovaciones tecnológicas, coherentes con la misión corporativa, las oportunidades y las amenazas del entorno, así como con el perfil competitivo propio. Tal vez eso pensaron dentro del banco Barclays cuando tuvieron la idea de instalar el primer cajero automático —creado por Sheperd-Barron y comercializado por la firma británica De La Rue— en junio de 1967, del cual, en 2017, según el Banco Mundial, Brasil era el país que más tenía (160 mil) seguido de Japón (casi 105 mil).

Eso demuestra que la innovación tecnológica no es sino un recurso estratégico y, por ello, su contenido óptimo se encuentra sometido a los mismos condicionantes que determinan la selección racional de estrategias por la empresa como recurso general de acción en el mediano y largo plazos.

Entre otras cosas, en el negocio bancario la difusión tecnológica es suficientemente rápida y no hay un único cambio tecnológico, sino multitud de planteamientos tecnológicos que se corresponden con la pluralidad de estrategias óptimas alternativas, determinados por una diversidad de elementos internos y externos concernientes a una empresa financiera concreta.

Si continuamos con el ejemplo del banco británico, podemos mencionar que ha seguido en el camino de la innovación: En 2013, cinco años después de la crisis hipotecaria, implementó Sales Cloud para dar seguimiento a las relaciones de los agentes, así como al volumen y tipo de acuerdos hipotecarios que se contrataban. El argumento del banco inglés fue: "La velocidad es la nueva divisa de los negocios". [13]

Son numerosos los expertos que han puesto de relieve la importancia estratégica de la Tecnología de Información en el sector financiero. Para el Banco Mundial,[14] las nuevas tecnologías aumentarán la digitalización

[13] "Barclays Bank simplifica el proceso de solicitud de hipotecas para miles de agentes y clientes del Reino Unido gracias a una plataforma de vanguardia para la comunidad", disponible en <https://www.salesforce.com/mx/customer-success-stories/barclays/>, consultado el 23 de enero de 2020.

[14] H. M. Queen Máxima y Jim Yong Kim, "La importancia de la tecnología financiera, el uso de las cuentas y la innovación para lograr la inclusión financiera", disponible en <https://blogs.worldbank.org/es/voices/la-importancia-de-la-tecnolog-financiera-el-uso-de-las-cuentas-y-la-innovaci-n-para-lograrla>, consultado el 23 de diciembre de 2019.

y reducirán el costo de la prestación de servicios financieros. Esta transformación digital es vista por BBVA[15] como una puerta del mercado de servicios financieros a nuevos tipos de proveedores: empresas emergentes conocidas como fintechs y, más recientemente, las grandes empresas tecnológicas, como Google, Amazon y Apple (ya conocidas como las *American Big Techs* o GAFAP), que presentan un gran potencial disruptivo para el panorama competitivo por su tamaño y las características de los ecosistemas digitales en los que integran los servicios financieros.

Según BBVA (2018), desde finales de los años sesenta, con la incorporación de las primeras computadoras *mainframe* en los servicios centrales, y más adelante de computadoras personales en las sucursales, las entidades financieras han mecanizado progresivamente operaciones y procesos internos que eran muy intensivos en papel y mano de obra, lo que los llevó a ser más eficientes y a aprovechar más las ganancias de eficiencia. "Si hay algo que distingue la oleada más reciente de transformación digital es que, además de introducir nuevas ganancias de eficiencia en la operatividad de las entidades, ha alterado de forma significativa la forma de relacionarse con los clientes, ha dado lugar a nuevos servicios y modelos de negocio y ha reducido algunas de las barreras de entrada que hacían del sector financiero un mercado relativamente estanco", apunta BBVA.

Eso es evidente si consideramos el contexto de las etapas históricas de la incorporación tecnológica en la banca:

1. **Años sesenta.** Privaba una estrategia de reducción de los costos, mejora de la productividad y mayor seguridad, en un entorno de restricciones importantes derivadas de las propias limitaciones informáticas y de la falta de capacitación del personal que trabajaba en las entidades.
2. **Años setenta.** Se introdujo en el negocio bancario el teleproceso con el objetivo de mejorar el servicio ofrecido a los clientes y de conseguir una mayor rapidez en la gestión de la entidad, si bien también presentaba limitaciones en cuanto al sistema de telecomunicaciones que se precisaba, así como a la homologación y normativa.
3. **Años ochenta.** Con el propósito de conseguir una mayor autonomía, nuevos puntos de venta, introducir la ofimática y los sistemas de información para la dirección, se introdujo el sistema de banca electrónica.
4. **Años noventa.** Comenzó a introducirse el sistema de banca *online* o virtual, a través del cual se persigue la descentralización de muchas funciones, la reducción de puntos de venta, y la comunicación y distribución a través de la red.

El resultado de esas incorporaciones ha sido una disrupción —una veces más acelerada que otras— que ha transformado, y sigue haciéndolo, el panorama competitivo y la estructura del mercado de servicios financieros, que actualmente tienen en la mira, principalmente, tres grandes avances tecnológicos: las redes de banda ancha y los dis-

[15] Santiago Fernández de Lis y Pablo Urbiola Ortún, "Transformación digital y competencia en el sector financiero", 2018, disponible en <https://www.bbvaresearch.com/wp-content/uploads/2019/01/Transformacion-digital-y-competencia-en-el-sector-financiero-vf3_edi.pdf>, consultado el 5 de diciembre de 2019.

positivos móviles inteligentes, los servicios de computación en la nube y la explotación de grandes cantidades de datos, así como la inteligencia artificial en el contexto de dos fuerzas: la experiencia del consumidor y los beneficios económicos.

Estos avances han sido propiciados por la transformación digital y ésta ha fomentado la incorporación de nuevos participantes en un escenario para la innovación tecnológica, en el marco de una desregulación a la que, precisamente, los nuevos participantes propician que se le quite el prefijo *des* para actuar en un marco abierto, pero con reglas que eviten repetir situaciones del pasado.

Nuevos jugadores: American BigTechs (Google, Amazon y Apple), AsianTechs, Neo y Challengers Banks y fintechs

El informe "Impacto de los competidores en el ROE bancario en 2024"[16] se centró en los cuatro principales nuevos jugadores del sistema financiero: American BigTechs (Google, Amazon y Apple), AsianTechs, Neo y Challengers Banks y fintechs, y se destacó su importancia en la reconfiguración del sistema financiero.

Llegaron las grandes: American BigTechs y/o GAFP

De las American BigTechs, el informe "Impacto de los competidores en el ROE bancario en 2024" señaló que mueven en la actualidad 51 billones de dólares en transacciones entre 215 millones de usuarios (en contraposición, ICBC mantiene 475 millones de usuarios; Banco Santander, 121 millones; JPMorgan Chase, 66 millones; HSBC, 38 millones, y BNP Paribas, 35 millones de usuarios) y que de éstas, Apple tendrá un mayor impacto en el sector bancario global, seguido por Google y Amazon. Esto se debe a que mantienen una alta cuota de mercado, elevados volúmenes de datos, buena imagen de marca, gran capital y apetito por generar más valor.

En el informe se plantea la pregunta de si realmente esas "grandes" quieren ser bancos o colaborar con ellos y hasta qué punto van a ofrecer servicios financieros complejos o si se quedarán la mayoría en los pagos.

Actualmente, todas esas empresas tienen algún producto o servicio relacionado con el mundo de las finanzas. "Amazon destaca por su variedad, aunque ninguna ha mostrado una estrategia clara hasta el momento en su camino por competir fuertemente en el sector".

Según el informe mencionado, se cree que de entre las GAFP (Google, Amazon, Facebook, Apple y PayPal), Apple será la que más mermará el negocio de la banca tradicional en los próximos cinco años. Según su análisis, si se aíslan todos los cambios del entorno y se considera sólo el contexto macroeconómico esperado, la banca alcanzaría un ROE de 9.3 por ciento en 2024. Sin embargo, es imposible no considerar los cambios tecnológicos y la estrategia propuesta por cada banco en términos de transformación digital e innovación abierta, algo que "muy pocos hacen a la hora de elaborar sus previsiones", que se basan tan sólo en la evolución de los tipos de interés, el impacto de las provisiones o los cambios regulatorios.

Pero si se toma en cuenta la cuota de mercado perdida (*Market Share Lost*) y la re-

[16] Finnovating, 2019, "Impacto de los competidores en el roe bancario en 2024", disponible en <https://www.finnovating.com/news/impacto-de-los-competidores-en-el-roe-bancario-en-2024/>, consultado el 12 de enero de 2020.

ducción de los márgenes debido a la aparición de modelos más digitales con procesos muy eficientes (*Margin Profit Erosion*), según la misma fuente, Apple será entre las American Big Techs la que mayor impacto genere en la merma del ROE del sector financiero global, tanto por la pérdida de cuota de mercado que va a suponer a la banca tradicional como por la reducción de los márgenes que van a implementar a través de la eficiencia que aporta la digitalización de sus sistemas.

Bajo estas mismas variables, Google provocará un impacto similar en la pérdida de cuota de mercado, pero será menor en términos de reducción de márgenes, seguida por Amazon. En total, sólo estas tres compañías restarán casi 1 por ciento al ROE bancario en cinco años, por la pérdida de mercado, y otro 0.5 por ciento por el recorte de múltiplos.

El informe destaca los productos de las firmas en cuestión:

- **Apple.** Apple Card y Apple Pay. La primera es una tarjeta de crédito creada con el banco americano Goldman Sachs en febrero de 2019, diseñada para funcionar con Apple Wallet. El segundo es un servicio de pago móvil o cartera digital, que permite a los usuarios realizar pagos mediante aplicaciones iOS y web. Este servicio está presente actualmente en 21 países con 127 millones de usuarios, superando a Amazon y a Google, y un volumen de transacciones por año de 17 mil millones de dólares.
- **Google.** Cuenta con Google Pay. Este producto financiero es la fusión de Google y Android Pay; es un sistema de pago *online* o cartera digital para potenciar las compras mediante dispositivos móviles a través de *tap-to-pay*. Al cierre de 2019, contaba con 30 mil millones de usuarios en 17 países y movía anualmente 30 mil millones de dólares. La compañía se asoció recientemente con cuatro bancos indios para conceder préstamos en línea al consumo. Además, en diciembre de 2018, Google obtuvo una licencia del regulador lituano, y posteriormente del irlandés, que le permite operar como entidad de dinero electrónico en toda Europa. Asimismo, cuenta con uno de los VC más activos en inversión fintech, entre la que se encuentra Lending Club, la mayor fintech del mundo.
- **Amazon.** Cuenta con Amazon Pay, Amazon Lending y Amazon Cash. El primero tiene más de 33 millones de usuarios en 17 países; el volumen de transacciones por año es superior a 3 mil millones de dólares. El segundo es un programa bajo invitación que otorga préstamos a compañías de hasta 750 mil dólares. En 2017 concedió más de mil millones en cuatro países a más de 20 mil empresas. El tercero está disponible en Estados Unidos y México; brinda la posibilidad de añadir dinero en efectivo al saldo de la cuenta Amazon. En 2018, Amazon firmó una alianza estratégica con Bank of America para expandir su programa de préstamos y el producto Amazon Lending.

Del otro lado del mundo: Asian Techs

Respecto a las Asian Techs, originadas en China, una gran mayoría apunta a que han llegado para cambiar las reglas del juego en el sector bancario. "Más evolucionadas que las BigTechs, buscan incluir productos y servicios financieros de forma transparente en la vida cotidiana de sus clientes", asegura el documento de Finnovating (2019).

Las Asian Techs están lideradas por Alibaba, Baidu y Tencent; el estudio "Fintech

y estructura del mercado en servicios financieros: Desarrollo del mercado y posibles implicaciones para la estabilidad financiera"[17] señala que son muy activas en una amplia gama de servicios financieros y, en muchos casos, se asocian con las principales instituciones financieras o nuevos jugadores de fintechs.

Al inicio de 2019, Alibaba agrupaba a nueve empresas, las cuales demuestran su alcance:

- Taobao.com. Un *marketplace* que tiene similitudes con eBay. Es definido por Alibaba como "*social commerce*"; es el líder chino en *eCommerce* vía móvil.
- Tmall. El mayor *eCommerce* B2C de China, en el que marcas de todo el mundo, como las de Inditex, cuentan con tienda propia.
- Aliexpress. Un *marketplace* global pensado para que las marcas chinas hagan llegar sus productos a clientes de todo el mundo.
- Alibaba.com. Un *marketplace* B2B que actúa en 180 países de todo el mundo.
- 1688.com. *Marketplace* chino especializado en productos para el hogar y decoración.
- Alimama. Plataforma de marketing digital que ofrece servicios a los vendedores que utilizan los *marketplaces* del grupo.
- Alibaba Cloud. Uno de los mayores proveedores de servicios IaaS (*Internet as a Service*) del mundo, que ofrece servicios *cloud* a compañías de todo el planeta.
- Ant Financial. Nació en 2014 y agrupa el negocio generado por Alipay (el medio de pago *online* del grupo), que fue lanzado en 2004.
- Cainiao. El operador logístico del grupo, que ofrece soporte a las actividades de Alibaba en China.

Aunque en China tienen varias opciones para buscar información, el más usado es el buscador Baidu, el cual cuenta con una interfaz muy atractiva y los resultados que se ofrecen son muy rápidos. Este buscador en Estados Unidos apenas tiene 1.1 por ciento de visitantes, cuando en China tiene 90.9 por ciento. Baidu anunció que estaba desarrollando sus propias gafas inteligentes y coche autónomo capaz de conducirse sólo, únicamente cuando las persona así lo requieran. A 14 años de su fundación, se coloca en el quinto lugar del ranking mundial.

Tencent es una de las 10 más poderosas empresas del mundo y una de las más valiosas. Se trata de un conglomerado que se fundó en China hace casi 20 años y hoy es un gigante de las telecomunicaciones y el entretenimiento, que cuenta con servicios de mensajería, realidad virtual, bienes raíces y fintech. Además, fabrica *smartphones* y computadoras.

En 2017, Tencent Holdings tenía 44,796 empleados e ingresos anuales por 36 mil millones de dólares. La empresa china apunta a una expansión internacional, por lo que podría convertirse en los próximos años en una de las empresas más valiosas y poderosas al lado de Apple, Facebook y Microsoft.

[17] Financial Stability Board, 2019, "Fintech y estructura del mercado en servicios financieros: Desarrollo del mercado y posibles implicaciones para la estabilidad financiera", disponible en <http://www.asbasupervision.com/es/bibl/x-lecturas-recomendadas/1864-fintech-y-estructura-de-mercado-de-servicios-financieros-desarrollos-del-mercado-y-potenciales-implicaciones-en-la-estabilidad-financiera>, consultado el 20 de diciembre de 2019.

Totalmente digitales: Neo y Challenger Banks

De los Neo y Challenger Banks —que nacieron en 2013 y que a través del uso de canales 100 por ciento digitales ofrecen productos y servicios financieros, en muchos casos sin costo— Finnovating (2019) hace una pregunta: ¿podrán consolidar su posición, crecimiento y ser rentables?

Los Neo Banks ofrecen una experiencia *mobile-first* con un *partnership*, banco tradicional que hace de depositario del dinero y se encarga de temas como: cumplimiento normativo, *Know your Customer* (KYC) o controles y procesos de supervisión que tenga una entidad para conocer a sus clientes, lavado de dinero, etcétera. En resumen, desarrollan una capa *front-end* sobre unos servicios y una infraestructura de un banco tradicional.

Actualmente se conoce a Nubank como el neobanco más grande del mundo. Uno de los aspectos que ha impulsado el crecimiento de este banco brasileño, que ya cuenta con 12 millones de clientes, es la facilidad de abrir una cuenta y el servicio a clientes. Nubank ya tiene presencia en México.

Los Challenger Banks aspiran a convertirse en *fully-licensed banks*, creando una nueva experiencia bancaria para el cliente, con un modelo *data-driven* y con nuevas propuestas de precios, productos y servicios, propios o de terceros. En esa categoría se presenta Xpats, el primer Challenger Bank mexicano que nace del entendimiento de que hay un nicho de población, con grandes necesidades y potencial de desarrollo de servicios financieros, que hoy está absolutamente desatendido en su necesidad de inclusión financiera, más allá de la segmentación socioeconómica: los extranjeros.

Crecen las pequeñas: fintechs

En lo que respecta a las fintechs, para 2019 era un ecosistema compuesto por más de 15 mil *startups* y *saleups* a nivel mundial, que ya han recaudado más de 120 mil millones de dólares en los últimos siete años, según el informe de Finnovating (2019).

¿El futuro de las fintechs comienza hoy? Esta pregunta podría tener respuestas encontradas. Para algunos, es una tendencia y, para otros, es una realidad irrefutable; ambas visiones se sustentan en los hechos. De acuerdo con el Global Fintech Adoption Index 2019 de la firma EY,[18] a nivel global, 64 por ciento de los usuarios digitales utiliza servicios fintech, principalmente para pagos; en la versión de 2015, el porcentaje fue de 16 por ciento y en la de 2017, de 33 por ciento.

Según EY, la adopción de tecnología financiera entre los consumidores casi se ha duplicado en los últimos 18 meses y la tasa está creciendo más rápido de lo previsto, pues la mayoría de los usuarios digitalmente activos en todo el mundo conoce al menos un servicio de tecnología financiera que les puede ayudar a transferir dinero y realizar pagos.

En México, siete de cada 10 usuarios digitalmente activos utilizan opciones fintech, lo que colocó al país en 2019 como el octavo a nivel mundial con el mayor índice de adopción de estos servicios, según el estudio de EY que coloca a la cabeza a China y a la India, con una adopción de 87 por ciento; el de México es de 72 por ciento, en tanto que en 2017 la tasa que presentó fue de 36

[18] Global FinTech Adoption Index 2019, disponible en <https://fintechauscensus.ey.com/2019/Documents/ey-global-fintech-adoption-index-2019.pdf>, consultado el 10 de enero de 2020.

por ciento. EY menciona que México supera a países como Irlanda, Reino Unido, Argentina e, incluso, Estados Unidos.

El sector fintech está creciendo rápidamente y, sin duda, el panorama es muy positivo y, no obstante los retos (como el de la regulación), continúa siendo una alternativa a los servicios financieros que ofrece la Banca Abierta,[19] así como punta de lanza para la nueva fase de innovación llamada Open X,[20] la cual requiere mayor colaboración y especialización en un mundo en el que la tecnología ya no puede separarse del mundo financiero, a partir de las premisas de ofrecer mayor variedad de servicios, menos costosos y más eficientes.

Hay muchos parámetros para sustentar lo anterior, como la inversión a nivel mundial en la industria de fintechs, que en 2018 fue de 111,800 millones de dólares, o la cantidad de fintechs en el mundo (el cálculo, dependiendo de la fuente, va de 12 mil a 15 mil), de las cuales 39 han alcanzado el adjetivo de "unicornio", la nomenclatura empleada para definir a una compañía cuyo valor de mercado ha superado los mil millones de dólares. En conjunto, estas compañías están valuadas en 147 mil millones de dólares.

A nivel global, América ha sido el continente que ha visto el mayor desarrollo de la industria fintech. Tan sólo en 2018, la inversión superó la cifra de 54,500 millones de dólares, de los cuales 96.33 por ciento se colocó en Estados Unidos, país en el que todavía no existe una regulación vigente estandarizada, como es el caso de México, donde desde marzo de 2018 se tiene una Ley Fintech.

En el mundo fintech, el área que registra mayor inversión dentro de todo el espectro es la relativa a los pagos digitales, razón por la cual empresas como Apple, con el lanzamiento de su tarjeta de crédito, o Facebook, con la criptomoneda Libra, han incursionado en el sector. De hecho, Apple forma parte de las American BigTechs, de las que se ha expuesto en otro apartado.

Si bien las fintechs se han abierto camino en la banca tradicional y han sido el

[19] Open Banking es una tendencia que fomenta e impulsa a las instituciones financieras a abrir su infraestructura para conectar a terceros que podrán desarrollar ecosistemas digitales a favor de sus clientes y/o usuarios. El Open Banking (como se le conoce en inglés) es un esquema que permite a consumidores y empresas compartir de forma eficiente y segura su información bancaria con terceros (con previa autorización) para disfrutar de servicios financieros modernos, eficientes y a la medida. En este esquema, el banco emisor del cliente da acceso al proveedor externo a través de API abiertas. Una Interface de Programación de Aplicaciones o API (por sus siglas en inglés) es una tecnología ampliamente utilizada en el mercado mundial de servicios digitales y reconocida por su seguridad en el acceso e intercambio de información. Los bancos llevan varios años utilizando API internas para facilitar el intercambio de información entre diferentes unidades institucionales. Lo que cambia con la Banca Abierta es poder utilizar API para comunicarse externamente con socios estratégicos, programadores o emprendimientos de tecnología financiera (o Fintechs) y de esta forma acelerar ciclos de innovación de productos y servicios financieros. Un "banco abierto" es como una plataforma central de funcionalidad básica (por ejemplo, depósitos y otros servicios básicos), pero con un factor valor agregado inmenso por su capacidad de canalizar un ecosistema de innovación digital ofrecido por terceros.

[20] "La colaboración será el pilar de los futuros servicios financieros", comenta Vincent Bastid, secretario general de EFMA. "En la era del Open X, los participantes en el ecosistema tendrán que trabajar unidos de una manera más efectiva que antes. Los bancos y Fintech sólo podrán prosperar y prestar un servicio mejor a sus clientes mediante la colaboración y la creación de nuevas funciones especializadas. Es evidente que quedan todavía en pie muchas barreras y es una necesidad imperiosa derribarlas para lograr un beneficio colectivo", concluye.

objetivo de desarrollar el concepto de Banca Abierta que ha dado paso al Open X, el crecimiento y desarrollo de las fintechs aún se encuentra en una etapa temprana en la que aplicará la teoría de Darwin, donde los sistemas de regulación que se implementen definirán el modelo fintech que habrá de seguirse en la mancuerna permanente implementación-innovación.

Big Tech, ¿competencia o alianza?

En 2019, la presencia de los grandes tecnológicos Google, Apple, Facebook y Amazon (GAFA) en el mercado mexicano de servicios financieros era un hecho. Bancos y fintechs los tienen en su agenda y en la mira en cuanto a regulación, entre otros temas, que podrían referirse a competencia o alianza.

En ese marco, en el nuevo panorama los actores, los tradicionales (bancos) y los recientes (fintechs), ponen sobre la mesa dos temas: innovación y riesgos, por lo que consideran que debe aplicarse la misma regulación a la misma actividad. Algunos puntos de vista son:[21]

- **BBVA México.** Ante productos y riesgos iguales debe tenerse una misma regulación para no generar asimetrías entre unos jugadores y otros. Y, sobre todo, que esa regulación proteja al público ahorrador [...] Siempre un competidor es un riesgo, es una amenaza en cualquier industria.
- **Santander México.** Lo principal es que todos operen bajo el mismo terreno, mismas condiciones y mismos requerimientos. La regulación tiene que ser igual, deben tener los mismos requerimientos que el resto de los participantes.
- **Scotiabank México**. Las grandes tecnológicas son grandes competidores y han puesto énfasis en algo que la banca no necesariamente puso antes: la experiencia del cliente. Es muy importante que la regulación sea pareja y equivalente para que todos tengamos los mismos requerimientos de información, de autenticación y de controles vinculatorios con esa clientela. De otra manera, lo que estaríamos viendo sería un arbitraje a favor de estas entidades, hasta el momento no reguladas en un alto porcentaje de sus actividades o reguladas de una manera muy diferente.
- **Citibanamex**. La mejor manera es trabajar juntos. El modelo de colaborar es lo que va a terminar subsistiendo.

El estudio "Fintech y estructura del mercado en servicios financieros: Desarrollos del mercado y posibles implicaciones para la estabilidad financiera"[22] señala que, en algunas jurisdicciones, grandes empresas de tecnología bien establecidas han ingresado recientemente en los mercados de servicios financieros. Como ejemplo, menciona:

- Alibaba, Baidu y Tencent. De origen chino, están activas en una amplia gama de servicios financieros y en muchos casos se asocian con las principales instituciones financieras o nuevos jugadores de fintechs.
- Amazon tiene una asociación con Bank of America en préstamos para pequeñas empresas y podría relacionarse con bancos sobre un producto de cuenta corriente.

[21] "Bancos piden que *big tech* tengan las mismas reglas en servicios financieros", *El Economista*, disponible en <https://www.eleconomista.com.mx/sectorfinanciero/Bancos-piden-que-big-tech-tengan-las-mismas-reglas-en-servicios-financieros-20190414-0072.html>.

[22] Financial Stability Board.

- PayPal está incrementando los préstamos a las empresas en Australia, Japón y el Reino Unido.
- Vodafone M-Pesa tiene 32 millones de usuarios activos en pagos en África Oriental, Egipto e India, y en Kenia ofrece productos de crédito y depósitos a través de M-Shwari.
- Mercado Libre, con su plataforma de comercio electrónico, ha prestado en América Latina 127 millones de dólares en varios mercados a finales del 2017. Está experimentando con productos de seguros y gestión de activos.

El documento refiere que las empresas de *Big Tech* pueden tener acceso a las tecnologías de vanguardia para procesar *big data*, incluida la computación en nube, la inteligencia artificial y el aprendizaje automático, porque pueden disfrutar de algunas ventajas competitivas sobre las empresas de servicios financieros.

Un artículo de la calificadora Standard & Poor's[23] indica que Amazon está evaluando la posibilidad de adoptar el CoDi para que sus clientes mexicanos puedan pagar utilizando la tecnología de escaneo con códigos QR. Por ello, en opinión de S&P, la colaboración futura entre los bancos comerciales mexicanos y las compañías fintech será fundamental para competir con los titanes de la tecnología, que tienen una gran fuerza financiera y bases de clientes más sólidas.

Los cambios que se están dando en el tema tienen su sustento en el hecho de que el sector financiero mexicano ha mostrado gran adaptabilidad ante los cambios en las condiciones de negocio, gracias a su adopción de soluciones tecnológicas, como se menciona en el estudio "The State of Innovation in Latin America",[24] en el cual se evaluó el grado de innovación a partir de innovación, capacidad de ejecución, uso de nuevas tecnologías y capacidad de potenciar soluciones innovadoras.[25]

En el estudio, se plantea que acciones como la expansión del acceso a la banca, el desarrollo de soluciones omnicanal y métodos de pago alternativos para los consumidores que no tienen acceso a servicios bancarios hicieron que se catalogara positivamente al país. Se reconoce que cinco de las compañías más innovadoras de América Latina operan en México: BBVA, Banregio, HSBC (encabezan a las del sector bancario y tecnología de pagos), Amazon y Aeroméxico (lideran en *eCommerce*). Además, se menciona a Oxxo como uno de los líderes en innovación tradicional, mientras que, en el segmento de *startups*, PayClip y Conekta encabezan las compañías de la comunidad fintech.

[23] S&P Global Ratings, "El futuro de la banca: Tecnología e innovación podrían expandir el acceso a los servicios bancarios en México", 2019, disponible en <https://www.spratings.com/documents/20184/1493074/2019-03-26-El-futuro-de-la-banca-Tecnologia-e-innovacion-podrian-expandir-el-acceso-a-los-servicios-bancarios-en-Mexico/681ac5b6-2e82-79a7-168f-54a6b7cd04ae>, consultado el 11 de diciembre de 2019.

[24] Visa, 2019, "El panorama de la innovación en América Latina: Lecciones de las empresas innovadoras de la región", disponible en <hhttps://www.visa.com.pe/dam/VCOM/regional/lac/SPA/Default/The%20Visa%20Difference/Innovation/el-panorama-de-la-innovaci%C3%B3n-en-am%C3%A9rica-latina.pdf>, consultado 18 de diciembre de 2019.

[25] El reporte explora los indicadores y tendencias de múltiples organizaciones en América Latina, mediante la evaluación de su nivel de innovación desde la perspectiva de pagos y servicios financieros. Entre los países participantes se incorporó a los principales mercados de la región, como Argentina, Brasil, México, Chile, Colombia y Perú.

CUADRO 1.

¿Que hace que sean innovadoras?

Fuente: "El panorama de la innovación en América Latina: Lecciones de las empresas innovadoras de la región", Visa, 2019.

Banca Abierta: colaboración inminente

La Banca Abierta es un nuevo modelo bancario comparable al nacimiento de la banca telefónica u *online*. Para ello, las entidades deben activar un sistema tecnológico mediante API abiertas (enlaces tecnológicos que contienen información). De esta forma, terceras empresas pueden acceder a sus datos y obtener información sobre el comportamiento financiero de sus usuarios.

Esta modalidad de banca da la posibilidad de contratar productos financieros basados en las necesidades y posibilidades del cliente. Además, podrá tenerse toda la información sobre todas las cuentas, tarjetas y el resto de los productos contratados en más de un banco en una única aplicación.

El concepto de Banca Abierta u *Open Banking* surge de la normativa impulsada por la Unión Europea llamada Revised Payments Service Directive (PSD2),[26] que tiene por objetivo solicitar a los bancos que compartan la información de sus clientes con otras entidades que no sean bancarias. Se trata de un impulso para las empresas fintech que quieren hacerse un hueco en el mercado.

La regulación PSD2, que entró en vigor en enero de 2018, permite a los consumidores compartir sus datos financieros de forma segura con bancos y terceros, posibilitando que transfieran fondos con mayor facilidad, comparen y contraten nuevos productos o servicios y administren sus cuentas sin la participación de su banco.

Un estudio realizado por Accenture[27] señala que 99 de los 100 bancos más importantes del mundo planean invertir fuertemente en iniciativas de *Open Banking* para 2020. Sin embargo, a pesar de las ventajas que propone esta modalidad, los consumidores parecen tener sus dudas y preocupaciones acerca de los servicios financieros proporcionados por terceros no financieros.

La directiva PSD2 (y el concepto de *Open Banking* en su conjunto) quieren ser la palanca clave para optimizar el sector ban-

[26] "¿Qué es y cómo nos afecta la nueva Directiva PSD2?", disponible en <http://www.legaltoday.com/blogs/transversal/blog-ilp-abogados/que-es-y-como-nos-afecta-la-nueva-directiva-psd2>, consultado el 12 de enero de 2019.

[27] Accenture, s.f., "PSD2: How can banks seize the opportunities?", disponible en <https://www.accenture.com/us-en/insight-psd2- opportunities-banks#block-overview>.

cario y, al mismo tiempo, dar a los clientes mayor control y más información sobre sus datos financieros.

No obstante, a pesar de las supuestas ventajas del *Open Banking* para los usuarios, no ha habido una demanda activa de los clientes por productos innovadores. Por ejemplo, en Reino Unido, sólo 18 por ciento de los clientes saben lo que es el *Open Banking*, según un informe del Open Data Institute.[28] Este mismo informe sugiere que aún hay un apego importante a las marcas y métodos de banca tradicionales.

Paradójicamente, los bancos tradicionales se están convirtiendo en una herramienta clave para la difusión de la innovación procedente de las *startups*, que han tenido a menudo dificultades para facilitar la adopción de sus productos o servicios. El acceso a la base amplia de clientes de la banca tradicional por medio de API abiertas ha resultado crucial para avanzar.

En Reino Unido, hasta junio de 2018 había 1.2 millones de usuarios de API de Banca Abierta, casi el doble de los 720 mil usuarios de mayo, según la Open Banking Implementation Authority. Sin embargo, a pesar de estas alentadoras cifras, las fintechs afrontan obstáculos para acceder e integrarse con los bancos tradicionales porque éstos aún no están preparados para ser "abiertos por defecto", como lo son sus rivales digitales, que se crearon de cero con la integración de API en mente.[29]

Luego de la entrada de PSD2 en enero de 2018, se esperaba la implantación en septiembre de 2019 de los estándares técnicos SCA (autenticación reforzada del cliente) y SCS (estándares abiertos seguros de comunicación) de la Autoridad Bancaria Europea, normas que determinarían cómo los bancos podrían permitir el acceso a los datos del cliente a terceros autorizados con los que se integren. Según algunos puntos de vista, los estándares técnicos podrían ser un gran obstáculo para la innovación si los bancos no están convenientemente preparados, pero también podrían ser un estímulo para acelerar la colaboración de todo el sector en la *estandarización de las API para conseguir que el proceso sea más sencillo para todas las partes.*

La Banca Abierta desde una perspectiva internacional

Canadá

En el presupuesto de 2018 de Canadá, se anunció que el gobierno iniciaría una consulta para revisar los beneficios de la Banca Abierta para el sector bancario canadiense. El ministro de Finanzas en funciones en ese momento y el Comité de Asesoría sobre Banca Abierta dirigirían dicha revisión con el apoyo de una secretaría del Departamento de Finanzas y otros representantes de los intereses de todos los canadienses. En junio de 2019, el Comité Permanente del Senado para la Banca, la Industria y el Comercio publicó su reporte titulado "Open Banking: What It Means For You", el cual incluye una serie de recomendaciones para sentar las ba-

[28] "Open Banking, Preparing forlift of", disponible en <https://www.openbanking.org.uk/wp-content/uploads/open-banking-report-150719.pdf>, consultado el 5 de enero de 2019.

[29] "PSD2 y open banking: lo mejor aún está por llegar", 2018, disponible en <https://www.bbva.com/es/psd2-open-banking-mejor-aun-esta-llegar/>.

ses para el lanzamiento la Banca Abierta en Canadá.[30]

Estados Undios

En Estados Unidos hay un mercado grande y establecido de "screen-scraping". El movimiento hacia un Sistema de Banca Abierta ha sido encabezado por la Asociación Estadounidense de Pagos e Interoperabilidad Bancaria (NACHA, por sus siglas en inglés). El programa de estandarización de la Interfaz de Programación de Aplicaciones (API, por sus siglas en inglés) de NACHA se anunció a finales de 2017, basándose en tres áreas: reducción de fraudes y riesgos, intercambio de datos y acceso a pagos. Además, los principios de intercambio de datos de la Procuraduría de Protección Financiera del Consumidor de 2017 invitan a los bancos a introducir API para el intercambio de datos, aunque no las obliga a hacerlo.

México

México ha adoptado en gran medida el modelo de implementación del Reino Unido, pero también planea incluir API especiales pagadas desde el inicio. La ley que regula las instituciones financieras tecnológicas entró en vigor en marzo de 2018, y también rige la Banca Abierta y establece una regulación más estricta para las empresas fintech. El gobierno está finalizando la implementación general y es probable que la Banca Abierta en México sea regulada por la Comisión Nacional Bancaria y de Valores. Los principales objetivos son incrementar la innovación y la inclusión financiera, más que la competencia.

Nigeria

La Fundación de Tecnología Abierta (Open Technology Foundation), una organización no lucrativa, lanzó la Open Banking Nigeria (OBN) en 2018 con el propósito de promover la innovación y las opciones del sector bancario de Nigeria. Su objetivo es implementar API abiertas y motivar a los bancos y fintechs a adoptar normas abiertas para la implementación de API. A diferencia de muchos otros regímenes de Banca Abierta, la OBN considera que la norma británica es demasiado compleja para los propósitos de Nigeria. Esperan redactar su propia norma, la cual será más adecuada para Nigeria y otros países de África Occidental. La OBN espera que el marco de API reducirá el costo de la innovación a los proveedores de servicios y ofrecerá una buena experiencia al cliente. Adédèjì Olówé, fiduciario de Open Banking Nigeria, señaló que esperaba que Open Banking revolucionara el sector bancario nigeriano y diera un gran impulso para la economía en general.

Europa

La Directiva de Servicios de Pago 2 (PSD2, por sus siglas en inglés) es la fuerza rectora del intercambio de datos bancarios en Europa. A diferencia del Reino Unido, no hay un organismo regulador de implementación equivalente a la Open Banking Implementation Entity (OBIE), y los bancos han buscado diseñar voluntariamente sus propias normas. Se han propuesto diferentes normas por entidades regulatorias en representación de distintas coaliciones de bancos europeos. Éstas han tendido a ser menos prescriptivas

[30] "Open Banking: What It Means For You", disponible en <https://sencanada.ca/en/info-page/parl-42-1/banc-open-banking/>, consultado el 13 de enero de 2020.

que las normas de Reino Unido, con una mayor flexibilidad en la implementación técnica y menos enfoque en las experiencias del usuario.

India

India ya es un jugador avanzado en Banca Abierta, pues ya lanzó la Unified Payment Interface (UPI) en 2016. La UPI, desarrollada y administrada por la National Payments Corporation of India (NPCI), facilita las transacciones interbancarias a través de un método robusto de API junto a una solución de identidad digital aplicada actualmente en la mayoría de los mercados europeos y norteamericanos. La iniciativa de Banca Abierta de India aún no ha desarrollado un elemento de intercambio de datos. La Banca Abierta de India está construida, en parte, en Aadhar, la plataforma de identidad nacional del país. A partir de marzo de 2019, 142 bancos utilizan UPI, representando poco menos de 800 millones de transacciones al mes con un valor combinado de 19 mil millones de dólares.

Japón

En mayo de 2017, La Amended Banking Act introdujo un sistema de registro de terceros (Third Party Providers-TTP) y establece el método de colaboración entre los bancos y TPP. La ley insta a los bancos a abrir sus API en 2020, especialmente, para habilitar los pagos digitales antes de los Juegos Olímpicos. También ha habido asociaciones voluntarias entre instituciones financieras para lanzar iniciativas de pago digitales. Sin embargo, la adopción por parte de terceros ha sido baja, en cierta medida, debido a las dificultades que tienen los bancos y fintechs en la negociación de contratos.

Singapur

Singapur está convocando a las instituciones financieras a adoptar las API para promover la innovación y la interoperabilidad. En Hong Kong, la Autoridad Monetaria de Singapur (Monetary Authority of Singapore-MAS) no está adoptando un enfoque intervencionista ante la Banca Abierta. Como señaló el Chief Data Officer de MAS, "el camino hacia la Banca Abierta en el país será más exitoso si los actores de la industria no asumen una posición estricta". MAS y la Asociación de Bancos de Singapur publicaron un manual detallado sobre las API para motivar a más bancos a participar en la iniciativa. Desde entonces, Citibank, DBS, Standard Chartered y otros bancos han lanzado sus propios portales de API.

Australia

A pesar de importantes similitudes técnicas entre las normas de Reino Unido y Australia, hay diferencias en cuanto a su cobertura. Esto se deriva de la introducción por parte del gobierno australiano de la legislación intersectorial de Derechos de los Datos del Consumidor (Consumer Data Right legislation (CDR)26. La CDR se aplicará a un conjunto más amplio de datos del consumidor que los datos bancarios, a la cual pronto le seguirán los datos de energía y telecomunicaciones, con el propósito de establecer la interoperabilidad de los datos a través de diferentes sectores. La implementación de la Australian Open Banking se enfoca sólo en los datos y no en los pagos. La Australian Competition and Consumer Commission (ACCC) desempeña una función de supervisión similar a la asumida por la CMA en Reino Unido, a la vez que trabaja con entidades como la Australian Payments Network. Andy White, CEO de Australian Payments

Network, nos comentó que "la posición regulatoria se basa en un equilibrio entre estabilidad e innovación, pero existe el deseo de lograr una buena competencia con el surgimiento de bancos retadores (challenger banks)". Se espera que la legislación de la Banca Abierta se implemente a finales de 2019.

Fuente: Open Banking, "Preparing for lift of", disponible en <https://www.openbanking.org.uk/wp-content/uploads/open-banking-report-150719.pdf>.

Según la consultora EY, la regulación no es un requisito previo para el éxito de la Banca Abierta, ya que su aceleración y adopción a nivel mundial estará determinada por cuatro pilares fundamentales en los que, si bien el entorno regulatorio forma parte, no es un determinante. Los cuatro pilares contemplados en el EY Open Banking Opportunity Index 2018[31] son:

- Entorno regulatorio.
- Potencial de adopción.
- Sentimiento del consumidor.
- Entorno de innovación.

Para cada uno de los pilares, EY evalúo una amplia gama de indicadores a fin de desarrollar una visión de las condiciones de cada mercado, y encontró que, a diferencia de la adopción, la confianza del consumidor y la innovación, la regulación no es un requisito previo para el éxito de la Banca Abierta. Los resultados del índice demuestran que no existe una sola receta regulatoria para el éxito de la banca abierta.

En la Unión Europea, la Directiva Revisada sobre Servicios de Pago (PSD2) obliga a los bancos a compartir datos con terceros proveedores (TPP, por sus siglas en inglés), una vez que los consumidores den su consentimiento. Los reguladores del Reino Unido y Alemania son los más proactivos y ambos han participado en la determinación de los estándares para las API que conectarán los bancos y los TPP. La Open Banking Implementation Entity (OBIE) del Reino Uni-

CUADRO 2.

Open Banking: oportunidades

[31] "EY Open Banking Opportunity Index: donde la banca abierta está llamada a prosperar", disponible en <https://www.ey.com/es_mx/banking-capital-markets/ey-open-banking-opportunity-index-where-open-banking-is-set-to-thrive>, consultado el 9 de enero de 2020.

do también está supervisando de cerca el desarrollo del ecosistema de Banca Abierta del mercado.

Otros países favorecen un enfoque impulsado por el mercado. China continental es la que mejor lo demuestra. En este caso, los bancos y las fintechs ya están haciendo un uso significativo de las API abiertas, a pesar de que no existe ningún mandato legal para impulsar esto, ni existen normas en vigor.

En el campo de la inclusión financiera, se espera que el desarrollo de las API abiertas puedan contribuir a generar nuevos espacios, al margen de la discusión jurídica y legal que pueda presentarse sobre la titularidad de los datos y manejo de la información.[32]

Algunos ejemplos de Open API son:[33]

- **Barclays África.** Una aplicación que incentiva el uso de los servicios financieros a hogares de bajo ingreso.
- **Wave Money.** En la república de Minamar se ofrece una aplicación que permite mayores posibilidades de pago a los hogares a través de los celulares inteligentes.
- **BTPN.** En Indonesia involucra clientes, bancos, entidades crediticias no bancarias y otros proveedores de información que ofrecen servicios de diferente índole, creando un ecosistema.
- **MTM.** En Uganda, ofrece a los clientes diferentes opciones de billeteras móviles a través de API. Cada una está direccionada de acuerdo con las necesidades del cliente por edad, por nivel de ingreso y por región geográfica.
- **Karandaaz.** En Pakistan, la aplicación integra bancos, pagos gubernamentales, compañías de telecomunicaciones y fintechs en un solo ecosistema de trabajo que busca que el público utilice más los canales digitales.

API

Los datos en primer plano

La Ley Fintech contempló obligaciones cuyo cumplimiento debe estar sujeto al uso de estándares de datos, Interfaces de Programación de Aplicaciones o API abiertas (Application Programming Interface) y mejores prácticas en materia de seguridad de la información. En ese sentido, todos los actores del ecosistema eintech tienen que adaptarse haciendo necesaria la implementación de estándares, como el Estándar de Datos Bancarios Abiertos desarrollado por el Open Banking Working Group, un grupo de trabajo conformado por expertos de la banca, datos abiertos y comunidades integradas por empresas y clientes. El estándar es una guía que describe el proceso de crear, compartir y usar datos bancarios y financieros.

El concepto de API abierta no significa que todos los datos se distribuirán de manera pública, sino que los estándares tecnológicos y el estándar per sean abiertos. El acceso a datos privados usando API abiertas sólo se concibe con el consentimiento del dueño de los datos (ya sea un individuo o un negocio) y estando sujeto a normas técnicas y de seguridad.

En la actualidad, los datos bancarios (como los detalles de las transacciones de una cuenta bancaria personal o de un negocio) no son fáciles de compartir, a pesar de que las

[32] IV Informe de Inclusión Financiera 2018, Felaban, disponible en <http://felaban.s3-website-us-west-2.amazonaws.com/publicaciones/archivo20181211205300.pdf>, consultado el 14 de enero de 2020.

[33] *Idem*.

personas pueden acceder o bajar sus estados bancarios desde sitios web y aplicaciones proporcionadas por sus instituciones bancarias.

De manera similar, la información de productos bancarios es frecuentemente publicada en los sitios web en formatos que usualmente sólo son aptos para su revisión por humanos. En ese sentido, obtener acceso a datos bien estructurados para cualquiera que desee usar la información para crear servicios (como los negocios de tecnología financiera) es complicado. Por mencionar un ejemplo, actualmente existen sitios de comparación de precios que recurren a la técnica conocida como web scrapping para obtener datos de los sitios web; dicha técnica consiste en obtener el contenido de un sitio web (usualmente en formato HTML) para convertirlo en datos estructurados que pueden ser almacenados en una hoja de cálculo o en una base de datos para posteriormente ser empleados para fines como la búsqueda de mejores ofertas.

Conforme a lo anterior, la compartición de datos históricos bancarios constituye un mecanismo fundamental para mejorar la experiencia bancaria de las personas y que permitiría hacer eficientes los procesos en general; el uso de API abiertas para la compartición de datos, ya sea de manera segura o pública, permitirá el desarrollo de aplicaciones y recursos para ayudar a las personas a encontrar los productos más adecuados a sus necesidades.

Por ejemplo, la disponibilidad de datos detallados de productos bancarios podría facilitar la búsqueda de un crédito hipotecario; los bancos podrían buscar clientes con los perfiles más idóneos para un cierto producto y los negocios podrían compartir datos con sus contadores de una manera más rápida y precisa.

En suma: las API permiten a terceros tener acceso a datos que hoy tienen, en exclusiva, los bancos, con el fin de desarrollar diferentes productos y servicios con base en éstos. No se trata sólo de poder acceder a los datos de los clientes, sino de tener la capacidad de hacer cualquier transacción, operación o contratación de productos del banco.

Fuente: Estándar Bancario Abierto: Un estándar para migrar la banca a la economía digital del siglo XXI. https://datos.gob.mx/blog/estandar-bancario-abierto-un-estandar-para-migrar-la-banca-a-la-economia-digital-del-siglo-xxi

La banca abierta sólo tendrá éxito si se gana la confianza de los clientes y los hace sentir cómodos a la hora de compartir sus datos con terceros. Pero la investigación de EY (2019) muestra que la mayoría de los mercados aún necesitan ganarse la confianza de los consumidores, la cual sigue siendo baja o moderada en nueve de los 10 mercados estudiados, independientemente del entorno normativo.

Sólo los clientes de China continental obtienen una puntuación muy alta en su disposición a compartir información con terceros: aproximadamente la mitad (49 por ciento) dice que se siente cómodo compartiendo datos de transacciones con empresas fintech para obtener mejores servicios.

La realización del verdadero potencial de la banca abierta —tanto para los consumidores como para las instituciones financieras— depende de la obtención de la confianza de los consumidores. Los reguladores pueden desempeñar su papel creando entornos que apoyen la innovación y tranquilicen a los consumidores, pero, como demuestra la experiencia china, es en última instancia la capacidad de atraer a los clientes lo que determinará el éxito de la Banca Abierta.

La educación del consumidor sobre los riesgos y beneficios puede ayudar a acelerar la adopción, pero quizá la mayor palanca para cambiar el sentimiento del consumi-

dor sea mostrar a los clientes los beneficios que la Banca Abierta puede aportar. Como se ha visto con la adopción de plataformas populares de medios sociales, las personas compartirán voluntariamente información si perciben beneficios y si pueden hacerlo a través de aplicaciones fáciles de usar y divertidas.

La competencia en el mercado está llevando a los bancos a interesarse en la implementación de este modelo de servicio. Los retos no son sencillos; para convertirse en modelos comerciales habilitados para API abiertas, muchos bancos se enfrentan a varios desafíos derivados de la adaptación de sus sistemas y arquitectura heredados.

DESAFÍOS Y OPORTUNIDADES DEL *OPEN BANKING*

Desafíos	*Oportunidades*
Lograr una adecuada administración de los riesgos que pueden llegar a existir al compartir de forma abierta información sensible de los clientes.	Aumento en la competencia, lo que beneficiará al mercado, dado que todos los actores deberán crear productos completamente personalizados que respondan a necesidades del cliente.
Implementar esquemas y protocolos de seguridad y movilidad adecuada de la información.	Minimización de costos de innovación, pues la banca tendrá un relacionamiento más eficiente con desarrolladores y emprendedores, lo que permitirá la creación rápida de nuevos productos y servicios.
Crear estructuras adecuadas de relacionamiento con terceros (TPP).	Aumento de procesos de co-creación, ya que múltiples participantes trabajarán en la construcción de soluciones, lo cual permitirá que cada uno de los participantes provea distintos factores que crearán valor al producto o servicio.
Diseñar un modelo eficiente de gobernanza de API abiertas que beneficie a todos los actores involucrados.	Mayor empoderamiento de los clientes y transparencia en la administración de sus datos.
Cambio estructural y organizacional, que habilite la innovación abierta, de tal forma que pueda darse respuesta rápida y adecuada a los clientes, pues una gran ola de competidores irá apareciendo.	Aceleración del cambio tecnológico en el sector financiero.
Rediseñar procesos y distribución de productos, ya que los que están hoy no responderán a las necesidades del *Open Banking*.	Se habilitarán nuevas formas de distribución y se mejorarán las capacidades de servicio.
Responder a la demanda con un consumidor que está en control.	Reducción de costos implícitos en el momento de realizar un pago y aumento en la seguridad de los pagos electrónicos.

Fuente: Documento Semana Económica 1144 Asobancaria Colombia, disponible en <http://felaban.s3-website-us-west-2.amazonaws.com/publicaciones/archivo20181211205300.pdf>.

Transición: de la Banca Abierta al Open X

Durante su participación en el evento Revolution Banking,[34] Hugo Nájera Alva, director general de Desarrollo de Negocio de BBVA en México, destacó que "el *Open Banking* es una tendencia que fomenta e impulsa a las instituciones financieras a abrir su infraestructura para conectar a terceros que podrán desarrollar ecosistemas digitales a favor de sus clientes y/o usuarios".

Nájera explicó que es importante entenderla como un proceso donde se están diseñando experiencias para que la banca esté en los nuevos canales donde la gente está interactuando. "En la medida en que nosotros pongamos a disposición la funcionalidad de la banca a otros jugadores, los servicios en el móvil serán el eje de esta relación con el cliente".

El directivo señaló que no cabe duda de que ha llegado el momento de hacer *Open Banking* porque es un modelo de operación que crece a gran velocidad porque significa poner a disposición de otras empresas las capacidades del banco para que se construyan servicios sobre ellas. Además, las plataformas abiertas y colaborativas fomentan la creación de mejores productos y servicios para los usuarios.

Para Nájera, la Banca Abierta propicia un cambio en el paradigma bancario y es fundamental adaptarse a las nuevas metodologías de trabajo, como la *agile*, que permite diseñar proyectos en el menor tiempo posible basados en propósitos, valores y prioridades. Así, cuando llegan al usuario final, puede optarse entre "hacer un negocio o no hacerlo, adquirir un bien o no, ahorrar o tomar otro mecanismo y que lo pueda hacer de la forma correcta porque tiene al alcance todas las oportunidades para decidir".

Qué pasa con la Banca Abierta

No obstante los buenos augurios sobre la Banca Abierta, el Reporte Mundial de FinTech 2019 (WFTR 2019)[35] indica que, aunque el *Open Banking* todavía debe alcanzar la madurez, la industria de servicios financieros está entrando a una nueva fase de innovación llamada Open X, la cual requiere una mayor colaboración y especialización. El reporte sugiere que los bancos y otros actores del ecosistema de servicios financieros comiencen a planificar tomando en cuenta esto y evolucionen de acuerdo con sus modelos de negocio.

WFTR 2019 identifica un doble desafío: las empresas de fintech están luchando para escalar sus operaciones y los bancos se están estancando en la colaboración con las fintechs. Como resultado, los actores de la industria están buscando brincar directo desde la Banca Abierta hasta la Open X, que es una forma de colaboración más efectiva y estructurada, facilitada por la estandarización de la Interfaz de Programación de Aplicaciones y las perspectivas compartidas de los datos del cliente.

De acuerdo con el reporte, la era de la Open X creará un mercado integrado, con roles especializados para cada jugador a fin de permitir un intercambio perfecto de datos y servicios, mejorando la experiencia del

[34] "La banca abierta es el futuro del sistema financiero en México", 2019, disponible en <https://www.bbva.com/es/mx/la-banca-abierta-es-el-futuro-del-sistema-financiero-en-mexico/>, consultado el 19 de enero de 2020.

[35] Capgemini y Efma, 2019, "Banca Abierta, el Reporte Mundial de FinTech 2019 (WFTR 2019)", disponible en <https://www.capgemini.com/mx-es/wp-content/uploads/sites/24/2019/06/Reporte-Mundial-de-FinTech-2019-la-industria-est por cientoC3 por cientoA1-cambiando-de-Open-Banking-a-Open-X.pdf>, consultado el27 de diciembre de 2019.

cliente y acelerando la innovación de productos. Además, la llegada de Open X es impulsada por cuatro cambios fundamentales:

1. Pasar de un enfoque en el producto a un énfasis en la experiencia del cliente.
2. La evolución de los datos como activo crítico.
3. Un cambio: de priorizar la propiedad a facilitar el acceso compartido.
4. Énfasis en asociarse para innovar, en lugar de comprar o crear nuevas soluciones.

Open X llevará a la industria de servicios financieros a un ecosistema o mercado compartido, en el que la industria reintroduce el reagrupamiento de productos y servicios, y tanto los bancos como las fintechs deben reevaluar su estrategia para la innovación y el servicio a los clientes.

Las API serán facilitadores críticos para habilitar Open X, ya que permiten a terceros acceder a sistemas y datos bancarios en un entorno controlado. Mientras que los datos de los clientes ya son ampliamente compartidos y aprovechados en la industria, las API estandarizadas no son comunes. Aunque los requisitos y las regulaciones son complejas, la estandarización ayudará a reducir el fraude, mejorar la interoperabilidad, aumentar la velocidad al mercado y mejorar la escalabilidad.[36]

El Reporte Mundial de InsurTech 2019[37] también detectó que los actores de la industria están considerando dos modelos de monetización potenciales para las API: participación en los ingresos (que 60 por ciento de los bancos y 70 por ciento de las fintechs piensan que es factible) y acceso a las comisiones de las API (apoyadas por 46 por ciento de los bancos y 55 por ciento de las fintechs). Sin embargo, sólo alrededor de un tercio de los ejecutivos de banca dijeron que actualmente están bien equipados para monetizar las API.

Mientras que los bancos y las fintechs dicen que entienden la importancia de la colaboración, la aprehensión sobre la privacidad y seguridad sigue siendo el tema principal. Cuando se preguntó qué les preocupa sobre el *Open Banking*, la gran mayoría de los bancos identificó la seguridad de datos (76 por ciento), la privacidad del cliente (76 por ciento) y la pérdida de control de datos de clientes (63 por ciento). Las fintechs fueron más optimistas sobre la Banca Abierta, pero 50 por ciento expresó temores sobre la seguridad y la privacidad, y 38 por ciento, sobre la pérdida de control de los datos del cliente.

Cuando se les preguntó sobre los obstáculos para una colaboración efectiva, 66 por ciento de los bancos y 70 por ciento de las fintechs señalaron la diferencia en la cultura/mentalidad organizacional del otro; 52 por ciento de los bancos y 70 por ciento de las fintechs señalaron barreras en el proceso; la falta de visión y objetivos a largo plazo se mencionó por 54 por ciento de los bancos y 60 por ciento de las fintechs. Sólo 26 por ciento de los ejecutivos bancarios y 43 por ciento de los líderes de fintechs dijeron que habían identificado al socio de colaboración correcto de Banca Abierta. Estas respuestas sugieren que muchos de los bancos y fintechs no están preparados para la Banca Abierta, y mucho menos para la creciente demanda de intercambio de datos e integración que la Open X traerá.

[36] *Idem*.

[37] World InsurTech Report 2019, disponible en <https://www.capgemini.com/es-es/news/world-insurtech-report-2019/>, consultado el 27 de diciembre de 2019.

Los participantes de Open X deben elegir roles estratégicos basados en sus especialidades. Dentro del mercado Open X, los bancos primero deberán mejorar su modelo integrado (tradicional) y luego enfocarse en fortalecer sus áreas de especialización. El Reporte Mundial FinTech 2019 identifica tres roles estratégicos, los cuales se espera que evolucionen como parte de Open X:

1. Los proveedores desarrollarán productos y servicios.
2. Los agregadores acumularán productos y servicios del mercado y los distribuirán a través de canales internos, manteniendo relación con los clientes.
3. Los orquestadores actuarán como conectores y coordinadores del mercado, facilitando la interacción con los socios.

De acuerdo con el reporte, dentro del mercado Open X, es posible que muchos actores no estén bien posicionados para competir como orquestadores y que sus fortalezas los lleven a otros roles. Sin embargo, no importa qué papel asuman en la Open X, ellos deben reclutar el talento adecuado, aprovechar los datos y la tecnología, y colaborar con las fintechs para asegurar mejores capacidades internas para la entrega competitiva de servicios relevantes en el escenario actual de Banca Abierta.

La información obtenida en los reportes indica que la industria está al borde de una evolución más integral, donde existe la oportunidad de saltar a un mercado integrado, Open X, en el que habrá un intercambio perfecto de datos y los socios del ecosistema podrán colaborar de una manera más completa, por lo que los bancos y las fintechs necesitan prepararse para un cambio más radical.[38]

En la era de la colaboración o del Open X, los jugadores del ecosistema tendrán que trabajar de forma más eficiente para prosperar y servir mejor a sus clientes para lograr un beneficio colectivo, por lo que deben eliminarse las barreras.[39]

El cambio de paradigma en la manera en la que se proveen los servicios financieros, marcado por un fuerte aumento del componente tecnológico, ha atraído la atención de las autoridades reguladoras y supervisoras en todo el mundo.

Los esfuerzos de estos organismos para dar respuesta a los retos regulatorios que plantean las fintechs y sus nuevos modelos de negocio se han traducido en una serie de iniciativas que, en distintos niveles, pretenden articular mecanismos para regular eficientemente una realidad financiera cambiante.

Regulación: ¿motivación o desencanto?

Desde el punto de vista de Fintech Radar México, la promulgación de la Ley Fintech, el 9 de marzo de 2018, y la posterior publicación de las primeras disposiciones secundarias, el 10 de septiembre del mismo año, han contribuido a un crecimiento neto de 18 por ciento en el número de *startups* existentes, desde su última medición, publicada a finales de julio de 2018, por lo que, si bien la espera de las disposiciones generó incertidumbre sobre las medidas que deberán acatarse, en particular por las empresas de fondos de pago electrónico y de financiamiento colectivo, el ecosistema fintech mexicano

[38] Anirban Bose, CEO de Capgemini's Financial Services y miembro de la Junta Ejecutiva del Grupo.
[39] Vincent Bastid, secretario general de Efma.

observó un crecimiento que lo ubica en el primer puesto en Latinoamérica.

De acuerdo con el informe "Fintech en América Latina 2018: crecimiento y consolidación",[40] la regulación tiene importancia en el desarrollo del ecosistema. Según los resultados de la encuesta realizada, 9 por ciento considera que no se necesita una regulación específica, mientras que 35 por ciento cree que sí es necesaria y 35 por ciento que la regulación actual es adecuada. Según el informe, estos datos reflejan el progreso alcanzado en ciertas jurisdicciones en materia de regulación y resaltan avances logrados gracias al diálogo entre reguladores y la industria para propiciar la búsqueda de un marco favorable para la innovación.

En México, de acuerdo con la Comisión Federal de Competencia Económica (Cofece),[41] la motivación de la regulación de las fintechs tiene como objetivos: contribuir a la inclusión financiera, aumentar la calidad y creación de nuevos productos y servicios, tener flexibilidad que permita la innovación, contribuir a la reducción de costos de los productos y servicios, otorgar certeza jurídica a los inversionistas (favorecer la inversión en el sector), proteger al consumidor ante el fraude, asegurar estabilidad del sistema financiero y prevenir el lavado de dinero.

BBVA Research[42] indicó que 2019 sería el año en el que las autoridades deberían pasar a la acción e implementar una respuesta global para los retos de esta nueva era. Se detalló que la importancia de la regulación fintech no entiende de fronteras. "En Europa, Estados Unidos, América Latina, en todo el mundo se pretende aprovechar las oportunidades que ofrece la digitalización para avanzar en materia de inclusión financiera".

BBVA Research (1T19) apuntó que México es pionero en temas de regulación y algunos bancos e instituciones financieras no bancarias están empezando a explotar las oportunidades que representa este nicho de mercado; "el marco regulatorio le ha dado certeza a los grupos financieros y están dispuestos a invertir en este segmento, algunos bancos ya han decidido que prefieren tener al mundo fintech como un aliado y no como un competidor", se menciona en el informe, en el que se plantean denominadores comunes, como los relacionados con la tecnología, aunque existan contextos y situaciones completamente distintas en los países y regiones.

Los hallazgos del reporte "Termómetro Fintech: Los retos de la regulación"[43] se centran en el país y, desde varias características, como capital, empleo, índice de maduración e impacto de la regulación, plantea una radiografía que nos muestra la posición de las fintechs en México:

- El volumen anual de operación equivale a 68,409 millones de pesos, con 4.7 millones de usuarios registrados.[44]

[40] Banco Interamericano de Desarrollo (BID) y Finnovista, noviembre de 2018.

[41] Resoluciones. DOF, 2017, disponible en <https://www.cofece.mx/cfcresoluciones/docs/Opiniones/V20/6/3953499.pdf>, consultado el 22 de diciembre de 2019.

[42] Informe Situación Regulación Financiera 1T19. BBVA Research, disponible en <https://www.bbvaresearch.com/wp-content/uploads/2019/01/Situacion_Regulacion_1T19.pdf>, consultado el 18 de diciembre de 2019.

[43] Endeavor, Embajada Británica, Santander, Finnovista y Google. "Termómetro Fintech: Los retos de la regulación", disponible en <http://contenido.endeavor.org.mx/descarga-reporte-fintech-2019>.

[44] Se llegó a estos datos, que podrían equipararse a la cartera y activos manejados por un banco, por medio de una muestra de 148 fintechs.

- El ecosistema fintech en México es liderado por un pequeño grupo de emprendedores que han alcanzado una mayor escala. De las *startups*, 70 por ciento han levantado capital y deuda en los últimos cinco años, equivalentes a 629 millones de dólares. Sin embargo, de las 394 *startups* identificadas, sólo ocho concentran 80 por ciento de esos recursos.
- Este ecosistema es responsable de 3,600 empleos directos. Como reflejo de la etapa en la cual se encuentra la mayoría de las empresas, la productividad del sector está muy concentrada en siete empresas que han superado los 100 empleos y que generan 36 por ciento de los empleos del sector, mientras que 56 por ciento se encuentra en empresas entre uno y 10 empleados, seguido de 22 por ciento que está entre 11 y 25 empleos directos.
- Como resultado del Índice de Maduración del Ecosistema Fintech en México (INFIN), desarrollado por Endeavor, se encontró que las *startups* fintech mexicanas (considerando variables como ventas, empleos, inversión, volumen de operaciones, usuarios activos, mercado y tecnologías utilizadas) se encuentran en una etapa de crecimiento.
- El sector fintech en México está representado, en mayor medida, por emprendedores en una etapa temprana y de crecimiento, ya que la empresa típica del sector tiene tres años de fundación, 105 mil dólares de ingresos anuales, nueve empleados y ha levantado 230 mil dólares en capital.
- De las fintechs consultadas, 57 por ciento manifestó estar sujeto al cumplimiento de las nuevas disposiciones y el costo que esperan es de 35 mil dólares anuales; sin embargo, 21 por ciento de los emprendedores y la mayoría de los entrevistados calculan que el costo regulatorio esté alrededor de los 100 mil dólares (incluidos abogados, consultoría y oficial de cumplimiento certificado, entre otros).
- Los emprendedores manifiestan, sobre la Ley Fintech, principalmente, que: habrá fuertes barreras de entrada para las *startups* o nuevos jugadores (28 por ciento); los altos costos asociados al cumplimiento de la ley generarán ineficiencias (22 por ciento); habrá que cumplir un marco regulatorio riguroso (21 por ciento) y 13 por ciento manifiesta estar 100 por ciento conforme la ley y sus reglamentos, y estar listo para cumplir las disposiciones.
- La CNBV tiene mapeadas más de 515 fintechs que operan en México. De éstas, estimó que alrededor de 200 cumplirían con las nuevas disposiciones al encontrarse en las categorías de fondo de pago electrónicos (*wallets*), activos virtuales (cryptocurrencies) y financiamiento colectivo (*crowdfunding*).

Tras concluir el plazo, septiembre de 2019, la Comisión Nacional Bancaria y de Valores[45] recibió 85 solicitudes de autorización para operar como Instituciones de Tecnología Financiera, un total de 85 empresas, de las cuales 60 solicitan autorización para operar como Instituciones de Fondos de Pago Electrónico y 25 como instituciones de financiamiento colectivo.

Las personas que realizaban actividades de financiamiento colectivo o de fondos de pago electrónico con anterioridad a la

[45] "CNBV recibió 85 solicitudes de autorización para operar como Institución de Tecnología Financiera", CNBV, disponible en <https://www.gob.mx/cnbv/articulos/cnbv-recibio-85-solicitudes-de-autorizacion-para-operar-como-institucion-de-tecnologia-financiera>, consultado el 5 de enero de 2020.

entrada en vigor de la Ley Fintech y que presentaron su solicitud de autorización ante la CNBV en el periodo establecido, podrán continuar realizando dichas actividades hasta en tanto se resuelva su solicitud.

Las personas que realizaban actividades señaladas en la Ley Fintech que no presentaron su solicitud de autorización antes del 26 de septiembre de 2019, deberán abstenerse de continuar realizando dichas actividades o celebrando nuevas operaciones, y deberán realizar únicamente los actos tendientes a la conclusión o cesión de las operaciones existentes; de lo contrario, serán sujetas a las sanciones penales y administrativas que marca la ley.

Lo que comenzó como una respuesta a la crisis financiera de 2008, así como a las limitaciones que ofrece la banca tradicional, ha hecho que las fintechs se presenten como una opción más accesible y rápida que está promoviendo un cambio sin retorno con beneficios en el corto plazo.

Las fintechs han encontrado en México un terreno fértil, toda vez que las opciones a productos financieros benefician a empresas que antes no tenían acceso y posiciona a nuestro país como líder en América Latina; sin embargo, su universo está en constante movimiento.

Aunque al inicio de 2020 México era el país de América Latina con un mayor desarrollo fintech, para algunos la regulación aprobada en 2018 podría frenar el crecimiento, como plantea la investigación presentada en el Termómetro (2019), mientras que para otros podría consolidar el ecosistema por la depuración que podría hacerse para crecer con bases firmes.

SEGUNDA PARTE

Factores entrelazados. El cambio implica consecuencias

Las entidades clásicas están afrontando el modelo de la transformación digital. No obstante, la auténtica disrupción del sistema financiero está llegando de la mano de los nuevos participantes: las fintechs que están aportando tecnología, flexibilidad y, en muchos casos, liderazgo en un sistema que hasta hace poco no se movía a la velocidad que lo hace ahora.

La tecnología, que es a la vez carretera y vehículo por el cual las fintechs están llevando a las entidades clásicas o tradicionales a dar el salto cuantitativo y cualitativo —mancuerna insoslayable—, no respeta tiempos ni descansos y va en una ruta que no tiene retorno, no sólo para los que quieren liderar, sino para los que quieren permanecer.

4. Riesgos en escenarios cambiantes

La desregulación y liberalización financiera impulsaron una vasta financiarización de las economías —es decir, un desplazamiento de capital productivo hacia los mercados financieros—, grandes y profundas transformaciones en los sistemas bancario y financiero a través de la innovación de instrumentos y servicios financieros, así como la intervención de nuevos participantes.

El traslado de capitales ocasionó que, en la economía global, las tasas de crecimiento del Producto Interno Bruto (PIB) tuvieran un comportamiento errático y, en el ámbito empresarial, se modificara la estructura de las empresas: se crearon nuevas áreas y funciones, así como productos y servicios en un mercado marcado por la innovación.

La desregulación bancaria generó cambios en la libertad de los bancos para operar y agudizó la competencia entre intermediarios financieros bancarios y no bancarios. Los oligopolios bancarios se fortalecieron y los intermediarios financieros no bancarios —*non bank banks*— se consolidaron. Estos cambios alteraron la dinámica y naturaleza del capitalismo debido a la expansión del crédito, en muchos casos irresponsable, y al incremento del valor real de los bienes y de los activos financieros (letras, bonos, acciones, opciones, derivados, etcétera).

Las primeras crisis financieras globales durante la década de los noventa (México, 1994-1995; Asia, 1997; Rusia, 1998, y Brasil, 1999) mostraron que la evolución de los mercados financieros bajo un proceso de desregulación iniciado en los años setenta adoptó una forma de ciclos financieros alimentados por la innovación, que propició los *boom* financieros que concluían en crisis, por lo que, ante un aumento de los riesgos, se requirió una revisión de las instituciones y prácticas básicas del sistema financiero internacional.

Crisis: México 1994-1995

Previo a la crisis de 1994-1995, México recibió grandes flujos de capital extranjero. Esto obedeció, en parte, a las perspectivas favorables que presentaba la economía mexicana después de varios años de estabilización macroeconómica y de la implementación de importantes reformas estructurales. De 1991 a 1993, las entradas de capital a México al-

canzaron un promedio anual de casi 8 por ciento del PIB.

Ese escenario favorable tuvo un fuerte impacto sobre la economía mexicana: de 1988 a 1994, la relación entre M4, el agregado monetario más amplio, y el PIB, se incrementó en 20 puntos porcentuales. Las entradas de capital coincidieron con un fortalecimiento de las finanzas públicas y una fuerte demanda de crédito. De esta manera, se produjo un muy rápido crecimiento del crédito bancario al sector privado. De 1988 a 1994, el crédito bancario al sector privado, medido como proporción del PIB, se cuadruplicó.

Al mismo tiempo, la expansión de la demanda impulsada por una amplia disponibilidad de financiamiento condujo a un fuerte aumento del déficit en cuenta corriente de la balanza de pagos. En consecuencia, para 1994 ese déficit representaba ya 7 por ciento con respecto al PIB. En resumen, la abundante disponibilidad de financiamiento resultó en un elevado nivel de apalancamiento tanto de empresas como de hogares e instituciones financieras.

En aquella época, se decía que el déficit externo no podría ser fuente de problemas graves cuando estaba generado por el sector privado y las finanzas públicas mostraban una situación de fortaleza. Sin embargo, esta perspectiva no ponía suficiente atención en que el déficit con el exterior era financiado, principalmente, con capitales de corto plazo bajo un régimen de tipo de cambio semifijo o predeterminado.

El rápido crecimiento del crédito al sector privado, en ausencia de mecanismos adecuados de supervisión y regulación bancaria, dio lugar a otro frente de vulnerabilidad. Como resultado de la nacionalización bancaria de 1982, los bancos habían perdido a su personal con mayor experiencia y capacitación.

Tampoco contaban con experiencia en el otorgamiento de crédito al sector privado, ya que durante la década de los ochenta la mayor parte del financiamiento bancario se había canalizado al gobierno federal. De esta manera, la amplia disponibilidad de recursos, una competencia intensa entre los bancos recién privatizados por ampliar su participación de mercado y la falta de experiencia y de controles prudenciales, así como de riesgos suficientes impidieron que el crédito se otorgara de manera más adecuada.

En los bancos, el esquema de incentivos operó también para premiar la toma de riesgos excesivos. Los nuevos banqueros deseaban recuperar en un periodo corto su inversión sin tomar en cuenta el elevado riesgo que estaban asumiendo.

Los problemas se acentuaron por la insuficiente transparencia de las estadísticas oficiales y las prácticas contables de los bancos comerciales, lo cual dificultó una evaluación objetiva de la situación. En ese entorno de vulnerabilidad, el comienzo de un ciclo alcista de las tasas de interés internacionales a partir de febrero de 1994, junto con una situación de incertidumbre política creciente, detonaron la crisis. Los inversionistas cambiaron abruptamente su percepción acerca de las perspectivas de la economía mexicana, lo que dio lugar a salidas masivas de capital. Así, la reversión repentina de los flujos de capital y una depreciación pronunciada del peso frente al dólar ocasionaron una crisis profunda en el sector financiero mexicano.

En esa coyuntura, el reto principal para las autoridades fue evitar el colapso del sistema financiero y productivo, y restablecer la confianza de los inversionistas en el país. Debido a la naturaleza de la crisis, la respuesta de política se concentró en dos frentes. En primer lugar, se instrumentaron políticas fiscales y monetarias restrictivas y se adoptó un tipo de cambio flexible; en segundo lugar, se

negoció un cuantioso paquete internacional de apoyo que permitió fortalecer la confianza en la capacidad del país para cumplir con sus obligaciones financieras.

El deterioro del empleo y el alza de las tasas de interés provocaron un fuerte aumento de la cartera vencida en las Instituciones de Crédito y, por ende, un descenso marcado en los niveles de capitalización de la banca. En respuesta, se ejecutaron diversas medidas para apoyar tanto a los deudores como a los bancos. La finalidad fue prevenir una quiebra generalizada de las instituciones financieras.

Se adoptó para tal fin un enfoque integral, ya que se enfrentaban problemas de liquidez y solvencia con repercusiones sistémicas. Entre las medidas que se tomaron destacan las siguientes:

- El suministro de liquidez en moneda extranjera a los bancos comerciales para impedir presiones adicionales sobre el tipo de cambio.
- Un acuerdo de apoyo para deudores de la banca.
- La compra de cartera en problemas con el fin de fortalecer el capital bancario.
- La activación de un programa de capitalización temporal para los bancos.
- Reformas legales para facilitar una recapitalización efectiva de la banca. Con ese fin, se reforzaron las reglas de capitalización y se permitió una mayor participación de los inversionistas extranjeros en la banca mexicana.
- La intervención de varias Instituciones de Crédito.

Las autoridades estaban conscientes de los riesgos que implicaba la estrategia instrumentada. Sin embargo, también había conciencia de que el escenario alternativo de un posible colapso del sistema financiero, así como una profunda y prolongada recesión, conllevaban costos mucho más elevados.

Fuente: Extracto de "La crisis de 1994-95 y la actual crisis". Guillermo Ortiz, 2009. El texto fue publicado originalmente por la revista Este País. Tendencias y opiniones en su edición de febrero de 2009, como parte de la serie "La crisis: testimonios y perspectivas".

La innovación financiera aportó un catálogo de productos, pero no la capacidad de medir mejor los riesgos financieros y, en particular, los riesgos sistémicos. Como cambios relevantes en el ámbito financiero se pueden mencionar:

Innovación financiera

Producto	*Factor*	*Características*
Flotación de los tipos de cambio	Con la desaparición en 1973 del Sistema Monetario Internacional, aparece el riesgo de cambio y la posibilidad de realizar beneficios especulativos negociando los precios de las divisas.	Se desarrolla el mercado de contratos *forwards* sobre divisas y, en 1981, el Banco Mundial e IBM realizaron uno de los primeros *swaps* de divisas, mediante la permuta de dólares contra marcos alemanes y francos suizos.

Producto	*Factor*	*Características*
Cambio del régimen de financiación a los gobiernos	Los grandes déficits fiscales de los años setenta y ochenta favorecieron la búsqueda de mecanismos de financiamiento para captar el ahorro privado.	Se pasa del financiamiento bancario y la creación de base monetaria por los bancos centrales a la emisión de títulos (bonos) que, una vez emitidos, son negociados en los mercados secundarios de deuda pública. Los fondos del mercado monetario inversión, dotados de liquidez, fueron uno de los vehículos potenciados, además de los fondos de pensiones.
Reformas de los mercados de acciones	Se abrió paso la negociación electrónica, lo que facilitó la entrada de más inversonistas. La revolución de las comunicaciones permitió la interconexión internacional de los mercados bursátiles.	Se favoreció el aumento de las empresas cotizadas en Bolsa y el financiamiento de las empresas mediante emisión de acciones. El crecimiento de los fondos de inversión de renta variable o mixtos planteaba la obligación de valor a las posiciones a precios de mercado. La inclusión de los derivados en los fondos y la aparición de fondos garantizados que incorporan en muchos casos opciones exóticas es otra fuente de la necesidad de utilizar modelos de valoración, porque, en muchos casos, las opciones carecían de liquidez.
Creación de mercados organizados de instrumentos derivados	La existencia de modelos de valoración de los derivados y, especialmente de las opciones, junto con la necesidad de gestionar los riesgos de los instrumentos básicos o subyacentes, acciones, divisas y bonos, favorecieron la creación de mercados organizados de instrumentos derivados en las principales plazas financieras del mundo.	Los mercados organizados consiguen minimizar el riesgo de crédito mediante la exigencia de garantías, lo que favorece la negociación de los contratos estandarizados. La proliferación de mercados organizados potenció las operaciones especulativas, pero con ellos creció la preocupación por la gestión de los riesgos ante los desastres financieros, como los de Barings, condado de Orange, Daiwa, Long Term Capital Management y Enron, vinculados de una u otra forma a los instrumentos derivados.
Proliferación de nuevos instrumentos derivados	Creación de instrumentos financieros complejos que combinan instrumentos tradicionales (bonos, acciones, divisas) con instrumentos derivados, lo que permite el diseño de productos estructurados muy flexibles, capaces de modular y encajar el binomio rentabilidad-riesgo en un perfil deseado.	La teoría de valoración desarrollada por Black, Scholes y Merton se aplicó a la valoración de nuevos tipos de opciones, denominadas de forma genérica opciones exóticas. Estas opciones, combinadas con los instrumentos tradicionales, especialmente bonos, permitió el diseño de nuevos instrumentos de financiamiento, tanto para bancos como para las grandes empresas no financieras, que ofrecían a los inversionistas promesas de altos rendimientos con exposición a riesgos adicionales al de contraparte del emisor.

Producto	*Factor*	*Características*
		Estos productos se comercializaron profusamente antes de la crisis de 2008, y se siguen comercializando, en los segmentos mayorista y minorista. La mayoría de estas emisiones carecen de liquidez, y cuando existe la proporciona el emisor, con las implicaciones para el precio que esto supone. Estos instrumentos, que incorporan derivados, deben contabilizarse mediante modelos por la ausencia generalizada de precios negociados en mercados activos.
Crisis de la deuda externa y posterior creación de mercados de bonos soberanos	Tras la crisis que se inició en agosto de 1982 con el *default* de México, se produjo un cambio relevante en la forma de financiamiento de los gobiernos.	Con el Plan Brady surgió un nuevo mercado de bonos, denominados bonos Brady, con la posibilidad de realizar operaciones de compra y venta a corto plazo y la existencia de mercados más o menos líquidos para poder valorar las posiciones.
Aumento en el balance de los bancos de las carteras de instrumentos líquidos negociables en mercados secundarios con el objetivo de realizar beneficios a corto plazo	La desregulación financiera abrió muchas economías a los flujos de capitales a corto plazo, al mismo tiempo que los países receptores creaban o potenciaban sus propias bolsas de valores, especialmente para la negociación de la deuda pública y en mucha menor medida los instrumentos de capital, las acciones.	También la puesta en flotación de la divisa potenció los mercados de cambios, casi siempre acompañado de un mercado de contratos *forward* sobre la divisa, muchas veces liderado por los bancos extranjeros. Los bancos comerciales, incluso de pequeño tamaño, crearon mesas de tesorería para intentar obtener beneficios operando a corto plazo en los nuevos mercados, tanto nacionales como internacionales y en otros países. Por necesidades internas de gestión las posiciones tenían que ser valoradas a precios de mercado, tanto para conocer las ganancias o pérdidas potenciales como para la medición de los riesgos. El término *mark-to-market* es el antecedente del valor razonable en el contexto de la contabilidad analítica del banco.
Gran desarrollo de la titulización de activos	Una forma desarrollada de los primitivos bonos de titulización son los CDO (*collateralised debt obligations*).	La titulización de una cartera de activos consiste en su utilización como respaldo para la emisión de otros activos (bonos) de características más favorables para su negociación en los mercados, es decir, consiste en un proceso mediante el cual una o varias entidades, originador/cedente, venden a otra entidad o vehículo uno o más préstamos o derechos de crédito de características similares,

Producto	*Factor*	*Características*
		que dicho vehículo agrupa, y con su respaldo emite valores, existiendo cierta relación entre los flujos de caja que generan los activos adquiridos y los pagos, en concepto de principal e intereses, generados por los valores emitidos. Los bonos de titulización han ido adquiriendo formas más complejas al introducirse relaciones de subordinación entre los bonos pertenecientes a una misma emisión. Aunque la valoración de estos bonos presenta en muchos casos dificultades insalvables, por la carencia de informaciones esenciales sobre variables presentes en los modelos de valoración, este segmento de mercado ha tenido un crecimiento enorme, como se puso de manifiesto en la crisis de 2008.
Desarrollo de los fondos de inversión clásicos y crecimiento espectacular de los *hedge funds*	Un *hedge fund*, traducido literalmente como fondo de cobertura, es un vehículo de un conjunto de inversiones, gestionados y administrados por una organización privada.	Estos vehículos financieros no están abiertos a todos los inversionistas. Los participantes son, en muchos casos, inversionistas institucionales: bancos de inversión, bancos comerciales, sociedades de valores e inversionistas privados con grandes patrimonios, incluso bancos centrales. Es frecuente que los propios gestores tengan posiciones en los fondos y que reinviertan en ellos las altas remuneraciones que reciben por la gestión. Los *hedge funds* tienen diferencias significativas con otros vehículos financieros, como los fondos de inversión, que suelen estar reglamentados con prohibiciones o limitaciones para tomar posiciones cortas, y limitada la utilización de derivados. Los *hedge funds* carecen de dichas limitaciones y las únicas restricciones son autoimpuestas al especializarse en determinados mercados y activos. Otra diferencia con los fondos de inversión está en el apalancamiento, dado que los participantes en el fondo pueden aumentar su posición con préstamos otorgados por una entidad financiera que utiliza como garantía los activos en los que invierte el fondo. La valoración de los *hedge funds* plantea innumerables problemas porque en muchas ocasiones invierten en instrumentos financieros sin liquidez y, sin embargo, periódicamente, suele ser una vez al mes, deben informar del valor a los inversionistas.

Fuente: elaboración propia con información de "Regulación financiera y riesgos sistémicos bajo la hegemonía del capital financiero" (versión provisional), Ángel Vilariño, mayo de 2018, disponible en <https://www.ucm.es/data/cont/media/www/pag111196/Regulaci%C3%B3n%20financiera,%20riesgos%20sist%C3%A9micos%20y%20hegemon%C3%ADa%20del%20capital%20financiero.pdf>.

Como se ha visto, desde finales de los años sesenta del siglo pasado ocurrieron diversos acontecimientos que han marcado en gran parte le evolución de las finanzas internacionales y, por ende, de la estructura del sistema financiero. A partir de esa década se produjeron cambios relevantes en ámbitos como: el tipo de instrumentos financieros negociados, la importancia y diversidad de los mercados financieros, las prácticas de gestión en las empresas, las retribuciones de los directivos, los sistemas de información y comunicación, las teorías financieras de valoración de los instrumentos financieros, la importancia de la política monetaria y las normas de regulación y supervisión financiera, dentro de un profundo proceso de globalización y de acumulación y concentración de la riqueza financiera.[1]

Todas esas innovaciones trajeron consigo nuevos riesgos y la combinación de los riesgos tradicionales con los nuevos en el marco de tres factores fundamentales: el incremento generalizado en la desregulación de los mercados, acompañado de los movimientos de capitales; la creciente inversión institucional, y el incremento de la volatilidad.Y es justamente lo que les ha dado mayor dinamismo a los mercados financieros lo que le ha agregado un mayor coeficiente de riesgos.

Cambian los riesgos

Los mercados financieros están expuestos a distintas fuentes de riesgos: de crédito, de mercado, de liquidez, operacional y legal. El riesgo de crédito suele ser más acusado como consecuencia de la falta de contrapartes bien calificadas. Los riesgos de mercado y de liquidez son mayores debido a actividad de los mercados. Los operacionales podrían verse agravados por la inadecuación de los recursos humanos o por el mal funcionamiento de los sistemas manuales, mecánicos o electrónicos de procesamiento de pagos. Por último, el riesgo legal también puede estar presente en el entorno, por ejemplo, ante la incapacidad de ejecutar los activos de garantía.

[1] En el informe "The Changing Wealth of Nations 2018" ("La riqueza cambiante de las naciones 2018"), se hace un seguimiento de la riqueza de 141 países entre 1995 y 2014, combinando capital natural (como bosques y minerales), capital humano (ingresos a lo largo de la vida de una persona), capital producido (edificios, infraestructura, etcétera) y activos extranjeros netos. En el informe se llegó a la conclusión de que la riqueza mundial creció aproximadamente 66 por ciento (de 690 billones a 1,143 billones en dólares estadounidenses constantes de 2014 a precios de mercado). Pero la desigualdad fue considerable, dado que en los países de ingreso alto de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), la riqueza per cápita fue 52 veces mayor que la de los países de ingreso bajo. En el informe se concluyó que, durante las últimas dos décadas, más de 20 países de ingreso bajo, donde en 1995 el capital natural era el componente predominante de la riqueza general, pasaron a ser de ingreso mediano, en parte invirtiendo ganancias derivadas del capital natural en sectores como el de infraestructura, así como en los de educación y salud, que incrementan el capital humano.

Tipo de riesgos asociados al sistema bancario

Tipo de Riesgo	*Características*
Riesgo de mercado	Refleja la sensibilidad de los ingresos y de las posiciones del balance a los cambios en los precios de los activos. Con el tiempo, la importancia de este riesgo ha evolucionado. A modo de ejemplo, en los sistemas muy regulados desde tiempo atrás, las tasas de interés no desempeñaban una función de asignación significativa. Sin embargo, con la adopción de regímenes más liberales, las tasas de interés se han vuelto más volátiles, por lo que las entidades de crédito se encuentran cada vez más expuestas al riesgo de tasa de interés y no siempre están bien preparadas para afrontarlo, debido a la falta de instrumentos de cobertura adecuados.
Riesgo de crédito	Se da cuando un emisor de deuda deja de atender sus pagos. Se trata del riesgo más importante que asumen los bancos comerciales. En la evaluación del mismo, las Instituciones de Crédito deben tener en cuenta tres factores: las probabilidades de impago dentro del horizonte temporal de la obligación, su grado de exposición (el tamaño de la obligación si se produce el impago) y la tasa de recuperación (qué parte de la exposición puede recuperarse a través de procedimientos de insolvencia u otra clase de acuerdo). Existen dos cuestiones fundamentales asociadas a este riesgo que guardan relación con las economías de mercado emergentes: en primer lugar, el incremento del porcentaje de crédito al sector hogares observado en una serie de países podría reducir el riesgo de crédito si la concentración de activos bancarios disminuyera, si el crédito al consumo diversifica el riesgo entre un número mayor de prestatarios y si los beneficios de los préstamos al consumo demuestran ser más estables. No obstante, el riesgo de crédito podría aumentar si los bancos conceden préstamos a nuevos segmentos de mercado. En segundo lugar, existe un riesgo de crédito significativo vinculado a los efectos de las fluctuaciones de los precios de los activos en las carteras bancarias. En este sentido, hay dos motivos de preocupación: la volatilidad asociada a los precios de los inmuebles y la volatilidad de la tasa de cambio que puede generar riesgo de crédito en economías con dolarización financiera.
Riesgo de liquidez	Existen dos tipos: el primero es de mercado y se refiere al riesgo de que una entidad de crédito no pueda ejecutar una operación a un precio cercano al precio de mercado vigente, por lo que correría el riesgo de pérdidas en sus posiciones. El segundo es el riesgo de financiamiento, es decir, que una entidad de crédito no pueda captar dinero en efectivo suficiente para refinanciar su deuda o cumplir las exigencias de efectivo, márgenes y garantías de las contrapartes (por ejemplo, retiros de depósitos). En muchas ocasiones, este riesgo se agudiza a causa del subdesarrollo o inexistencia de mercados de valores. Una liquidez escasa o una crisis de liquidez en situaciones difíciles puede producir cambios importantes en los precios y la volatilidad del mercado y provocar pérdidas considerables a los participantes en el mercado que se basan en su capacidad de hacer rotar posiciones rápidamente y a precios ventajosos. Los sistemas modernos de gestión del riesgo también dependen de unos niveles de liquidez adecuados, principalmente porque se basan en el cálculo de tasas de referencia precisas para la fijación de precios de carteras y para el buen funcionamiento de los mercados para el frecuente reajuste de posiciones.

Tipo de Riesgo	*Características*
Riesgo operacional	Es inherente a todas las actividades, productos, sistemas y procesos, y sus orígenes son muy variados (procesos, fraudes internos y externos, tecnológicos, recursos humanos, prácticas comerciales, desastres, proveedores).
Riesgo legal	Proviene de la legislación que afecta a los contratos mercantiles o financieros realizados. Es decir, que el ordenamiento jurídico nacional e internacional, en su caso, ofrezca la seguridad necesaria de que los contratos se ajustan a derecho, son válidos y que pueden hacerse cumplir.

Fuente: "Las entidades de crédito y la naturaleza cambiante de los riesgos en América Latina y el Caribe", Camilo E. Tovar, disponible en <https://www.bis.org/publ/bppdf/bispap33esp_c.pdf>.

Los riesgos para el sector bancario han experimentado cambios como consecuencia de la evolución de la estructura del mercado que, como hemos visto, se basa en tres componentes: la innovación tecnológica, la regulación-desregulación y la titularidad de las entidades de crédito (estatales-privadas y nacionales-extranjeras).

Sobre el último componente, diversos autores se han pronunciado; algunos consideran que los riesgos se incrementan si los bancos son públicos más que si son privados. Lo primero, porque constituye una fuente de riesgo para el sector bancario, ya que reduce la competencia, la productividad y el crecimiento económico, y porque, incluso, podrían incrementar la probabilidad de que se produzcan crisis bancarias. No obstante, a pesar de estos inconvenientes, también es posible que estos bancos tengan un efecto positivo sobre el riesgo, pues el crédito concedido por ellos es menos procíclico que el concedido por el sector privado.

En contraparte, se afirma que la titularidad extranjera mejora la eficiencia operativa, la intermediación financiera y el crecimiento a largo plazo del sector bancario, pueden mejorar la asignación del crédito y cuentan con mejores prácticas de gestión del riesgo, lo que seguramente haría que las entidades de crédito extranjeras mejoraran la correlación entre riesgo y beneficio por su capacidad de diseminar el riesgo, retener los depósitos locales y obtener fácilmente acceso a financiamiento externo. Otra tesis a favor indica que las entidades de crédito extranjeras podrían reducir la probabilidad de que se produzcan crisis bancarias, al ocasionar un crecimiento de los préstamos más fuerte y menos volátil que el generado por los bancos nacionales.

A pesar de estas ventajas, la titularidad extranjera de las entidades de crédito puede conllevar riesgos para el sistema bancario del país de acogida, puesto que su compromiso con el sistema bancario interno podría ser menor. También existe el inconveniente de que los bancos extranjeros puedan contagiar las perturbaciones de sus respectivos países.

Después de la crisis que se desencadenó en 2007, parece que la gestión de riesgos ha mejorado. El marco institucional ha desempeñado un papel fundamental, así como los marcos normativo y de supervisión, acompañados de mejor transparencia y gobernanza, con una tendencia a armonizar en cierta medida las normas y prácticas contables con los estándares internacionales. Basilea III ha tenido un papel fundamental.

Ejemplo de la armonización de las normas y practicas contables es la IFRS 9 "Instrumentos financieros" que fue emitida en julio de 2014 y obligatoria a partir del 1 de enero de 2018 para entidades que aplican IFRS.

La IFRS 9 que incluye: Clasificación y valuación, Contabilidad de coberturas y Deterioro fue necesaria después de la crisis financiera iniciada en 2008 en la que se identificó como una de las debilidades en las normas contables existentes el reconocimiento insuficiente y tardío de las pérdidas crediticias.

Una de las prioridades esenciales de IFRS 9 es lograr que las entidades reflejen más fielmente el riesgo de crédito que consta en su balance. Para conseguirlo los préstamos quedaron clasificados en tres etapas en función de su riesgo; los catalogados dentro de la Etapa 1 se considera que tienen un riesgo de impago bajo. Cuando se estime que la calidad crediticia de un préstamo ha empeorado significativamente (aunque sin generar pérdidas) se trasladará a la Etapa 2. La Etapa 3 comenzaría cuando el préstamo se deteriora hasta alcanzar el punto de "dudoso".

En México en 2017, la CNBV inició el proyecto para adaptar la regulación aplicable a las entidades supervisadas al nuevo marco internacional. Como resultado de la emisión de la IFRS 9, el Consejo Mexicano para la Investigación y Desarrollo de Normas de Información Financiera (CINIF) publicó 10 nuevas Normas de Información Financiera (NIF) que entraron en vigor el 1 de enero de 2018. Al cierre de esta edición (febrero de 2020) ya se contaba con la modificación a la Circular Única de Bancos (CUB) en materia de IFRS9, aunque aún no estaba publicada en el Diario Oficial de la Federación.

Supervisión

La capacidad total de absorción de pérdidas (TLAC) es un buen ejemplo de la supervisión con estándares internacionales. En la nota conceptual sobre el TLAC (22 de noviembre de 2019), se establece la composición del capital en el marco de Basilea III y el requerimiento de TLAC:

Conforme al requerimiento mínimo de capital para los bancos que se establece en el marco de Basilea III, el capital regulatorio debe cubrir, al menos, 8 por ciento de los activos ponderados por riesgo (APR), compuesto de la siguiente forma:

- Capital básico (Tier 1 o "T1", por sus siglas en inglés): debe cubrir por lo menos 6 por ciento de APR y puede ser de dos tipos:
- Capital fundamental (Common Equity Tier 1 CET1, por sus siglas en inglés): debe cubrir, al menos, 4.5 por ciento de APR.
- Capital básico no fundamental (Additional Tier 1 o AT1, por sus siglas en inglés): debe cubrir al menos la diferencia, si hubiera, entre 6 por ciento y CET1 de APR.
- Capital complementario (Tier 2 o T2, por sus siglas en inglés): debe cubrir al menos la diferencia, si hubiera, entre 8 por ciento y T1 de APR.

Adicionalmente, los bancos deben constituir suplementos de capital en exceso del requerimiento mínimo. Estos suplementos son los siguientes:

- Suplemento de conservación de capital (Capital Conservation Buffer o CCB, por sus siglas en inglés): debe constituirse

con CET1 por 2.5 por ciento del monto de APR.
- Suplemento de capital contracíclico (Countercyclical capital buffer o CCyB, por sus siglas en inglés): debe constituirse con CET1 por 0-2.5 por ciento del monto de APR, a juicio de la autoridad competente.
- Suplemento de capital para bancos de importancia sistémica:
    - Bancos de importancia sistémica global (Global Systemically Important Banks o G-SIB, por sus siglas en inglés): debe constituirse con CET1 por 1-3.5 por ciento del monto de APR.
    - Bancos de importancia sistémica local (Domestic Systemically Important Banks o D-SIB, por sus siglas en inglés): cada jurisdicción establece el porcentaje de APR por el que se constituirá. En México, este suplemento va de 0.6 a 2.25 por ciento de APR.

Por lo anterior, en México, el requerimiento de capital mínimo de Basilea III, considerando también los suplementos, puede ir desde 10.5 hasta 15.25 por ciento de APR, dependiendo de las características de la institución y del nivel del CCyB.

Respecto al requerimiento de TLAC, este estándar forma parte de la agenda del Consejo de Estabilidad Financiera (FSB, por sus siglas en inglés) para mitigar el riesgo que representan las G-SIB y el problema de instituciones que son demasiado grandes o importantes para dejarlas quebrar, conocido como *Too Big To Fail*. El objetivo del requerimiento TLAC es que las G-SIB puedan absorber pérdidas y ser recapitalizadas durante un proceso de resolución, sin interrumpir sus funciones críticas y sin la necesidad de hacer uso de recursos públicos (*bail-out*). Como es costumbre, se espera que las jurisdicciones miembros del FSB adopten el estándar.

El requerimiento adicional de capital para cumplir con el estándar TLAC para las entidades de resolución de las G-SIB ubicadas en mercados desarrollados es de 8 por ciento de APR a partir de enero de 2019 y de 10 por ciento de APR a partir de 2022 (es decir, el requerimiento total de capital y TLAC, sin tomar en cuenta los suplementos y sobrecargas de capital, será de 16 por ciento en 2019 y de 18 por ciento en 2022).

Preocupación explícita

El reconocimiento, por parte de las entidades de crédito, de la importancia de la gestión de riesgos se refleja, en primer lugar, en la creación de unidades internas de gestión de riesgo y, en segundo, en el hecho de que los consejos de administración de las entidades de crédito tomen en consideración de forma explícita la gestión de riesgos.

Además, se han producido mejoras técnicas importantes, como el cambio de manera de enfocar la valoración, la cuantificación de los riesgos y la fijación de precios del crédito, así como la asignación de éste. Las entidades de crédito de la región están adoptando técnicas de evaluación de riesgos más avanzadas, como las de valor en riesgo, pruebas de estrés y la calificación del riesgo crediticio. Sin embargo, la implementación de técnicas de evaluación de riesgos más sofisticadas conlleva la aparición de una serie de problemas, como la dificultad para obtener datos para calcular las probabilidades de impago y la falta de técnicas adecuadas para diseñar y calibrar modelos para la evaluación de escenarios alternativos.

La manera en la que se gestionan todas aquellas actividades que ayudan al manteni-

miento y éxito de una compañía dependerá del tipo de organización y mercado. En el caso del sector bancario, es de vital importancia el manejo de todos los riesgos que de distintas formas alteran e impiden el desarrollo de todos sus procesos.

No obstante, en este escenario de mejoras vuelven a aparecer, con una importancia muy grande, las Tecnologías de Información, que han mejorado los productos desarrollados a raíz de la desregulación y han incorporado otros productos y servicios, así como nuevos actores para plantear una nueva ingeniería financiera en la que las fintechs están en primer plano para transformar la arquitectura del sistema financiero.

5. La gestión de riesgos se abre a nuevos actores

Las diversas situaciones financieras adversas que se han suscitado han propiciado que se les tengan presentes para medir y evaluar diversos aspectos como el qué y el cómo, pero, sobre todo, para establecer acciones que eviten su repetición o que sirvan para dar respuesta a situaciones que surgen en los nuevos contextos. En este sentido, cobra importancia la administración de riesgos y su alcance, dependiendo de su manejo y perspectiva.

Un sistema de administración de riesgos es un conjunto de prácticas y procedimientos llevados a cabo por una organización para identificar, evaluar, controlar y mitigar todas aquellas circunstancias que, de un modo u otro, impidan el cumplimiento de sus objetivos y el mejoramiento continuo de sus procesos. Cualquier organización que desee permanecer en el mercado, desarrollarse, crecer y ser competitiva deberá necesariamente implementar un sistema que contribuya a abordar y gestionar de la mejor manera todo aquello que impida el logro de sus metas.

Para que un sistema de administración de riesgos sea efectivo para una empresa financiera, es necesario un continuo conocimiento y actualización en relación con los estándares y prácticas internacionales. Sin embargo, la restructuración bancaria, unida a un fortalecimiento de la regulación internacional, son necesarios, pero no suficientes, para evitar situaciones de crisis futuras, por lo que la clave radicará en el modelo de gestión de riesgos desarrollado por entidades financieras.

Recientemente, se ha podido constatar cómo, dentro de un mismo sistema financiero, con idénticas normas regulatorias, las estrategias de expansión han sido diferentes, así como la intensidad del crecimiento de la cartera crediticia y su nivel de concentración. Incluso, dentro de una misma estrategia, no todas la entidades han realizado la misma selección de riesgo de crédito, lo que ha quedado reflejado, por ejemplo, en los diferentes ratios de morosidad y cobertura.

El riesgo es esencial en toda actividad empresarial, y en el ámbito bancario, el análisis, la medición y la gestión del riesgo adquieren una importancia capital por la cantidad de recursos que moviliza la industria bancaria, afectando transversalmente todos los sectores productivos, y por la propia estructura de balance de la empresa bancaria. La importancia estratégica de la banca en la economía productiva ha motivado que la regulación del riesgo de la banca no sea autónoma ni discrecional. De hecho, las autoridades económicas y monetarias están muy interesadas en la viabilidad permanente, a raíz de las dinámicas consecuencias que han aportado las quiebras de importantes entidades en el pasado.

En el estudio "Banking Banana Skins 2015 The CSFI Survey of bank risk",[2] se concluyó que los cambios dramáticos en la industria bancaria global se reflejan en transformaciones igualmente importantes en las percepciones de los riesgos, y que la preocupación por la calidad de la administración de los riesgos de los bancos está aumentando.

La banca, dada su estrecha relación con los mercados, es muy consciente de la necesidad de innovación, de nuevos escenarios tecnológicos y de los beneficios de la gestión del cambio; para ello, precisa el desarrollo de nuevos servicios y productos, de la gestión de nuevos canales de distribución, de un mayor desarrollo relacional con sus clientes y de la mejora de la calidad del servicio. Una de las prioridades en casi todas las instituciones financieras a nivel mundial es atraer y retener a los clientes, pero siempre considerando la administración de riesgos para evitar males mayores.

6. Ciberseguridad: riesgos al acecho

El sector financiero ha experimentado uno de los mayores índices de digitalización en los últimos años. Los avances en la tecnología de la información han hecho que los intermediarios y los mercados financieros se entrelacen fuertemente y, a la vez, que los ataques cibernéticos aumenten y se conviertan en riesgos para el sistema.

En mayo de 2018, se prendieron las alertas del sistema financiero mexicano ante una falla a gran escala en operaciones de la Banca. Días después, se confirmó un hackeo estimado en alrededor de 400 millones de pesos al Sistema de Pagos Electrónicos Interbancarios (SPEI) del Banco de México, destacando como uno de los más grandes delitos cibernéticos conocidos en el país. El incidente puso al descubierto vulnerabilidades tecnológicas del sistema financiero, así como la necesidad de robustecer el marco regulatorio que en ese momento se tenía en el país, en materia de ciberseguridad.[3]

---

[2] "Banking Banana Skins 2015 The CSFI Survey of bank risk", PwC/Centre for Study of Financial Innovation, 2015.

[3] Con el propósito de propiciar el buen funcionamiento de los sistemas de pagos, el Banco de México (Banxico) publicó nuevos requerimientos a los participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI) para reforzar las políticas y controles en las transferencias de fondos. Banxico estableció obligaciones adicionales a los participantes del SPEI, como mejorar los esquemas de respuesta ante posibles riesgos y contar con una identificación plena de las operaciones, en particular cuando se traten de transferencias a empresas que pueden permitir la salida de recursos del sector financiero hacia activos virtuales. De conformidad con los "Principios para reforzar la seguridad de la información en el sistema financiero", reconocidos por el Consejo de Estabilidad Financiera, publicó las circulares 10/2018 y 11/2018, que atienden aspectos como seguir los protocolos de acción ante posibles ataques a la infraestructura tecnológica relacionada con el SPEI, que establezca el Banco de México en su carácter de administrador del sistema, mediante los avisos que este emita. Se obliga a contar con protocolos y procedimientos que documenten las medidas y acciones que se deben tomar en caso de que se materialicen riesgos de ciberseguridad en su infraestructura tecnológica, en sus canales electrónicos y en la infraestructura tecnológica provista por terceros, que pudiera afectar la operación de la institución financiera en el SPEI. Asimismo, los participantes deberán establecer e implementar pruebas de confianza e integridad a su personal, así como al de terceros que provean servicios de tecnología de la información y comunicación, que tengan acceso a información y sistemas relevantes en su operación con el SPEI. Además, debe designarse un oficial de seguridad de la información responsable del diseño, implementación y verifica-

Ya en 2016, el gobierno de Estados Unidos había atendido el tema al crear el Centro de Análisis y Resiliencia del Sistema Financiero (FSARC) para identificar el riesgo sistémico del sistema financiero ante las amenazas actuales y emergentes de ciberseguridad.

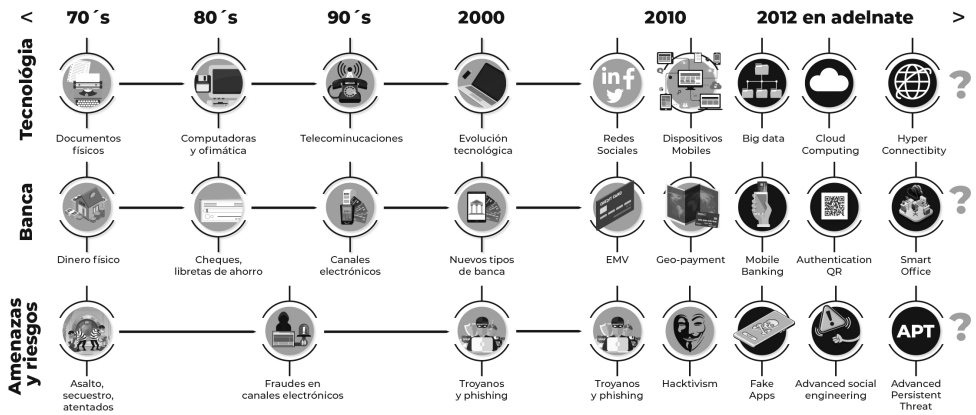
El FSARC surgió como respuesta a la necesidad de identificar entidades financieras a las cuales un incidente cibernético pudiera generarles un impacto significativo y, a la vez, de comprender y mitigar el riesgo de los ataques cibernéticos y su impacto en la estabilidad financiera, dado que, históricamente, las vulnerabilidades del sistema financiero han conducido a recesiones o crisis económicas, periodos de deflación, bajo crecimiento económico y desempleo.

Lo anterior era un tema que no podía postergarse, dado que los ataques cibernéticos pueden comprometer los ingresos netos del sistema bancario. Un estudio del Fondo Monetario Internacional (FMI),[4] a través de modelaciones de riesgo financiero y con una muestra de 7,947 entidades bancarias de todo el mundo, señala que pueden comprometerse desde 9 a 62 por ciento de los ingresos netos de las entidades (97 mil millones de dólares a 642 mil millones) por ataques cibernéticos.

El estudio asume dos escenarios a partir del número de ataques, de la posibilidad de riesgo de contagio y de metodologías de cálculo de riesgo financiero:

CUADRO 3.

Evolución de los riesgos de seguridad en la industria bancaria



ción de las políticas de prevención de riesgos de ciberseguridad, así como de la implementación de medidas correctivas ante la materialización de estos riesgos que pudiera afectar la operación de la institución en el SPEI. Banxico apuntó que, de manera adicional a estas circulares, se establecieron requerimientos para robustecer los elementos de seguridad en la prestación de servicios de transferencias de fondos a aquellos clientes o empresas que ofrezcan el intercambio o compraventa de activos virtuales.

[4] Antoine Bouveret, 2018, "Cyber Risk for the Financial Sector: A framework for Quantitative Assesment", IMF Working Paper WP/18/143.

Escenario de línea base e independencia	*Escenario dos*
Se asumen el número de ataques registrados en 2013 y sin riesgo de contagio.	Asume que la cantidad de ataques cibernéticos es dos veces la registrada en 2013.
Bajo estos supuestos, pueden comprometerse de 9 por ciento de los ingresos netos (97mil millones de dólares) hasta 19 por ciento (201 mil millones). Si se asume riesgo de contagio, los ingresos comprometidos pueden ser desde 12 por ciento de los ingresos (97 mil millones) hasta 32 por ciento (que representa cerca de 329 mil millones).	Con el supuesto de independencia, sin riesgo de contagio, pueden comprometerse desde 26 por ciento de los ingresos (268 mil millones) hasta 52 por ciento (539 mil millones). Si se asume riesgo de contagio, los ingresos comprometidos ascienden desde l 34 por ciento de los ingresos (351 mil millones) hasta 62 por ciento (642 mil millones).

Según la Oficina de Investigación Financiera (OFR) del Departamento del Tesoro de Estados Unidos, los incidentes de ciberseguridad generan riesgos de contagio, financiamiento y liquidez, y hay cuatro canales a través de los cuales los riesgos pueden ser transmitidos:

1. Pocos actores sustitutos

El sistema financiero está altamente interconectado y relacionado con empresas de sectores, como servicios públicos, sistemas de comercio electrónico y cámaras de compensación, que desempeñan funciones vitales para toda la sociedad. La industria de servicios financieros, sin embargo, basa su infraestructura en el uso de Tecnologías de la Información y Comunicaciones para realizar transacciones y pagos. En el caso de una afectación sistémica, habría pocas alternativas, instituciones y empresas de servicios públicos.

2. Pérdida de confianza y reputación

Ataques a cajeros automáticos, denegación de servicio a una o más instituciones financieras, fallas en los sistemas inducidos y fugas de información sensible de los banqueros o reguladores podrían provocar pérdidas de confianza sistémicas.

3. Integridad de los datos

Los impactos sistémicos pueden surgir a partir de incidentes que afectan la calidad de los datos del mercado y el consumidor, y causar una pérdida de integridad de los datos.

4. Pocos proveedores

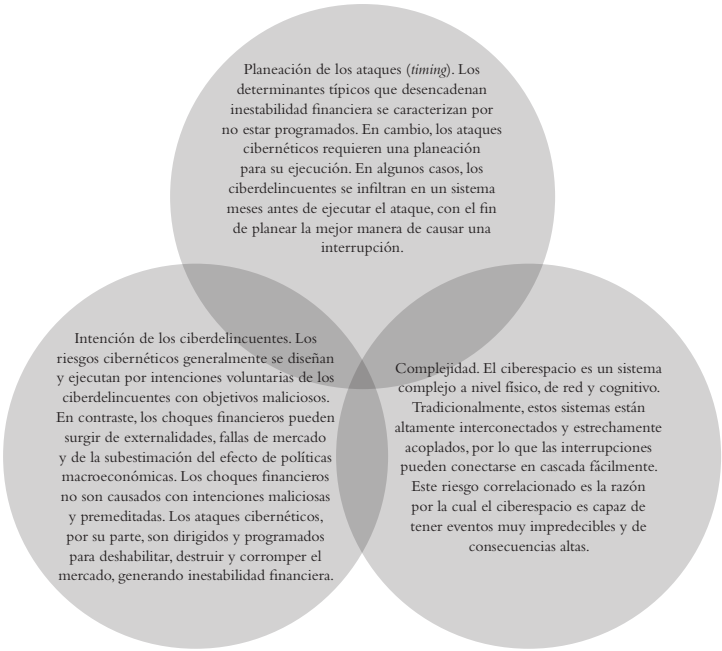
La computación y el almacenamiento del mundo se concentra en pocos proveedores de servicios en la nube, por lo que la afectación puede ser en industrias enteras o zona geográficas.

Según la OFR, existen tres diferencias entre los choques cibernéticos y financieros que pueden crear inestabilidad financiera sistémica: planeación (*timing*), complejidad e intención adversa.[5]

[5] U.S. Treasury Department Office of Financial Research, 2017, "Cybersecurity and Financial Stability: Risks and Resilience", disponible en <https://www.financialresearch.gov/viewpoint-papers/files/OFRvp_17-01_Cybersecurity.pdf>, consultado el 13 de enero de 2020.

CUADRO 4.

Choques cibernéticos y financieros



Los ataques cibernéticos, como ya se explicó, difieren de los choques financieros y de políticas tradicionales tanto en la intención como en el momento. Si bien, ningún ataque hasta la fecha ha generado inestabilidad financiera, el impacto potencial de un ataque cibernético programado para desestabilizar las funciones y vulnerabilidades de los canales tradicionales del sistema financiero no se ha examinado suficientemente.

Según el reporte "Riesgo cibernético y el futuro de la estabilidad financiera",[6] los delincuentes cibernéticos pueden causar tres tipos de crisis:

1. **Crisis de combustión lenta.** Se producen cuando un ciberdelicuente usa las capacidades cibernéticas para causar fricción a largo plazo, pérdida de confianza e interrupción de los servicios.
2. **Crisis exacerbadas.** Ocurren cuando una crisis financiera ya está en progreso, o cuando una nación está al borde de una, y un adversario intencionalmente le da un empujón con un ataque cibernético.
3. **Crisis premeditadas.** Surgen cuando los ciberdelincuentes utilizan capacidades para crear desde cero una crisis financiera. Ejemplo de ello son los

[6] Asobancaria. Semana económica, marzo de 2019.

ataques a una infraestructura financiera crítica cibernética, como sistemas de pago.

Por otra parte, el Instituto de Finanzas Internacionales (IFF) considera cuatro escenarios de riesgo cibernético que pueden afectar la estabilidad financiera.[7]

1. **Ataque cibernético a sistemas de pago al por mayor y minoristas.** Un ataque a estos sistemas puede interrumpir la prestación de servicios esenciales durante periodos de tiempo prolongados.
2. **Robos a gran escala de datos.** Ataques cibernéticos dirigidos a depósitos de centrales de valores pueden generar cambios en la estabilidad financiera.
3. **Ataques a la infraestructura de la que depende el sistema financiero, como la red eléctrica.**
4. **Ataques a consumidores minoristas y a la sociedad en general.** Provocaría desconfianza en la seguridad y la solidez de las partes del sistema financiero, debido a unos pocos ataques cibernéticos muy significativos o muchos ataques menores muy frecuentes y exitosos contra instituciones financieras o infraestructuras de mercados financieros.

Si realizáramos un ejercicio a partir de los tipos de crisis y escenarios, podríamos dimensionar el tamaño de una crisis en el sistema financiero a partir de un ciberataque. Para ejemplificar este punto, podemos referir tres experiencias pasadas.

En febrero de 2016, en el Banco Central de Bangladesh, un grupo de atacantes consiguió infectar el sistema con malware creado específicamente para la ocasión e intentó realizar transferencias fraudulentas por un valor de 951 millones de dólares. Dicha cantidad se encontraba en la cuenta que el Banco Central de Bangladesh tenía en el Banco de la Reserva Federal de Nueva York. Afortunadamente, la mayoría de trasferencias pudieron ser bloqueadas y únicamente se robaron 81 millones de dólares.

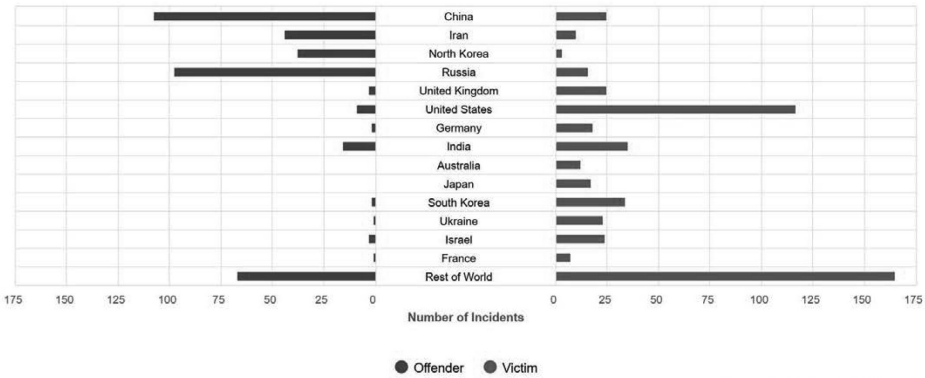
Otro caso se dio en el último trimestre de 2015 en el banco Tien Phon Bank, un banco comercial vietnamita donde los ciberdelincuentes también trataron de realizar transferencias a través de SWIFT, pero la entidad se dio cuenta a tiempo y logró bloquearlas, mismas que ascendían a un millón de dólares. Un poco antes, en enero de 2015, el banco ecuatoriano Banco del Austro sufrió un ataque parecido y le lograron robar 9 millones de dólares.

Esfuerzos conjuntos

El riesgo cibernético representa una amenaza creciente a nivel mundial, no sólo en cuanto a la frecuencia de los ataques, sino en relación con la cuantía o severidad del impacto monetario que ocasiona en las entidades. El sector financiero se constituye como el principal segmento de la economía que es objeto de ataques cibernéticos; por eso, y debido a su importancia sistémica, en la mayoría de los países entidades públicas y privadas se han abocado a desarrollar acciones de protección, resiliencia y políticas públicas.

[7] Martin Boer y Jaime Vazquez, 2017, "Cyber Security & Financial Stability: How Cyber-Attacks Could Materially Impact the Global Financial System", Institute of International Finance, disponible en <www.iif.com/system/files/iif_cyber_financial_stability_paper_final_11_13_2017_clean.pdf>.

GRÁFICA 1.
Número de ciberataques por país



Fuente: CSIS & Hackmageddon, disponible en <https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf>.

Podemos mencionar que, en 2013, en Estados Unidos, el Departamento de Seguridad diseñó una política pública para identificar infraestructuras que pudieran verse afectadas por ataques cibernéticos, como el sistema de salud pública, seguridad económica y seguridad nacional. A partir de esto, ocho de los bancos decidieron, a nivel de CEO, unirse para crear el Centro de Resistencia y Análisis Sistémico Financiero (FSARC), que ahora es una subsidiaria del FS-ISAC.

Los miembros fundadores —Bank of America, BNY Mellon, Citigroup, Goldman Sachs, JPMorgan Chase, Morgan Stanley, State Street y Wells Fargo— tuvieron como objetivo identificar, analizar, evaluar y coordinar de manera proactiva las actividades a fin de mitigar el riesgo sistémico para el sector financiero estadounidense.

Además, crearon el sistema de amenazas de seguridad cibernética actuales y emergentes a través de operaciones enfocadas y de una mejor colaboración entre las firmas participantes, socios de la industria y el gobierno de Estados Unidos.[8] Dentro de esos sistemas se realizan ejercicios de ataques cibernéticos en los sectores público y privado, que desempeñan un papel importante en la identificación de brechas y puntos débiles para una posible explotación.

Sheltered Harbor, una organización encargada de proteger la confianza del público en el sistema financiero de Estados Unidos, fue el resultado directo de las lecciones aprendidas de estos ejercicios cibernéticos. Trimestralmente, los principales actores de la industria bancaria se someten a un ejercicio que simula un escenario de ataque diferente.

De acuerdo con la National Automated Clearance House Association (NACHA), estas simulaciones ayudan a:

- Identificar brechas en los planes de respuesta a incidentes.

[8] Office of Financial Research, 2016, "2016 Financial Stability Report", disponible en <https://www.financialresearch.gov/financial-stabilityreports/files/OFR_2016_Financial-Stability-Report.pdf>.

- Fortalecer las relaciones del equipo de respuesta a incidentes.
- Desarrollar la comprensión de las vulnerabilidades del sistema.
- Impulsar la exploración de mejoras en la respuesta.

El sistema financiero ha logrado un gran progreso en la defensa cibernética, tanto a nivel nacional como transfronterizo. Ahora se están realizando ejercicios de simulación de crisis cibernética, se mapean los riesgos de ciberseguridad y pueden detectarse las vulnerabilidades en las redes; sin embargo, el uso de nuevas tecnologías y la participación de nuevos actores, como las fintechs, presenta un escenario en el que algunas tecnologías tendrán un impacto sistémico, otras acelerarán el riesgo y otras más lo reducirán, lo que plantea retos para mantener la estabilidad financiera y reducir el riesgo cibernético.

Para atenderlos, diversas organizaciones han planteado acciones como: armonizar las regulaciones internacionales que fomenten la resistencia a los ataques cibernéticos y mitiguen el riesgo en caso de un ataque, llevar a cabo investigaciones adicionales para identificar datos y facilitar el diseño de modelos para medir o cuantificar el riesgo cibernético, compartir y desarrollar mapas para comprender mejor el riesgo cibernético en los mercados e instituciones y realizar más ejercicios de simulación de incidentes cibernéticos, a nivel nacional y transfronterizo.

El ataque cibernético que sufrió el Banco de Bangladesh en 2016 es un ejemplo de la no existencia de fronteras y de la necesidad de acciones conjuntas, ya que ese incidente involucró, además de a Bangladesh, a Estados Unidos y Filipinas, de acuerdo con la ruta de los atacantes que cada año se vuelven más severos, por lo que, de acuerdo con el Informe Global de Riesgos del Foro Económico Mundial 2019, los ataques cibernéticos a gran escala y el desglose de las redes y la infraestructura esencial de la información (colapso de la infraestructura de información esencial) son considerados riesgos tecnológicos a escala mundial.

La tecnología sigue desempeñando una función profunda en la conformación del panorama de riesgos mundiales para individuos, gobiernos y compañías. "En la GRPS, el fraude y robo masivo de datos se ubicó en el número cuatro de riesgo mundial por probabilidad, en un lapso de 10 años, y los ataques cibernéticos quedaron situados en el número cinco. Esto mantiene un patrón que

CUADRO 5.

Evolución de los riesgos globales en términos de probabilidad

	2015	2016	2017	2018	2019
1	Conflicto interestatal con consecuencias regionales	Migraciones involuntarias a gran escala	Cambio climático extremo	Cambio climático extremo	Cambio climático extremo
2	Cambio climático extremo	Cambio climático extremo	Migraciones involuntarias a gran escala	Grandes desastres naturales	Falla en la mitigación y adaptación del cambio climático
3	Fallas de gobernanza nacional	Falla en la mitigación y adaptación del cambio climático	Grandes desastres naturales	Ciberataques	Grandes desastres naturales
4	Crisis de Estados	Conflicto interestatal con consecuencias regionales	Ataques terroristas a gran escala	Robo de datos y fraude	Robo de datos y fraude
5	Alto desempleo estructural o informalidad	Grandes catástrofes naturales	Incidente masivo de robo de datos	Falla en la mitigación y adaptación del cambio climático	Ciberataques

Económicos | Ambientales | Tecnológicos | Sociales | Geopolíticos

Fuente: Foro Económico Mundial.

se registró el año pasado, con la consolidación de la posición de los riesgos cibernéticos junto a los riesgos ambientales en el cuadrante de alto impacto y alta probabilidad del panorama de riesgos mundiales" (WEF, 2019).

Actualmente, la ciberseguridad es un aspecto crítico y las entidades e instituciones financieras tienen que estar preparadas para recibir ataques sin precedentes que no sólo pretenderán obtener sus recursos económicos y los de sus clientes (socios, asociados o usuarios), sino también, y cada vez más, información sobre estos últimos.

¿Cómo pinta México?

En los últimos dos años, entidades financieras en México han sufrido con mayor frecuencia ataques a las infraestructuras de pagos y cajeros automáticos, que han representado pérdidas por montos significativos. En un esfuerzo por conocer el panorama, la Organización de Estados Americanos y la Comisión Nacional Bancaria y de Valores realizaron el estudio "Estado de la ciberseguridad en el sistema financiero mexicano".[9] Los resultados del informe[10] muestran el estado actual de las entidades a nivel de gestión de riesgos de seguridad digital y el impacto que han tenido los incidentes de seguridad digital; asimismo, realiza recomendaciones al sistema financiero.

En cuanto a preparación y gobernanza, el informe indica que la mayoría de las entidades e instituciones financieras (70 por ciento) dicen tener una única área responsable de la seguridad de la información (lo que incluye ciberseguridad) y prevención del fraude por medios digitales. Las organizaciones de mayor tamaño, como los bancos tradicionales, suelen tener más de una (43 por ciento) en un porcentaje mucho mayor que las pequeñas (24 por ciento).

Otro elemento que muestra es la distancia jerárquica entre el CEO y el responsable de la ciberseguridad, ya que un trato directo con el director de la organización suele traducirse en respuestas más rápidas a incidentes y un mejor acompañamiento de los objetivos de negocio. La distancia más corta puede encontrarse con mayor facilidad en las entidades pequeñas, de las que 60 por ciento declaró que el responsable de seguridad digital reporta directamente al CEO, mientras que en ninguna entidad grande ocurre de esta manera: 50 por ciento reporta tener dos niveles entre su director general y el encargado de la ciberseguridad. Además, mientras más grande es la organización, más niveles se suman entre estas dos figuras.

Por otro lado, el consejo de administración de 50 por ciento de las entidades e instituciones financieras en el país recibe reportes periódicos acerca de indicadores, riesgos, gestión de riesgos de seguridad de la información y fraudes ocurridos a través de medios digitales. A pesar de la distancia mayor entre CEO y equipos de seguridad, las entidades grandes llevan la delantera en este apartado, con 86 por ciento de instituciones que mantienen esta práctica, frente a 45 por ciento de las medianas. Sectores como el bursátil o el de banca comercial superan además el porcentaje presentado por América Latina y el Caribe.

Sin embargo, la alta dirección no está entregando los recursos suficientes a las áreas de seguridad. "El rol que juega la alta dirección

[9] "Estado de la ciberseguridad en el sistema financiero mexicano", OEA/CNBV, 2019.

[10] El estudio presenta los resultados y análisis sobre los incidentes de seguridad de la información (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales), producto de las encuestas realizadas a diversas entidades e instituciones financieras del sistema financiero mexicano.

y la junta de las organizaciones respecto de la seguridad digital es fundamental", indica el estudio, y explica que, para la mayoría de las entidades e instituciones financieras (48 por ciento del total), es medianamente complejo lograr que la alta dirección de la organización tome decisiones de inversión en soluciones de seguridad digital, mientras que tan sólo 17 por ciento de las organizaciones lo consideran altamente complejo. Se destaca el hecho de que sectores como fintechs y de ahorro y crédito popular encuentran, mayoritariamente (ambos con 53 por ciento), que es poco complejo que la alta dirección tome decisiones de inversión en soluciones de seguridad digital.

Respecto del tamaño del equipo que maneja procesos asociados a la seguridad de la información (incluida la ciberseguridad) y fraudes ocurridos a través de medios digitales, se aprecia que en promedio una entidad financiera en México cuenta con un equipo conformado por nueve personas. Este valor varía significativamente, dependiendo del tamaño y sector de la entidad, pues mientras que en la banca comercial el promedio es de 37 profesionales, en sectores como el de ahorro y crédito popular es tan sólo de tres. Entre las entidades e instituciones financieras en México, 68 por ciento considera adecuado que estos equipos crezcan en el corto plazo.

Los servicios más contratados por las organizaciones financieras suelen estar más ligados a asegurar la robustez de sus servicios: pruebas de seguridad y análisis de vulnerabilidades (34 por ciento), monitoreo de la infraestructura de seguridad (31 por ciento), gestión de cumplimiento (18 por ciento) y servicios de seguridad en la nube (18 por ciento).

La adopción de marcos de seguridad internacionales es clave para otorgar estándares altos, pero la adopción en México no sigue un camino unificado. De acuerdo con la OEA, el costo total de respuesta y de recuperación ante incidentes de seguridad digital, para una entidad financiera grande promedio en México, equivale aproximadamente a 2.3 millones de dólares al año; para una entidad mediana promedio, supone aproximadamente 634,689 dólares, y para una entidad pequeña promedio equivale a 317,615 dólares.

Según el informe, las principales acciones y medidas técnicas que las entidades e instituciones financieras de México ejecutan son los *firewalls* (85 por ciento), actualización automatizada de antivirus y sistemas (76 por ciento), copias de seguridad automatizadas (68 por ciento) y *network security* —como VPN, NAC, ISE, IDS/IPS, entre otras— (54 por ciento).

El uso de tecnologías digitales emergentes se encuentra aún rezagado. Sólo 22 por ciento de instituciones financieras implementan analítica de datos en herramientas, controles o procesos, 13 por ciento de entidades e instituciones financieras implementan *machine learning* y 9 por ciento, inteligencia artificial. El informe destaca el hecho de que en el sector bancario el uso de big data registra un promedio de 45 por ciento, lo cual supera por mucho el promedio del sector financiero de América Latina y el Caribe (29 por ciento).

En cuento a la inversión, 51 por ciento de las entidades mexicanas manifiesta que su presupuesto de seguridad digital equivale a menos de 1 por ciento del EBITDA del año fiscal anterior. Además, en comparación con el año fiscal inmediato anterior, 57 por ciento manifiesta que se mantuvo sin variación el presupuesto de seguridad de la información y prevención del fraude digital, 38 por ciento, que había aumentado y sólo 5 por ciento, que había disminuido. Los grandes bancos de México invierten con mayor ímpetu: 31 por ciento señalaron que el presupuesto se mantuvo sin variación, 64 por ciento, que aumenta y 5 por ciento, que disminuye.

La OEA confía en que hay un camino correcto por seguir para reforzar los niveles de protección y respuesta a incidentes en sus

organizaciones. Una cultura de colaboración más robusta, la necesidad de que la ciberseguridad sea una preocupación que alcance a toda la organización y el cambio del paradigma del *compliance* a uno de ciber-resiliencia fueron las ideas esgrimidas con mayor confianza.

En el informe, la OEA emitió algunas recomendaciones para mejorar la ciberseguridad de las instituciones que integran el sistema financiero nacional. Entre ellas:

- Informar a la alta dirección de las empresas o instituciones sobre los riesgos de ciberseguridad detectados.
- Tener claro, en los niveles más altos de las organizaciones, que las situaciones que deben atenderse son algo fundamental para darle visibilidad a los problemas y tomar decisiones acertadas.
- Trabajar en la construcción de barreras o perímetros seguros, así como en la detección de eventos a través de un monitoreo constante y el registro de comportamientos anómalos.
- Compartir información entre instituciones financieras para generar mayor inteligencia y que esto les permita estar mejor preparados ante cualquier amenaza.
- Saber cómo proceder cuando se detecta algún incidente o la posibilidad de que ocurra. Esto es, prever cómo se va a responder a un incidente, cómo se va a escalar, a quién se le va a reportar o, más allá de lo que exija la autoridad, si se tiene que reportar a los cuentahabientes y de qué forma hacerlo.

Radiografía: situación, alcances y respuesta

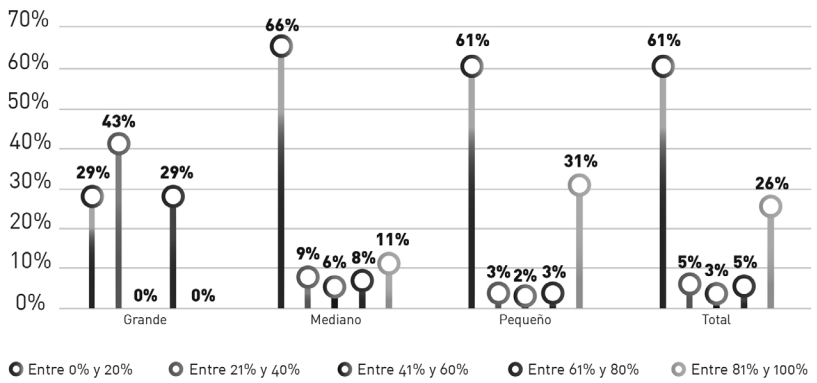
En la siguiente sección se muestra una selección de gráficas del estudio realizado por la OEA, con la finalidad de tener una idea de la situación, alcances y respuesta de las entidades que forman el sistema financiero mexicano.

7. Prácticas regulatorias de seguridad cibernética

De acuerdo con el Instituto de Estabilidad Financiera del BIS, son pocas las economías a nivel mundial que cuentan con re-

GRÁFICA 2.

Porcentaje de operaciones que se realizaron por medio de canales transccionales no presenciales



Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

CUADRO 6.

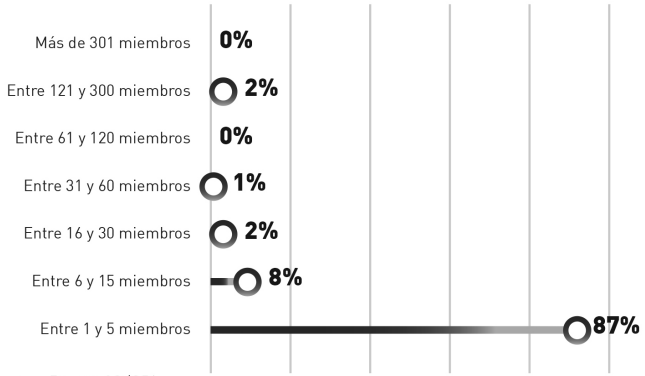
Porcentaje de profesionales de seguridad de la información (incluyendo ciberseguridad) por sector y tamaño de Entidad / Institución Financiera en México

	Grande	Mediana	Pequeña	Total
Banca Comercial o Múltiple	91	25	24	37
Banca de Desarrollo		10	7	9
Sector Bursátil			36	36
Sector de Ahorro y Crédito Popular (SOCAP)		4	3	3
Sector de Ahorro y Crédito Popular (SOFIPO)	3	3	3	3
Sector de Intermediarios Financieros No Bancarios		3	3	3
Sector FINTECH			4	4
SISTEMA FINANCIERO MEXICANO	79	9	7	9

Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

GRÁFICA 3.

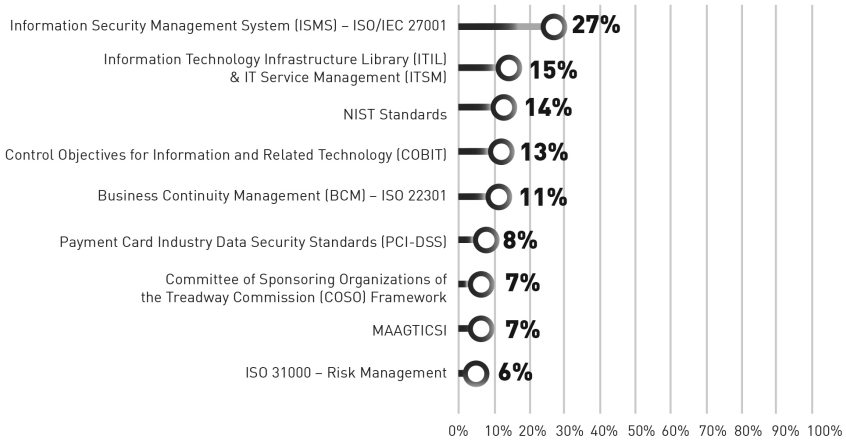
Personas que conforman la totalidad de equipos que manejan procesos asociados a la seguridad de la información (incluyendo ciberseguridad) y fraudes ocuridos a través de medios digitales.



Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

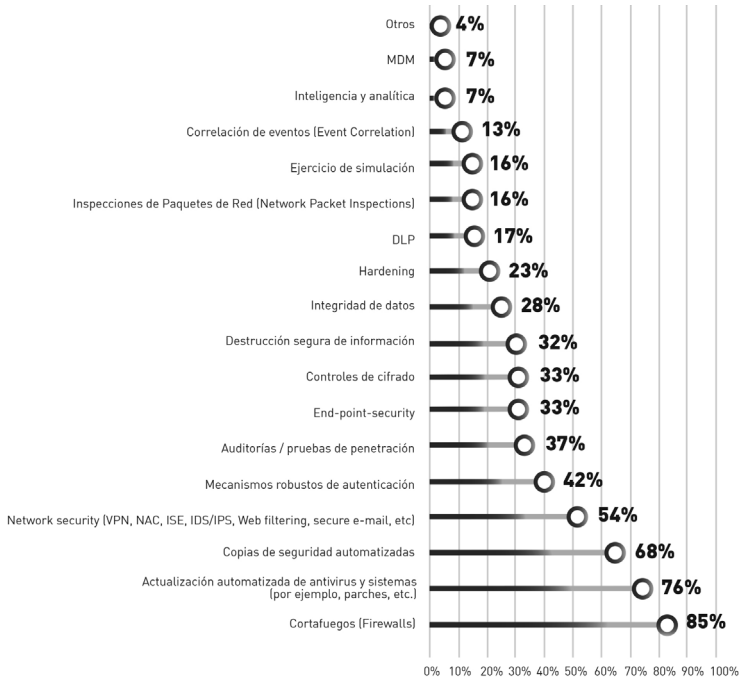
GRÁFICA 4.

Marcos de seguridad y/o estándares internacionales adoptados



GRÁFICA 5.

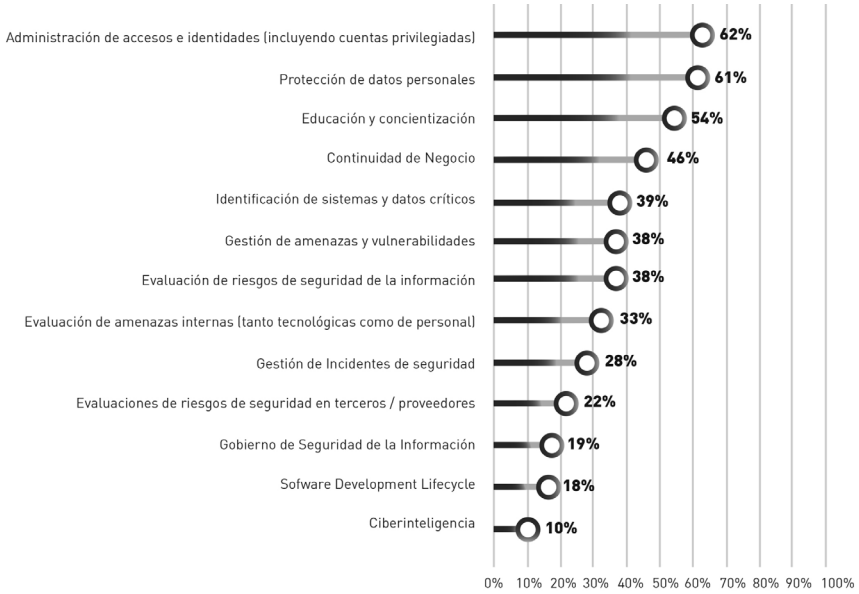
Acciones y medidas técnicas de seguridad de la información (incluyendo ciberseguridad) para proteger los sistemas de información críticos



Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

GRÁFICA 6.

Procesos / programas respecto a la seguridad digital implementados actualmente por las entidades e instituciones financieras



CUADRO 7.

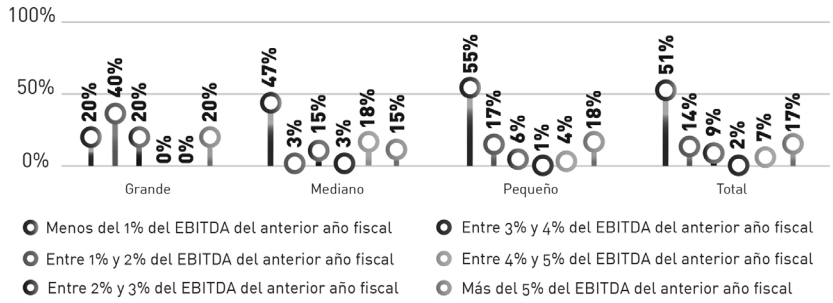
Riesgos cibernéticos que merecen mayor atención por parte de la Entidad / Institución Financiera

	Grande	Mediana	Pequeña	Total
Pérdida / robo de activos de información clasificada (confidencial o sensible)	1,71	2,35	2,64	**2,55**
Secuestro de información	4,71	3,18	2,75	**2,91**
Compromiso de credenciales de usuarios privilegiados	2,29	3,08	3,24	**3,17**
Sabotaje o fraude a través de un insider (personal interno)	2,43	3,04	3,35	**3,25**
Denegación del servicio	4,57	3,80	3,88	**3,88**
Defacement – alteración en sitio web	5,29	5,00	4,66	**4,76**

Nota: 240 registros y los entrevistados priorizaban los riesgos del 1 al 7, siendo el 1 el riesgo más alto y 7 el riesgo más bajo.
Fuente: SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

GRÁFICA 7.

Presupuesto de seguridad de la información (incluyendo ciberseguridad) como % del EBITDA del año inmediato anterior



Nota: 235 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

CUADRO 8.

Estimación del presupuesto y del costo total anual relacionados con la seguridad digital del año inmediato anterior (milones de dólares americanos)

	Presupuesto por sector				Costo por sector			
	Grande	Mediana	Pequeña	Total	Grande	Mediana	Pequeña	Total
Banca Comercial o Múltiple	38	19	11	68	17	9	10	35
Banca de Desarrollo		24	18	43		15	7	22
Sector Bursátil			1	1			1	1
Sector de Ahorro y Crédito Popular (SOCAP)		1	3	4		1	2	3
Sector de Ahorro y Crédito Popular (SOFIPO)		1	0	1		0	0	0
Sector de Intermediarios Financieros No Bancarios			14	14			13	13
Sector FINTECH			26	26			26	26
SISTEMA FINANCIERO MEXICANO	38	45	74	157	17	34	57	107

Fuente: SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

CUADRO 9.

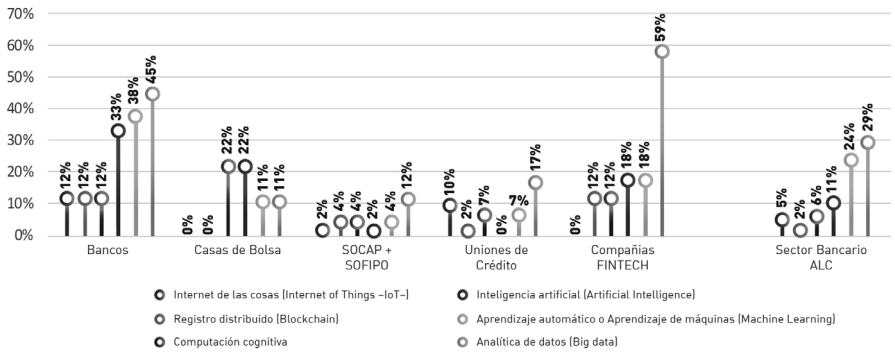
Retorno de inversión (roi) en seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de mediios digitales

	Grande	Mediana	Pequeña	Total
Banca Comercial o Múltiple	15,00%	7,50%	17,50%	**11,56%**
Banca de Desarrollo				
Sector Bursátil			2,50%	**2,50%**
Sector de Ahorro y Crédito Popular (SOCAP)		13,75%	5,00%	**9,38%**
Sector de Ahorro y Crédito Popular (SOFIPO)				
Sector de Intermediarios Financieros No Bancarios			17,50%	**17,50%**
Sector FINTECH			12,50%	**12,50%**
SISTEMA FINANCIERO MEXICANO	**15,00%**	**9,58%**	**10,36%**	**10,94%**

Nota: 19 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

GRÁFICA 8.

Tecnologías digitales emergentes aplicas a herraminetas, controles o processos de seguridad digital en la entidad / institución financiera - Comparacion entre sectores



Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

gulaciones explícitas y marcos o políticas en vigor para el riesgo cibernético. Dentro de este grupo de naciones se encuentran Estados Unidos, el Eurosistema, Hong Kong, México, Reino Unido y República Dominicana, por mencionar algunos (en un intento por plantear el nivel de desarrollo y la geografía).

En cuanto a experiencias nacionales, primero debe señalarse que los aspectos institucionales, legales e idiosincráticos de cada jurisdicción hacen que sea imposible pensar que este tipo de orientación pueda convertirse en un estándar a nivel internacional, aun cuando el NIST o el marco del Banco Central Europeo sí puedan considerarse estándares nacionales (o regional) con amplia aceptación; no obstante, puede reconocerse que la experiencia doméstica de las distintas economías que han avanzado en materia de riesgo cibernético puede arrojar luz sobre acciones y componentes de una estrategia con resultados favorables, o bien sobre, aspectos que pueden mejorarse o adaptarse de cierta forma en otras jurisdicciones.[11]

Países con regulaciones explícitas y marcos o políticas en vigor para el riesgo cibernético

País	*Acciones*
México	Con motivo de un incidente cibernético de escala considerable en una de las principales infraestructuras financieras, se revisaron profundamente las prácticas de gestión del riesgo cibernético y se estableció una estrategia de ciberseguridad encabezada por el Banco de México en coordinación con el Consejo Nacional para la Estabilidad Financiera. Se adopta una postura activa en el manejo del riesgo cibernético, yendo más allá de la seguridad de las redes de comunicación financiera, la seguridad del sistema de información y las amenazas de seguridad cibernética. Adopta un papel preponderante en el seguimiento y control de la seguridad de la información entre las principales infraestructuras y entidades del sistema financiero, incluyendo conceptos tales como: gobernanza, políticas, procedimientos para incidentes (prevención, detección, respuesta y recuperación), concientización y colaboración. Se busca una estrategia centrada en el flujo de información y los canales que atraviesa ésta en el sistema financiero, incluyendo participantes directos y terceras partes. Para ello, se establece, en la regulación, que existan mecanismos de control de seguridad de la información, por ejemplo, acerca de quién y cómo decide sobre los estándares que se van a emplear; además, que se identifique y responsabilice a un equipo o a personas con la autoridad

[11] "Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina", 2019. Disponible en <https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf>, consultado el 18 de enero de 2020.

País	*Acciones*
México	para conducir toda la estrategia y así poder influir dentro de una entidad; y, finalmente, fomentar un equilibrio de prioridades operativas y seguridad dentro de todo el conjunto de medidas de gestión de riesgos para cada entidad. Otra práctica importante es la necesidad de que infraestructuras, entidades o actores relevantes con acceso a la principal red de comunicación financiera interbancaria cuenten con la figura de director de Seguridad de la Información (CISO) y con un equipo de respuesta de seguridad cibernética que además esté coordinado con las autoridades pertinentes, en materia de protocolos de prevención y respuesta.
Hong Kong	En 2017 se lanzó la Iniciativa de Fortalecimiento de la Ciberseguridad (CFI, por sus siglas en inglés), que se fundamenta en tres pilares: un marco general para evaluar la seguridad cibernética, incluidos elementos de examinación de riesgos inherentes, aspectos de madurez y una prueba de simulación de ataque cibernético basada en inteligencia (iCAST); un programa de desarrollo profesional en las entidades que busca aumentar la oferta de profesionales de seguridad cibernética calificados y donde, por ejemplo, entes académicos han logrado desarrollar un esquema de certificación y un programa de capacitación para profesionales de la seguridad cibernética; y, finalmente, una plataforma de intercambio de información, denominada Cyber Intelligence Sharing Platform, que busca proporcionar una infraestructura efectiva para compartir inteligencia acerca de incidentes y donde la coordinación interinstitucional ha sido un aspecto fundamental en los ciberataques, la cual fue establecida por la HKMA junto con la Asociación de Bancos de Hong Kong. Algo que puede destacarse respecto de otros países es el hecho de que en sus prácticas prima la exigencia para todas las entidades bajo el marco de regulación de cumplir con el requisito de integrarse a una red de inteligencia por el bien común del sistema financiero.
Reino Unido	Cuenta con un marco de trabajo conocido como CBEST que se ha apuntalado como un referente internacional guiado por el uso de inteligencia, que se centra en validar la vulnerabilidad y capacidad de recuperación del riesgo cibernético de una entidad o infraestructura, todo ello adoptando una postura en la que los objetivos probables y métodos de ataque son el principal elemento de análisis y seguimiento. Este marco es conducido por el banco central de ese país y cuenta con elementos adicionales que fortalecen su imagen como referencia a nivel internacional, especialmente en materia de evaluación de capacidades de detección y respuesta que permiten establecer si los niveles de seguridad cibernética de las entidades, infraestructuras y agentes son proporcionales a los riesgos cibernéticos que enfrenta.
República Dominicana	En 2018 se emitió el Programa de Seguridad Cibernética y de la Información que el banco central y la agencia de supervisión financiera de ese país emplean como principal herramienta de trabajo para fomentar controles, políticas y medidas más rigurosas de control del riesgo cibernético, con un foco en la integridad y disponibilidad de información y servicios críticos para el sistema financiero. Este marco de trabajo es un enfoque mucho más tradicional en el que las entidades financieras están encargadas de asegurar una estructura de gobierno y medidas que les permitan ser acreditadas en el Programa (nacional) de

País	*Acciones*
República Dominicana	Seguridad Cibernética, que pone especial énfasis en la criticidad de las infraestructuras de mercado, particularmente en el principal sistema interbancario de transferencia de fondos. Parte de este énfasis tiene que ver con la interconexión dentro del sistema financiero como una de las principales fuentes del riesgo tecnológico. Del mismo modo, el Programa busca que los aspectos de cultura institucional y la gestión de riesgos con terceras partes tenga un valor importante dentro de todas las medidas que puedan adoptar las entidades sujetas a cumplir con esta normativa.
Eurosistema	El Banco Central Europeo ha desarrollado un marco de trabajo enfocado en garantizar la protección, disponibilidad e integridad de la información en el sistema inanciero, particularmente de las economías que lo componen. Gracias a que el BCE responde a la necesidad de tener una arquitectura financiera regional, los esfuerzos y la vinculación normativa que se han emprendido recientemente contribuyen a que las potenciales consecuencias y efectos del riesgo cibernético se mitiguen. El marco de trabajo del BCE en cuestiones cibernéticas tiene tres componentes: Plan de acción sobre resiliencia cibernética para infraestructuras de mercado (APCR), expectativas de supervisión sobre resiliencia cibernética (CROE) e iniciativa de *hacking* ético basada en inteligencia de amenazas (TIBER-UE). Estos tres pilares son la base para la estrategia contra ataques dentro de los bancos centrales nacionales de Europa, y que se extienden al sistema financiero de esa región. Se puede destacar que, para la implementación del APCR, el BCE contó con un órgano de gobierno, denominado Consejo de Infraestructuras Financieras, para poner en funcionamiento dicho plan en 2017. La importancia del APCR radica en el grado de coordinación que se alcanzó con su lanzamiento, poniendo atención especial a aspectos de gobernanza y organizacionales, con tal de asegurar que las medidas de detección, prevención, respuesta y recuperación estuvieran plenamente identificadas, soportadas y cubiertas por los países miembros del Eurosistema. Asimismo, el APCR es constantemente actualizado por el BCE, con miras a permanecer vigente como la principal línea de defensa contra el crimen cibernético, por ejemplo, promoviendo la mejora de las actividades de monitoreo y registro de incidentes en la principal infraestructura tecnológica, así como reforzando las actividades de prueba de los controles de seguridad, como es el caso de la formación y el funcionamiento de equipos rojos (para ejercicios de penetración y pruebas basadas en escenarios). En 2019, se estaba trabajando para emitir directrices sobre la gestión del riesgo cibernético, dentro de las propias entidades financieras. La colaboración que existe entre el Parlamento Europeo, el Consejo, la Comisión Europea y el BCE ha permitido poner en funcionamiento un Equipo de Respuesta a Emergencias Informáticas (CERT-UE) que sirve de mecanismo de alerta para quienes son miembros de este equipo acerca de nuevas amenazas.

Fuente: elaboración propia con base en "Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina, disponible en <https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf>.

Cooperación internacional

Organismo	*Acciones*
G7	En 2016 se promulgó un conjunto de recomendaciones no vinculantes para tratar de aglomerar aspectos clave para el establecimiento de un marco único de prácticas de ciberseguridad para entidades privadas y públicas del sector financiero. A la par, el CEG del G7 continuó trabajando en el desarrollo de un marco de evaluación de estas recomendaciones y en identificar los riesgos cibernéticos a partir de la mayor presencia de terceras partes, así como en promover una mayor coordinación intersectorial. En 2018, el CEG publicó lineamientos para promover la seguridad cibernética en terceras partes y un conjunto de lineamientos para pruebas de penetración basadas en amenazas. Si bien, ninguna de estas recomendaciones tiene carácter vinculante, han sentado un importante antecedente a nivel de las principales economías avanzadas para promover mayores esfuerzos y herramientas de convergencia hacia un marco apropiado de atención del riesgo cibernético, tanto en el sistema financiero como entre instituciones oficiales y autoridades financieras.
Financial Stability Board (FSB)	En octubre de 2017, divulgó un informe que revisa las prácticas y normativa de ciberseguridad en los países miembros del G20 con el fin de identificar aspectos que pueden resultar clave en materia de cooperación transfronteriza. De acuerdo con este informe, 75 por ciento de países considerados en el estudio está tomando como referencia el Guidance on Cyber Resilience for Financial Market Infrastructures publicado por el Comité de Pagos e Infraestructuras de Mercado y la Organización Internacional de Comisiones de Valores en 2016; 68 por ciento de los países están certificándose con el estándar ISO/IEC 27000, adoptando con ello directrices para la gestión de riesgos informáticos y la constitución de un Sistema de Gestión de Seguridad de la Información; un porcentaje muy similar está tomando como punto de partida el marco del NIST que surgió en 2014 en Estados Unidos y que estaba originalmente pensado para infraestructuras críticas, pero que, al ofrecer un enfoque integral, distintas entidades y organizaciones lo han visto como una herramienta útil para mejorar su capacidad de prevenir, detectar y responder a los ciberataques. El FSB creó un glosario de términos asociados con la seguridad cibernética, en el que se incluyen más de 50 términos de uso cada vez más común entre las autoridades financieras y las entidades del sistema financiero a nivel doméstico e internacional. El glosario, o Cyber Lexicon, busca armonizar el trabajo y los esfuerzos para abordar el riesgo cibernético. Otra vía con la que el FSB ha continuado sus esfuerzos de coordinación internacional son los grupos consultivos regionales; actualmente, el FSB cuenta con seis, incluido uno para América, con los que busca ampliar su ámbito de divulgación y aplicación más allá del G20; de esta forma, también ha promovido una mayor concientización y necesidad de mecanismos más formales de cooperación a nivel mundial en materia de seguridad cibernética.

Organismo	*Acciones*
Comité de Pagos e Infraestructuras de Mercado (CPMI)	En 2016 publicó una guía para el fortalecimiento de la seguridad cibernética dentro de las principales infraestructuras del mercado financiero, incluidos los sistemas de pago de importancia sistémica. La guía también es pertinente para las autoridades de regulación y supervisión financiera en el desempeño de sus responsabilidades microprudenciales. En general, la guía se propone como una orientación para que todas las autoridades financieras relevantes promuevan su uso de acuerdo con las leyes y regulaciones aplicables en cada país, reconociendo que es importante adaptarla según el marco institucional existente. El enfoque propuesto por el CPMI ha sido adoptado por sus 27 miembros, y a través de un ámbito de cooperación internacional, como el que promueven instituciones como el CEMLA en América Latina y el Caribe, el SEACEN en Asia o el Banco Central Europeo en Europa, también ha sido posible ampliar su adopción.
Banco Central Europeo (BCE)	Ha desarrollado un marco de trabajo enfocado en garantizar la protección, disponibilidad e integridad de la información en el sistema financiero, particularmente de las economías que lo componen. Gracias a que el BCE responde a la necesidad de tener una arquitectura financiera regional, en este caso para el Eurosistema, los esfuerzos y la vinculación normativa que se han emprendido recientemente contribuyen a que las potenciales consecuencias y efectos del riesgo cibernético se mitiguen. El marco de trabajo del BCE en cuestiones cibernéticas puede desagregarse en tres componentes: Plan de acción sobre resiliencia cibernética para infraestructuras de mercado (APCR), expectativas de supervisión sobre resiliencia cibernética (CROE) e iniciativa de *hacking* ético basada en inteligencia de amenazas (TIBER-UE). Estos tres pilares son la base para la estrategia contra ataques dentro de los bancos centrales nacionales de Europa, y que se extienden al sistema financiero de esa región.
Grupo de Trabajo de Resiliencia Operativa del Comité de Supervisión Bancaria de Basilea (BCBS)	En 2018 reconoció la importancia de estudiar el estado de la resiliencia operativa, más allá del alcance de la gestión del riesgo operacional y del riesgo cibernético; para ello, estableció el Grupo de Trabajo de Resiliencia Operacional, buscando contribuir con otros esfuerzos de carácter internacional al tratamiento de este fenómeno en una escala transfronteriza y coordinada. Adicionalmente, como parte de su proceso de reforma poscrisis, en 2016 presentó una revisión, "Principios para la Gestión del Riesgo Operacional", que se enfocó en incorporar aspectos y lecciones de la CFG, incluidas algunas cuestiones asociadas con el riesgo cibernético. Estos Principios establecen expectativas comunes que son de aplicación a entidades financieras de importancia sistémica, pero, dado el papel que el BCBS tiene a nivel de regulación financiera internacional, constituyen un referente más para orientar la implementación de políticas, procedimientos y prácticas para administrar el riesgo operacional y cibernético.

Fuente: elaboración propia con base en "Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina, disponible en <https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf>.

Ante la amenaza que representa el riesgo cibernético, es importante aprovechar los recursos y la experiencia que se tiene e irlos adaptando de acuerdo con las circunstancias, es decir, conforme la evolución tecnológica, en el marco de una arquitectura financiera que, desde la crisis de 2008, se reconfigura constantemente. Algunos de los trabajos que ya son referencia para el establecimiento de políticas públicas corresponden a entidades nacionales, así como a organizaciones internacionales. En la siguiente lista puede apreciarse la fecha de cada uno de los documentos, lo que demuestra el interés, ya sin tregua, y la importancia que tiene el tema en prácticamente todo el mundo.

- **Banco de México.** Estrategia de Ciberseguridad del Banco de México. Octubre de 2018.
- **Bank of England.** CBEST framework. Junio de 2013.
- **Basel Committee on Banking Supervision.** Cyber-resilience: range of practices. Diciembre de 2018.
- **Committee on Payments and Market Infrastructures and International Organization of Securities Commissions**. Guidance on cyber resilience for financial market infrastructures. Junio de 2016.
- **Committee on Payments and Market Infrastructures.** Reducing the risk of wholesale payments fraud related to endpoint security. Mayo de 2018.
- **European Central Bank.** TIBER-EU framework. Mayo de 2018.
- **European Central Bank.** Cyber resilience oversight expectations for financial market infrastructures. Diciembre de 2018.
- **Financial Stability Board**. FSB 2017 workplan. Noviembre de 2016.
- **Financial Stability Board.** Financial stability implications from fintech: supervisory and regulatory issues that merit authorities' attention. Junio de 2017.
- **Financial Stability Board.** Cyber Lexicon. Noviembre de 2018.
- **Financial Stability Institute.** Regulatory approaches to enhance banks' cyber-security frameworks. Agosto de 2017.
- **G-7**. Fundamental Elements of Cybersecurity for the Financial Sector. Octubre de 2016.
- **G-7.** Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector. Octubre de 2017.
- **Hong Kong Monetary Authority.** Cybersecurity Fortification Initiative, Mayo de 2016.
- **Superintendencia de Bancos**. Reglamento de seguridad cibernética de la información. Noviembre 2018.

La evolución de los riesgos de ciberseguridad requiere talento e intercambio de información para enfrentar este nuevo ecosistema digital que permita empoderar el negocio e innovar, a la vez que fomentar la seguridad bajo una nueva visión.

8. Tecnología, ¿y después qué…?

La innovación tecnológica no se detendrá; la transformación digital quedará como un tópico del que se desprenderán acciones, estrategias e innovaciones; en suma, nuevas realidades que se irán adaptando en un entorno que para algunos será complejo, mientras que para otros será facilitador. Y sin importar cuál sea la óptica, los escenarios nacientes implicarán retos que requerirán

entender experiencias pasadas, sacarles provecho y mirar hacia delante.

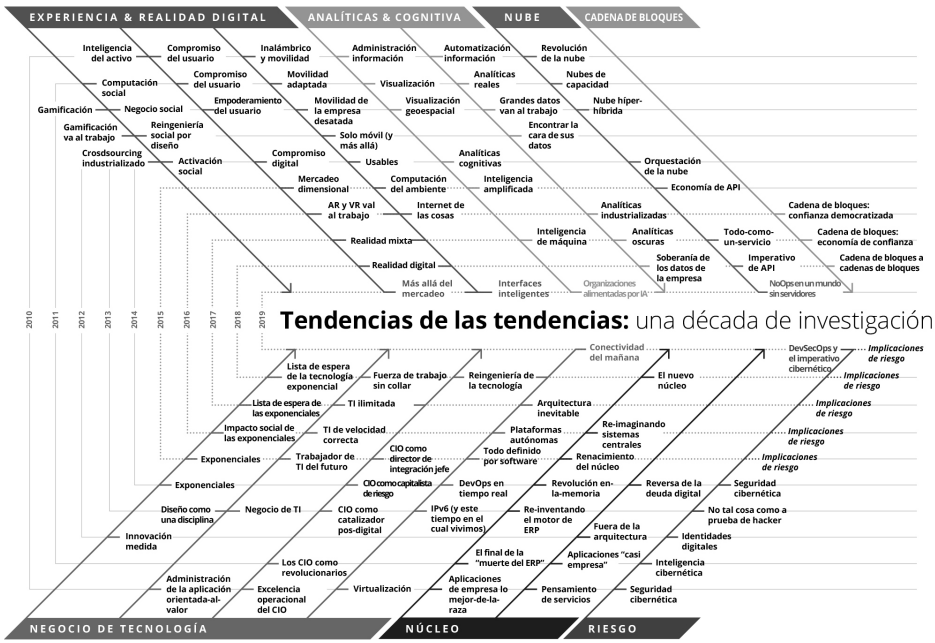
La tecnología de la que hoy echamos mano irá evolucionando o dará paso a otra que responda a las nuevas necesidades, o que al presentarse cree nuevas necesidades, como ha sido el caso con muchas de las innovaciones que han colocado al cliente en un lugar que antaño ni se pensaba.

En los años setenta del siglo pasado comenzaba la carrera tecnológica; una innovación llevaba a otra hasta cambiar por completo las estructuras y las fachadas. Lo que podemos decir y ver 50 años después es que la tecnología con la que contamos actualmente tiene potenciales aplicaciones en el sector financiero, y las tendencias derivadas de éstas esperamos utilizarlas en el corto plazo.

Desde nuestra óptica, y considerando la adopción tecnológica actual, así como las perspectivas que plantean, las principales tecnologías que representarán una disrupción en el sector financiero durante los próximos años son: *blockchain*, big data, *internet of things* e inteligencia artificial.

Sin la intención de ser exhaustivos, y para efectos de este trabajo, en este apartado mencionaremos las generalidades de estas cuatro tecnologías. La intención es que, con las características generales de estas tecnologías, el lector pueda inferir cómo podría cambiar la relación con el cliente, el enfoque de riesgos y el marco regulatorio en el que se moverían todos los participantes.

GRÁFICO 1.



Fuente: "Tendencias tecnológicas 2019. Más allá de la frontera digital", Deloitte, enero de 2019, disponible en <https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/technology/Tendencias_tecnologicas_2019%20(Reporte%20Completo).pdf>.

Blockchain inicia la revolución

La cadena de bloques ya se usa en procesos o actividades que van más allá de las operaciones con criptomonedas, su origen; sectores como el financiero, logística, seguros, el área legal y hasta la gestión de información en el ámbito público la están empleando.

Don Tapscott y Alex Tapscott[12] señalan que los grandes bancos y algunos gobiernos están usando cadenas de bloques a modo de registros distribuidos (Distributed Ledger Technology, DLT) con la idea de revolucionar la manera de almacenar información y realizar transacciones. "Sus aspiraciones son loables: mayor velocidad, menores costos, más seguridad, menos errores y eliminación de puntos centrales que puedan atacarse o fallar".

Las entidades financieras son conscientes de esta nueva realidad. Así, al menos, se desprende de encuestas como la elaborada por la consultora Bain & Company, en la que 80 por ciento de los ejecutivos financieros auguraba que *blockchain* será una tecnología transformadora, con un impacto considerable en los mercados, y un porcentaje similar esperaba que su entidad empezará a usarla antes de 2020.

Para D. Tapscott y A. Tapscott (2017), la tecnología *blockchain* tiene profundas implicaciones en muchas instituciones. Esto explica el entusiasmo que ha despertado en muchas personas listas e influyentes. Los autores citan a *The Economist,* medio que en octubre de 2015 publicaba un reportaje titulado "La máquina fiable", en el que se decía que "la tecnología en la que se basa bitcoin podría cambiar el funcionamiento de la economía", porque, para *The Economist*, la tecnología *blockchain* es "el mejor modo de estar seguro de las cosas".

Significado y proceso

Blockchain significa "cadena de bloques". Es la tecnología o el sistema de codificación de la información que está detrás de la moneda virtual bitcoin y que sustenta toda su estructura. Su potencial y la cantidad de aplicaciones que permite en otras áreas, más allá de las transacciones financieras, se vieron casi de inmediato. Ya tiene más de 10 años de vida y su presencia es significativa no sólo en empresas pequeñas y/o *startups*, según la consultora británica Elwood.[13]

Ejemplo de ello, cita Elwood, es el caso de IBM, que lanzó su plataforma de *blockchain* en marzo de 2017 y ya está generando ingresos con varias soluciones basadas en esta tecnología; además, "la misma TradeLens —utilizada por Maersk para identificar ineficiencias en las cadenas globales de suministro— y Food Trust, usada por Carrefour y Walmart en el ámbito de la seguridad alimentaria".

Don Tapscott, fundador del Blockchain Research Institute (BRI), con sede en Canadá, considera que *blockchain* es una arquitectura distribuida que utiliza criptografía y un concepto de "escribe un registro una sola vez", que brinda un valor enorme a los casos de uso que se requieren como parte de las transformaciones digitales para mejorar la validación de algunos de esos datos sin alterar las bases de datos existentes, las cuales cumplen con varios requerimientos.

[12] Don Tapscott y Alex Tapscotta, *La revolución blockchain*, Ediciones Deusto, 2017.

[13] "El sector financiero lidera el uso del blockchain", disponible en <https://www.fundssociety.com/es/noticias/etf/el-sector-financiero-lidera-el-uso-del-blockchain>.

Pero, además, contribuye con una tremenda novedad: esta transferencia no requiere de un intermediario centralizado que identifique y certifique la información, sino que está distribuida en múltiples nodos independientes entre sí que la registran y la validan sin necesidad de que haya confianza entre ellos. Una vez introducida, la información no puede ser borrada, sólo podrán añadirse nuevos registros, y no será legitimada, a menos que la mayoría de ellos se pongan de acuerdo para hacerlo.

Junto al grado de seguridad que proporciona este sistema frente a hackeos, existe otra ventaja: aunque la red se cayera, con que sólo uno de esas computadoras o nodos no lo hiciera, la información nunca se perdería o el servicio seguiría funcionando.

Cada bloque de la cadena porta el paquete de transacciones y dos códigos, uno que indica cuál es el bloque que lo precede (excepto el bloque origen) y otro para el bloque que le sigue, es decir que están entrelazados o encadenados, por lo que se llaman códigos o apuntadores *hash*.

También hay un proceso de validación de la información. En este proceso de minado o comprobación, cuando hay dos bloques que apuntan al mismo bloque previo, sencillamente gana el primero en ser desencriptado por la mayoría de los nodos, es decir que la mayoría de los puntos de la red deben ponerse de acuerdo para validar la información. Por eso, aunque *blockchain* genera múltiples cadenas de bloques, siempre será legitimada la cadena de bloques más larga.

Los expertos comparan la llegada del *blockchain* con hitos como la integración de las computadoras en el uso doméstico o el desarrollo de internet, es decir, un sistema que cambiará nuestra forma de entender los negocios y la sociedad.

D. Tapscott (2017) sitúa en este nuevo sistema a la confianza, la cual, dice, consiste en esperar que la otra parte se comporte de acuerdo con los cuatro principios de la integridad: honradez, consideración, responsabilidad y transparencia.

> Para ser claros, digamos que la confianza se refiere a la compraventa de bienes y servicios, así como a la integridad y protección de la información […] un registro global de información fidedigna puede contribuir a que nuestras instituciones sean más íntegras y el mundo más seguro y fiable. En nuestra opinión, las empresas que realicen parte de sus operaciones o todas ellas en el sistema *blockchain* verán aumentar rápidamente su cotización. Accionistas y ciudadanos querrán que todas las empresas y organismos públicos gestionen sus fondos, como mínimo, en el sistema *blockchain* […]. Describimos a *blockchain* como un protocolo de confianza, debido a que es descentralizado, seguro e inmutable; la confianza está integrada en la red.

El BRI realiza estudios sobre el impacto de la tecnología *blockchain* en los negocios, el gobierno y la sociedad; en 2017 contaba con más de 70 proyectos dedicados a explorar, comprender, documentar e informar a los líderes sobre las estrategias *blockchain*, las oportunidades de mercado y los desafíos de implementación. La investigación es financiada por sus miembros, entre los que se incluyen grandes corporaciones y gobiernos de todo el mundo, como IBM, Microsoft, KPMG, Fedex, Pepsico, SAP, Capgemini, Deloitte, Accenture y Thomson Reuters, entre otros.

Del internet de la información al internet del valor

Alex Preukschat[14] considera que con la cadena de bloques habrá muchos más operadores y que el poder no va a estar tan centralizado. "Eso cambia la operativa de las empresas, pero también la de las personas, cómo interactuamos entre nosotros. Y esto es realmente fascinante, tratar de imaginar cómo va a ser el futuro en 20, 30 o 40 años. Y *blockchain* va a ser uno de los principales agentes de ese cambio".

Blockchain, dicen los expertos, va a posibilitar dar el salto del llamado internet de la información al internet del valor. "Se le llama internet de la información porque hasta ahora lo que se ha compartido ha sido fundamentalmente información, pero ya se compartirá valor y esta ola es mucho mayor que la primera, por lo que no puede descartarse que empresas disruptivas como Amazon o Ebay se vean disrumpidas a su vez", sentencia Preukschat.

En noviembre de 2018, Amazon publicó en la página <https://aws.amazon.com/es/about-aws/whats-new/2018/11/introducing-amazon-managed-blockchain/> la siguiente nota, una presentación de sus servicios basados en *blockchain*:

> Amazon Managed Blockchain es un servicio completamente administrado que le permite configurar y administrar una red de cadenas de bloques escalable con unos pocos clics. Con Amazon Managed Blockchain se elimina la sobrecarga que implica la creación de la red. Además, el servicio ajusta su escala automáticamente para satisfacer las demandas de miles de aplicaciones que ejecutan millones de transacciones. Una vez que su red esté funcionando, se facilitará la tarea de administrar y mantener su red de cadenas de bloques con Managed Blockchain. El servicio administra sus certificados, le permite invitar de forma sencilla a nuevos miembros para que se unan a la red y, además, realiza un seguimiento de las métricas operacionales como, por ejemplo, el uso de recursos informáticos, de memoria y almacenamiento. Además, Managed Blockchain puede repetir una copia inmutable de su actividad de red de cadenas de bloques a Amazon Quantum Ledger Database (QLDB), una base de datos de libro mayor completamente administrada. Esta repetición le permite analizar fácilmente la actividad de la red de manera externa y obtener información acerca de las tendencias.

Preukschat (2017) apunta que la principal diferencia entre *blockchain* e internet es que mientras la segunda se limita al intercambio de información, la cadena de bloques permite intercambiar valor.

Blockchain es mucho más que una alternativa al dinero: es una infraestructura que permite construir sobre internet y crear otra capa sobre la que las personas van a poder intercambiar valor entre ellas. Eso afecta a todos los sectores: ya tocó a la banca, pero va a afectar también al sector de las energías, a las telecomunicaciones, a las cadenas de valor de logística, etcétera (Preukschat, 2017).

Para Julio Faura,[15] si esta tecnología llega a ser efectivamente adoptada por la mayoría de la industria, o por toda la industria, entonces sí que es cierto que puede llegar a te-

[14] Alex Preukschat, *Blockchain, la revolución industrial de Internet*, Gestión 2000/Grupo Planeta, 2017.

[15] Julio Faura, responsable de *blockchain* de Banco Santander España, citado en <https://retina.elpais.com/retina/2017/03/30/tendencias/1490871615_134683.html>.

ner el potencial de reconfigurar realmente la manera como funcionan los modelos de negocio; no sólo de la banca, sino del mundo en general. "Quienes ya se han introducido en la cadena de bloques dicen que ésta constituye una oportunidad más que un riesgo".

En el libro *Blockchain, la revolución industrial de internet* (Preukschat, 2017), los autores presentan la aportación de la cadena de bloques en diferentes sectores:

Quién	*Sector*	*Aportación blockchain*
Daniel Díez, responsable de *blockchain* en Everis.	Banca y seguros	Habilita la aparición de un nuevo internet del valor en el cual la interoperabilidad, descentralización, liquidez de experiencias de usuario e innovación abierta cambiarán la forma en la que se relacionan las empresas y los clientes, redefiniendo la propia naturaleza de las compañías y sus actuales modelos de negocio. Es factible porque *blockchain* es el primer sistema construido de forma nativa sobre el consenso y contabilidad distribuidos, la integridad de la información y la gestión segura de identidades.
Gonzalo Gómez, responsable de estrategia de negocio digital y servicios financieros de informática en El Corte Inglés.		En el sector bancario nos va a permitir optimizar los procesos actuales y reconfigurar completamente, no sólo dichos procesos o la experiencia de usuario, sino también la propia naturaleza de las entidades financieras, con nuevos modelos de negocio e involucrando a actores ajenos al sector. El sector asegurador se encuentra algo menos maduro tecnológicamente hablando, pese a ser uno de los que mayor potencial de implantación tiene en áreas como automatización de pagos, certificación de procesos y garantía de integridad de la información, interoperabilidad, identidad digital y ciberseguridad o en la simplificación de contratación y ejecución de pólizas de reaseguro.
Roberto Fernández, responsable de nuevos negocios digitales en Everis.	Sector público	Refleja los valores cien por ciento digitales: empatía, simplicidad, persona a persona, transparencia y horizontalidad. Los ciudadanos demandan un nuevo modelo de administración pública: más transparente, más rápida, más eficiente y más integrada en la vida diaria de la ciudadanía. Quieren participar en aquello que les interesa y *blockchain* es el elemento clave para la generación de este nuevo modelo de administración.
Íñigo Molero, consultor de comunicación.	ONG	Brinda al tercer sector una oportunidad tan extraordinaria como única para optimizar prácticamente todos sus procedimientos actuales e inaugurar nuevos escenarios de confianza y transparencia.

Quién	*Sector*	*Aportación blockchain*
Christoph Steck, director de políticas públicas e internet en Telefónica.	Telecomunicaciones	Permitirá el proceso más rápido y rentable para conectar a usuarios finales, operadores móviles y proveedores de servicios, descentralizando de manera efectiva la industria.
Óscar Lage, responsable de Ciberseguridad en Tecnalia.	Industria 4.0	La Industria 4.0 es uno de los ámbitos en los que *blockchain* puede suponer una mayor revolución, ya que permitirá la automatización de los procesos y las relaciones industriales entre todos los actores, habilitando la fabricación de series cortas e incluso unitarias en los mismos rangos de precios que la actual fabricación en grandes lotes.
Óscar Lage, responsable de Ciberseguridad en Tecnalia.	Voto *online*	Uno de los mayores frenos de la digitalización de los procesos de participación y votación *online* es la desconfianza en la privacidad y auditabilidad de las actuales tecnologías, por lo que *blockchain* se postula como la tecnología para poner fin a estos temores.

Lo ya cuantificable

Carlos Kuchkovsky[16] afirma que estamos evolucionando del internet de la comunicación a un nuevo internet para la cooperación y colaboración. Nos encontramos en el comienzo y aún nos quedan grandes retos que resolver y en los cuales trabajar juntos, pero la potencia de impacto en la sociedad es enorme.

> El sector financiero ha sido el primero en crear consorcios para explorar oportunidades con *blockchain*. La coyuntura de generar eficiencias para poder realizar pagos internacionales en tiempo real, en lugar de en tres días, y la posibilidad de ofrecer sistemas de alta calidad a nuevos clientes de manera más segura y fácil son dos de los grandes ejemplos en los que varios bancos estamos trabajando en común. Por otro lado, la posibilidad de generar nuevos modelos de negocio y de poder cubrir las necesidades de interacción de persona a persona o entre colectivos de manera diferente es otra de las grandes oportunidades que brinda esta tecnología.

Se estima que la cadena de bloques hará posible una de cada cinco transacciones globales en 2020 y será la estrategia financiera de 60 por ciento de los bancos. Por ejemplo, en 2018, BBVA realizó una transacción comercial entre España y México, a través de la tecnología *blockchain*. Otros, como Santander, ya han adoptado esta herramienta en ciertos países. El Banco de Pagos Internacionales ha referido (2018) que 63 bancos centrales ya están trabajando o experimentando con esta tecnología, por lo que una vez que

[16] Carlos Kuchkovsky, *Chief technology officer* de nuevos negocios digitales de BBVA y autor del capítulo sobre la utilización de *blockchain* en el futuro, citado en <https://retina.elpais.com/retina/2017/03/30/tendencias/1490871615_134683.html>.

éstos la adopten, la banca comercial tendrá que hacerlo también.

A continuación, veremos cuáles son las funciones potenciales y las más importantes para las que se está planteando la utilización del *blockchain*, así como las dificultades y barreras que hay que tener en cuenta para su aplicación. Según autores como A. Tapscott y D. Tapscott (2017) o H. Peter y A. Moser (2017), la tecnología de registros distribuidos (DLT) puede tener un gran impacto en funciones como:

- Correcta identificación de las partes.
- Traspasos de valor (sistemas de pagos) y titulización.
- Ahorro, financiamiento y crédito.
- Movimientos de capital (mercados financieros).
- Aseguramiento y gestión del riesgo.
- Funciones de auditoría y control fiscal.
- Liquidación postransacciones.
- Custodia de valores.
- Emisiones de deuda o títulos en mercados primarios.
- *Reporting* automatizado.
- Seguimiento de la propiedad de activos.

Disrupción en la disrupción

Blockchain, la tecnología que está detrás de Bitcoin, ha llegado para quedarse. Su característica es su capacidad para descentralizar la confianza, una cualidad que permite eliminar los intermediarios en muchos procesos y servicios empresariales y que da lugar a nuevos modelos de negocio basados en la desintermediación y la colaboración.

La Alianza Blockchain Iberoamérica, Blockchain Summit Latam y la ONG Bitcoin Argentina presentaron el "Radar sobre el ecosistema *blockchain* latinoamericano", donde se observa que Argentina es líder con 22 empresas de este tipo y México está en segundo sitio con 21.

Después están, con crecimientos importantes, Chile y Colombia. Y más abajo se encuentran Perú, Uruguay, Costa Rica y Venezuela. De acuerdo con este reporte, fue en 2017 y 2018 cuando se dio el crecimiento más importante de empresas de *blockchain* en la región, las cuales tienen la siguiente distribución: 25 por ciento, servicios y software empresarial; 20 por ciento, servicios financieros; 15 por ciento, educación; 10 por ciento, medios, y 5.8 por ciento, otros servicios.

La naturaleza del propio bitcoin, así como la de la DLT en la que se basa y su capacidad de transacción directamente entre las partes implicadas, ha hecho que muchas personas pongan en el centro del sector financiero a esta tecnología. Si bien, aunque es posible que *blockchain* se integre en el sistema de pagos internacional, existen todavía muchas barreras para su aplicación, como establecer criterios para determinar quién podrá acceder a una cadena de bloques o cómo se integrarían los nuevos sistemas de manejo del riesgo con una regulación.

Inteligencia artificial

La inteligencia artificial (IA) trata de explicar el funcionamiento mental basándose en el desarrollo de algoritmos para controlar diferentes cosas; es considerada una rama de la computación donde se relaciona un fenómeno natural con una analogía artificial a través de programas informáticos. La IA combina varios campos, como la robótica; ambas tienen un mismo objetivo: tratar de crear máquinas que puedan pensar por sí solas, lo que origina que hasta la fecha existan varios estudios y aplicaciones, dentro de las que se encuentran las redes neuronales, el control de procesos o los algoritmos genéticos.

Se cree que los comienzos de la IA ocurrieron en 1943 al definirse la neurona como un dispositivo binario con varias entradas y salidas. En 1956 se volvió a tocar el tema y se establecieron las bases de la IA como un campo independiente dentro de la informática.

Hoy en día entendemos la inteligencia artificial como un sistema capaz de resolver complejos problemas de análisis, que funciona sobre una computadora o una máquina. Tiene la habilidad de recordar, entender y reconocer patrones; tomar decisiones, adaptarse al cambio y aprender del entendimiento. Tiene una codificación que hace que su comportamiento funcione bajo un orden lógico similar al de las neuronas y está consiguiendo que computadoras y máquinas que soportan estos sistemas tengan un comportamiento similar al humano.

La inteligencia artificial posee dos componentes básicos: automatización e inteligencia. Entendemos esta inteligencia como la capacidad de percibir, analizar y reaccionar a determinados patrones. Dos características relevantes de la IA son el análisis predictivo, entendido como la capacidad de generar *outputs* de forma autónoma y predictiva, gracias al análisis de eventos pasados y presentes, y sistemas de recomendación, derivados de la capacidad de análisis anterior.

La IA tiene numerosas aplicaciones potenciales. Según Hussain[17] y Marous,[18] son:

- Análisis algorítmico en mercados bursátiles.
- Intercambios de información bursátil.
- Estudios de mercado.
- Recopilación de datos.
- Gestión de carteras de activos.
- En el *back office* de las entidades: automatización y mejora de procesos, por ejemplo, resolución de consultas de los empleados o recopilación y *reporting* de datos.
- En el *front office*: mejora de la interacción con clientes mediante sistemas de atención al cliente basados en IA, sistemas de asesoramiento o promoción comercial.
- Establecimiento de precios.
- Vinculación de clientes y personalización del marketing.

Lo anterior es posible porque la IA es:

- Es programática: La inteligencia artificial o el *robotic process automation* (automatización robótica de procesos, RPA, por sus siglas en inglés) tiene la capacidad de ofrecer soluciones a tareas repetitivas, relativamente sencillas y que, por ende, e pueden automatizarse, ahorrando de esta manera tiempo y costos.
- Es cognitiva: Las cualidades de aprendizaje y análisis que hemos mencionado anteriormente hacen que la inteligencia artificial permita crear y escoger productos y servicios individualizados para cada cliente y, por lo tanto, aportar valor en la oferta.

En 2017 se estimó que la industria general de IA crecería a un ritmo de 50 por ciento anual en los siguientes 10 años. Doug Fitz[19] señala

[17] K. Hussain (2018), "Artificial intelligence and its applications goal", *International research journal of engineering and technology* (*IRJET*), vol. 5, t. 1, enero, pp. 838-841, disponible en <https://irjet.net/archives/v5/i1/irjet-v5i1180.pdf>.

[18] J. Marous (2018), "The 'year of ai and machine learning' for financial marketers", *Thefinancialbrand.com*, disponible en <https://thefinancialbrand.com/69686/ai-machinelearning-banking-marketing-martech-data-trends/>.

[19] Fundador de la consultoría F2 Strategy.

que en un futuro próximo los equipos de control de riesgos y cumplimiento normativos se verán muy favorecidos por la aplicación de la inteligencia artificial, debido a que desarrollará la capacidad de detectar patrones de riesgo y fraude que históricamente han sido imposibles de detectar por las capacidades humanas.

Según Marous (2018), en un futuro esta tecnología se usará de forma más exhaustiva para la planificación mediática y la personalización del marketing, gracias a las herramientas de analítica de datos comportamentales. Por otro lado, expone que la creciente accesibilidad a las grandes bases de datos y el menor costo de las capacidades de análisis de éstas harán de la IA una herramienta fundamental y necesaria para el sector financiero, por lo que prevé un continuo desarrollo de ésta en el corto plazo. En conclusión, IA es una de las tecnologías con mayor potencial en el sector financiero, especialmente en el ámbito del marketing, la experiencia del cliente, el cumplimiento normativo y el control de riesgos.

Blockchain / *IA*

Complementarias y sinérgicas

Santiago Franco, socio responsable de tecnología en el área de Consulting de PwC España, define a la IA y a blockchain como el yin y el yang de la tecnología, porque mientras la IA nos ayuda a valorar, comprender, reconocer y decidir, blockchain nos ayuda a verificar, ejecutar y registrar. "Mientras los métodos de aprendizaje automático que forman parte de la inteligencia artificial nos ayudan a encontrar oportunidades y a mejorar la toma de decisiones, los smart contracts y las tecnologías blockchain pueden automatizar la verificación de las partes transaccionales del proceso".

(Smart contracts o contratos inteligentes son un desarrollo que permite firmar acuerdos que se ejecutan automáticamente en el momento en que se produzca una de las condiciones predeterminadas, sin necesidad de intermediarios que verifiquen su veracidad y cumplimiento).

"La IA y la tecnología blockchain son complementarias y sinérgicas. Son dos extremos del abanico de potentes tecnologías emergentes que hemos incluido entre las ocho tecnologías esenciales para las empresas. La IA añade inteligencia e información a los procesos de toma de decisiones. Blockchain proporciona integridad, seguridad y descentraliza el entorno en el que tienen lugar las transacciones, lo que puede contribuir enormemente a la mejora de los procesos". Lo anterior plantea una diferenciación útil:

IA	*Blockchain*
El reto es conseguir que las máquinas sean capaces de realizar conjeturas, a una escala y con un nivel de precisión que nosotros como humanos no podemos alcanzar. Las máquinas "aprenden" mientras procesan datos especialmente diseñados y recogidos para su formación. La inteligencia artificial se basa en el método probabilístico, según el cual máquinas se orientan hacia lo que perciben como la realidad más probable. Y esta realidad cambia constantemente.	Se centra en la validación, permanencia y en conseguir mayores niveles de certeza y control. Como resolviendo un rompecabezas bloque por bloque, una cadena de transacciones queda encriptada y guardada de manera que no puede alterarse.

IA	*Blockchain*
Conduce al descubrimiento de oportunidades y a la evaluación de riesgos.	Entra en acción en el momento de ejecutar el plan, por lo que, al igual que los smart contracts, debe ser, sobre todo, determinista no probabilística.
Los algoritmos que usa son vitales para sus objetivos cognitivos y de percepción.	Son medios para validar y registrar la veracidad de las transacciones.
Es la creativa del equipo, la que piensa de manera abstracta y estudia las complejidades del entorno de negocio.	Tiene la misión de contar la verdad, garantizarla y actuar de mediador: poner de acuerdo a las partes para formar y documentar un acuerdo de manera inmutable.

Jean Turgeon, vicepresidente y director tecnológico de Avaya, dice que la IA, IoT y blockchian unidos están aportando un gran valor a las empresas y a las personas que los utilizan.

> Mientras que la automatización (IA) es una prioridad para brindar mejores experiencias conforme se elevan los niveles de eficiencia para las empresas, el IoT, ha sido un tema recurrente en los últimos años y su función es llevar el análisis en tiempo real a los procesos automatizados (de los cuales la AI forma parte). El IoT genera un flujo de trabajo sofisticado para personalizar las experiencias que las empresas ofrecen a sus clientes y usuarios.

En el contexto del blockchian, Turgeon señala:

> cuando empiezas a ofrecer servicios personalizados es probable que necesites acceder o almacenar cantidades grandes de información personal, lo que requiere una arquitectura de seguridad mucho más fuerte a la que hemos visto en el pasado con el modelo centralizado. Debido a que blockchain es una arquitectura distribuida que utiliza criptografía y un concepto de 'escribe un registro una sola vez', brinda un valor enorme a los casos de uso que se requieren como parte de las transformaciones digitales para mejorar la validación de algunos de esos datos sin alterar las bases de datos existentes, las cuales cumplen con varios requerimientos de cumplimiento. Todos esos factores combinados proporcionan una solución muy potente y pienso que éstos se implementarán juntos de manera mucho más frecuente en el futuro cercano.

Internet de las cosas

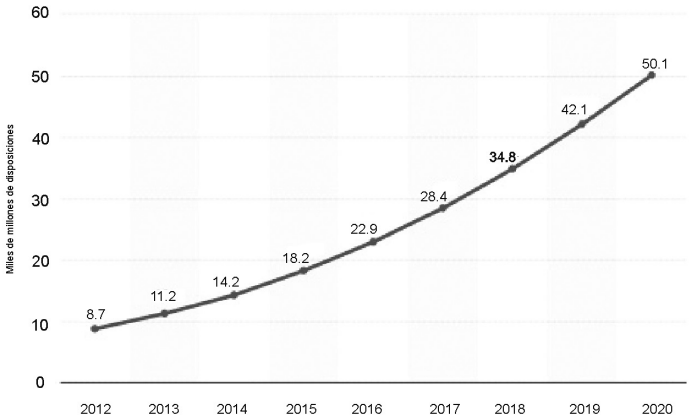
El internet de las cosas (IoT, por sus siglas en inglés) es una de las tecnologías con mayores posibilidades. Sus aplicaciones son casi infinitas. Según Statista,[20] en 2012 había 8,700 millones de dispositivos conectados en todo el mundo; en 2019 la cantidad subió a 42,100 millones y se espera que en 2020 la cifra llegué a los 50,100 millones.

En 2014, un estudio basado en 1,600 opiniones de expertos indicaba que para 2025

[20] "Previsión de la evolución de los dispositivos conectados a internet en el mundo de 2012 a 2020", *Statista*, disponible en <https://es.statista.com/estadisticas/517654/prevision-de-la-evolucion-de-los-dispositivos-conectados-para-el-internet-de-las-cosas-en-el-mundo/>.

GRÁFICA 9.

Dispositivos conectados: previsión mundial del número de conexiones 2012-2020



nuestros cuerpos y la enorme mayoría de los objetos que usamos a diario estarán conectados y generarán información en tiempo real, lo que provocará un cambio enorme en temas importantes como salud, transporte, compras, producción industrial, medio ambiente y finanzas.

El término "internet de las cosas" se le atribuye al investigador británico Kevin Ashton, quien a fines de los años noventa sostenía que los objetos de la vida diaria deberán ser capaces de introducir información en la web sin la necesidad ni la ayuda de las personas. Otro de los pioneros en instalar el concepto fue el físico Neil Gershenfeld, que en 2001 publicó su libro *Cuando las cosas empiecen a pensar*, que sirvió como punto de partida para lo que hoy se observa como una tendencia global. Ya en aquel entonces Gershenfeld hablaba de la desaparición física de las computadoras, la necesidad de las interfaces naturales y de la ropa inteligente con chips incorporados.

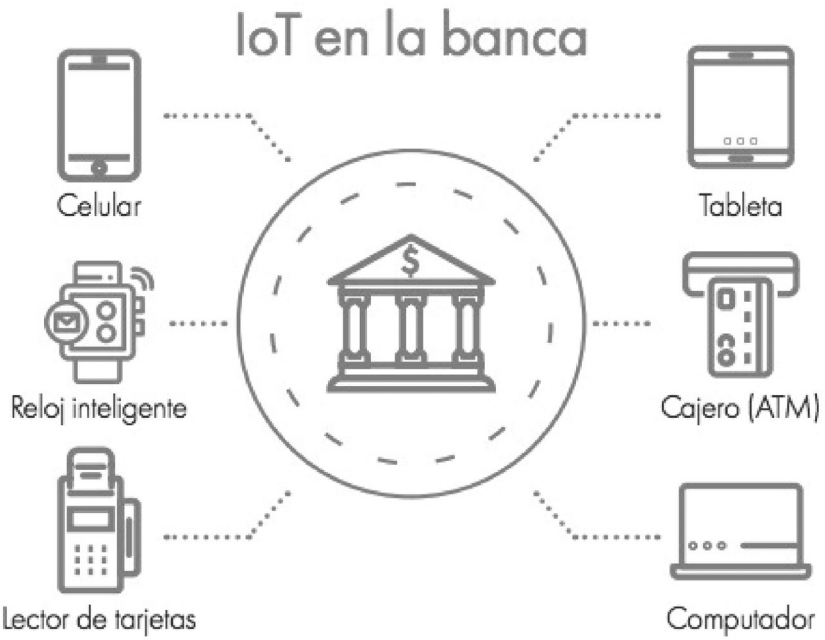
El internet de las cosas está revolucionando la industria. Para Francisco Igual Peña,[21] el IoT podría permitir a los bancos entender mejor los comportamientos y necesidades de sus clientes. "El despliegue masivo de sensores puede ayudar al sector bancario en una interacción más sencilla y eficiente entre el cliente y la oficina en aspectos tan variados como identificación biométrica, seguridad en la oficina o l desarrollo de nuevos métodos de pago en comercios".

Para visualizar cómo explotar el potencial del internet de las cosas, en Deloitte[22] se desarrolló un ejercicio de simulación

[21] Francisco Igual Peña, "¿Qué puede hacer el internet de las cosas por la banca", junio de 2019, disponible en <https://www.bbva.com/es/que-puede-hacer-el-internet-de-las-cosas-por-la-banca/>, consultado el 19 de enero de 2020.

[22] Salvador Hernández, socio líder de Estrategia y Operaciones en Servicios Financieros en Consultoría, Deloitte México, "Internet de las cosas: lo tangible a lo financiero", disponible en <https://www.forbes.com.mx/internet-de-las-cosas-lo-tangible-a-lo-financiero/>.

GRÁFICO 2.



dirigido por Wikistrat, la consultora en análisis geoestratégico y comercial considerada como la primera especializada en *crowdsourcing*.[23] Se reunió el conocimiento de académicos, analistas y empresarios con el objetivo de trazar las oportunidades para capitalizar la información del internet de las cosas.

Los resultados, además de atractivos, también representan desafíos para aquellas empresas que buscan detonar su nivel de competitividad:

- **Apertura de nuevos negocios para los bancos.** Con el uso de sensores biométricos y posicionales, las instituciones financieras podrían realizar un seguimiento del rendimiento de cada usuario, de tal manera que lograrían abrir nuevos créditos, especialmente en segmentos de clientes que carecen de un historial crediticio.[24]
- **Servicio a la medida del cliente.** Crear servicios personalizados es otra de las posibilidades que trae el internet de las cosas; por ejemplo, un banco podría

[23] Tendencia que se ha ido desarrollando con la evolución de internet; el término, como su nombre lo dice en inglés, *crowd* traducido como masas y *sourcing*, fuente, es prácticamente nuevo y se utiliza para exteriorizar un problema e involucrar a la audiencia.

[24] Los autores refieren que esto ya ocurre en algunos bancos localizados en Dubái y Londres, pero advierten que habría que esperar que, en países como el nuestro, se trabaje en la legislación correspondiente con fines de autenticar su aspecto legal.

asociarse con fabricantes de línea blanca y empresas de electrónica de consumo (bocina, *smartphones*, pantallas, consolas de videojuego, entre otros), de tal manera que lograrían lanzar ofertas de crédito a las personas cuyos dispositivos comienzan a deteriorarse.

- **Inversión y gestión de carteras más acertada.** Utilizar información del ecosistema del internet de las cosas del cliente permitiría a las empresas adaptar sus decisiones de inversión y asignación de activos basados en los comportamientos, preferencias y ubicación de los usuarios. Además, sustituiría los inciertos cuestionarios por algoritmos que, a través del análisis de patrones de vida, proporcionen una imagen más precisa de cada cliente.
- **Administración de carteras.** Internet de las cosas permitiría combinar los flujos de datos en tiempo real de una variedad de sensores con tecnologías cognitivas y comunicación M2M para automatizar el fondo de gestión mucho más allá de lo que se ve hoy, provocando un aumento en la diferenciación entre tipos de inversión, fondos y estrategias de fijación de precios.
- **Más transparencia y autenticación en la gestión de riesgos.** Las compañías podrían monitorear los niveles de estrés de los empleados, patrones de movimiento y otros factores como una forma de predecir el potencial de fraude interno, mientras que los minoristas podrían autenticar las transacciones de tarjetas de crédito al hacer posible que la presencia del plástico coincida con otro objeto físico (como un teléfono móvil o incluso *wearables*).

Datos de Bancomext indican que 88 por ciento de las instituciones financieras a nivel global cuentan con una estrategia donde la tecnología es el habilitador principal de su oferta de productos y servicios financieros. Actualmente existen 2 mil millones de usuarios de banca móvil, lo que representa 50 por ciento de todos los usuarios de banca a nivel global.

En México, el sector financiero está adoptando el uso de nuevas tecnologías para adaptarse mejor a las necesidades de los clientes; el uso de IoT permite la introducción de nuevas formas de automatización en los procesos de los clientes y de las instituciones financieras. En un futuro cercano permitirá lanzar nuevos servicios y generar ingresos adicionales, así como brindar una mejor experiencia del cliente y conseguir mayores niveles de fidelización con la marca. Sin embargo, existe un reto: hacer frente a las amenazas de seguridad y encontrar las soluciones para la protección de la integridad y la confidencialidad de los datos, ya que en el centro de IoT están los datos que se generan e intercambian.

Big Data

BBVA New Technologies define a big data como el término que se emplea para describir el conjunto de procesos, tecnologías y modelos de negocio que están basados en datos y en capturar el valor que los propios datos encierran.

El valor es grande, considerando que actualmente existen más de 2.5 trillones de datos, de los cuales 90 por ciento se han generado en los dos últimos años. Además, actualmente la naturaleza de la información es diferente a la del pasado. Los datos se han dividido en estructurados y no estructurados.

Los primeros son la información que puede encontrarse en la mayoría de bases de datos: archivos de tipo texto que se sue-

len mostrar en filas y columnas con títulos, y pueden ser ordenados y procesados fácilmente por todas las herramientas de minería de datos. Los segundos, generalmente, son un conglomerado masivo y desorganizado de varios objetos que no tienen valor hasta que se identifican y almacenan de manera organizada. Sus principales características son: origen, volumen, crecimiento y almacenamiento.

El origen de los datos es muy diverso: datos generados en redes sociales, en foros, *e-mails*, extraídos de la web, documentos internos de la compañía (word, pdf, ppt). Por su estructura no puede emplearse arquitectura relacional, siendo necesario trabajar con herramientas big data. Algunas cifras sobre estos datos: cada día se realizan más de un billón de consultas en Google, más de 250 millones de tuits, 800 millones de actualizaciones en Facebook, 60 horas de videos subidos por minuto en YouTube y 10 mil transacciones mediante tarjeta de crédito por segundo.

De ahí que big data aplique para toda la información que no puede ser procesada o analizada utilizando procesos o herramientas tradicionales. Según Kenneth Cukier, autor del libro *Big Data. La revolución de los datos masivos*,[25] "se trata de hacer cosas a partir del análisis de inmensas cantidades de información, que simplemente no son posibles con volúmenes más pequeños". Define a big data como "la capacidad de la sociedad para asimilar la información mediante vías novedosas con el objetivo de producir conocimientos, bienes y servicios de valor significativo".

Big data aplicado a los negocios es básicamente el análisis masivo de datos para usarlos a la hora de tomar decisiones determinantes para el futuro de una empresa. Por ello las compañías adoptan sistemas capaces de analizar en segundos grandes cantidades de datos que permiten responder a las demandas del negocio en tiempo real.

"Esto puede lograrse tanto a través de una mejora en la eficiencia gracias al análisis de los datos (una visión más tradicional) como mediante la aparición de nuevos modelos de negocio que supongan un motor de crecimiento. Se habla mucho del aspecto tecnológico, pero hay que tener presente que es crítico encontrar la forma de dar valor a los datos para crear nuevos modelos de negocio o de ayudar a los existentes", señala un documento de BBVA New Technologies.

Generación de valor

En los años noventa, John Mashey publicó un artículo titulado *Big Data and the Next Wave of Infrastress* popularizando el término. Mashey hacía referencia al estrés que iban a sufrir las infraestructuras físicas y humanas de la informática debido al imparable *tsunami* de datos que ya se veía y se planteaba como inmanejable con la tecnología de la época.

De acuerdo con los resultados de la encuesta sectorial sobre big data de E&Y,[26] en todo el mundo las organizaciones han empezado a explotar las oportunidades que big data ofrece. Sin embargo, el avance ha sido muy pequeño en cuanto a la cuantificación del valor que se va a obtener con el análisis de datos estructurados y no estructurados de forma conjunta para generar conocimiento que apoye la toma de decisiones.

[25] *La revolución de los datos masivos*, Mayer-Schönberger, Viktor/Cukier, Kenneth, Editorial Turner, 2013.

[26] "Informe sobre big data en el sector financiero", disponible en <https://www.ey.com/es/es/home/ey-informe-sobre-big-data-y-analytics-en-el-sector-financiero-espanol#.Xi4pkyPhBlA>, consultado el 6 de enero de 2020.

E&Y destaca que es precisamente el valor que se deriva de la gestión de los datos y su transformación en conocimiento útil lo que, probablemente, constituye la mayor ventaja de big data, que completa las "3Vs" y los tres retos que tan frecuentemente se mencionan asociados a estos conceptos:

- **Volumen:** cantidad ingente de datos que no pueden ser manejados por las herramientas tradicionales de gestión de bases de datos.
- **Variedad:** datos obtenidos de una gran diversidad de fuentes, internas y externas, con diferentes formatos, tanto estructurados como no estructurados.
- **Velocidad:** datos que cambian y evolucionan a una gran velocidad, y necesidades de negocio que precisan de análisis y respuestas casi en tiempo real.

E&Y añade que muchas empresas aún no han desarrollado el marco adecuado para generar ese valor, por lo que "el primer paso para derivar valor de big data no debería ser hablar de cómo hacerlo, sino empezar preguntando qué decisiones de negocio debo adoptar de modo más eficiente y eficaz".

Comprender y aplicar

Por lo anterior, tiene importancia el documento *Benefitting from Big*, de Booz & Company, en el que señala algunos ejemplos de la aplicación de big data:

Análisis de los clientes

- **Marketing impulsado por los clientes:** promociones y ofertas personalizadas basándose en las pautas de compras individuales. Prevención de la pérdida de clientes.
- **Recomendación de productos:** filtros colaborativos, recomendaciones basadas en la actividad multicanal.

Análisis de marketing

- **Modelos del marketing mix:** optimización del marketing mix y de las promociones utilizando modelos econométricos para evaluar el aumento de ventas con diferentes herramientas de marketing, e identificar el más efectivo.
- **Optimización de los precios:** utilizar los datos para evaluar la sensibilidad de la demanda a los precios y para optimizarlos en diversos puntos del ciclo de vida del producto.

Análisis de internet/celulares/redes sociales

- **Análisis de la actividad del cliente:** almacenar las preferencias del cliente para personalizar lo que se muestra, monitorizar el uso para evaluar las métricas de la web.
- **Monitorizar los medios sociales:** analizar los sentimientos del consumidor hacia la marca y sus productos en redes sociales.

Efectividad operativa

- **Análisis de datos operativos** aprovechando abundantes datos de producción para mejorar los procesos y la calidad del producto.
- **Mejor planificación y predicción** aprovechando la cantidad de datos de procesos históricos, recursos y productos.

Análisis de fraude y riesgo

- **Análisis de datos** sobre clientes, transacciones y mercados para cuantificar el riesgo de clientes y productos.

- **Detección de fraude** en tiempo real aprovechando datos de los puntos de venta y de los sistemas de transacciones y análisis.

Las soluciones basadas en big data tienen como objetivo extraer información de valor mediante el análisis de grandes conjuntos de datos. Según el nivel de valor de la información obtenida pueden distinguirse tres clases de analítica:

- **Analítica descriptiva**. Consiste en almacenar y realizar agregaciones de datos históricos, visualizándolos de forma que puedan ayudar a la comprensión del estado actual y pasado del negocio. Da cuenta de cómo ha funcionado nuestro negocio hasta la fecha.
- **Analítica predictiva.** Se construye sobre la analítica descriptiva y usa modelos estadísticos avanzados para añadir datos que no conocemos a la base de información. Esto se traduce en técnicas como la predicción de valores futuros en series históricas de precios y demandas, pero también en la clasificación automática de textos u operaciones o en la segmentación de clientes. De esta forma, la analítica predictiva nos dice cómo va a funcionar nuestro negocio.
- **Analítica prescriptiva.** Supone el nivel más alto de analítica y explota los niveles anteriores junto con estrategias de optimización operativa para indicar qué acciones de negocio proporcionarán los mejores resultados. Mediante la analítica prescriptiva pueden obtenerse recomendaciones automatizadas sobre el momento idóneo para ejecutar pedidos, mantenimientos u otras operaciones cuantificables del negocio. Puede saberse qué hacer para optimizar nuestro negocio.

De acuerdo con Teradata en su informe global *Big data y Data Analytics: Desarrollo de nuevos modelos de negocio, el descubrimiento de nuevas ofertas de producto y la monetización,* "las empresas han llegado a un punto de transición en el que en lugar de hablar sobre los resultados que podrían conseguir con big data están empezando a ver beneficios reales".

The Data Warehouse Institute realizó un informe donde describe los aspectos necesarios para obtener mayor conocimiento de los clientes a través de analíticas con big data:

- Comprender el comportamiento de los clientes y clientes potenciales en todos los canales.
- Introducir procesos de analítica predictiva para llegar a ser más efectivos y proactivos.
- Generar un mayor *engagement* gracias al desarrollo de una analítica avanzada.
- Afinar la estrategia en medios sociales gracias a una analítica avanzada.
- Reducir la duración del proceso analítico para obtener información en tiempo real.
- Contar con una arquitectura que ofrezca flexibilidad y seguridad en la gestión de los datos.

El Instituto de Ingeniería del Conocimiento destaca dos de los beneficios del uso de big data:

1. **Mayor ROI en los procesos de negocio.** Al emplear técnicas de analítica prescriptiva que recomienden acciones basadas en datos sólidos sobre costos y beneficios esperados.
2. **Nuevos productos y servicios.** Con la capacidad de medir las necesidades de los clientes y la satisfacción a través de análisis viene el poder de dar a los clientes lo que quieren.

En el sector financiero

Para la consultora E&Y, el sector financiero ha sido tradicionalmente uno de los sectores más propensos a la inversión en tecnología, especialmente relacionada con los datos, por lo que no es extraño encontrar soluciones de big data orientadas a este mercado; sin embargo,

> las principales barreras identificadas en la adopción de una estrategia de Big Data en las entidades encuestadas se relacionan principalmente con las capacidades tecnológicas necesarias. Existe la percepción en la industria de que es necesario realizar fuertes inversiones en tecnología para poder acometer dichas iniciativas, algo difícil de asumir si se tienen en cuenta las restricciones presupuestarias actuales y la dificultad de estimar y cuantificar el retorno y rentabilidad de estas inversiones.

Agrega:

> No obstante, desde el punto de vista de las oportunidades y aplicaciones percibidas por parte del sector financiero, las respuestas de los encuestados develan que la principal área de aplicación de big data y Analytics la constituye la segmentación avanzada de clientes porque la incorporación de nuevas fuentes de datos a las segmentaciones tradicionales posibilita la obtención de una visión y un entendimiento más completos de los clientes de las entidades, lo que lleva aparejada la definición de propuestas de valor más adaptadas a los diferentes perfiles de clientes.

Otras aplicaciones que menciona son la fidelización de clientes y una mejor gestión de la omnicanalidad, lo que es realmente importante por el contexto en el que las nuevas tecnologías ponen a disposición de los clientes un mayor número de canales de comunicación mejorados y alta capacidad de transacción con las empresas.

Barreras y soluciones

La IE Business School considera que la gran barrera que tienen muchas de las empresas del sector financiero para instaurar una estrategia de big data está relacionada con la percepción que tienen éstas de su adaptación, ya que muchas tienen una idea equivocada de que para implementar el big data es necesario hacer una gran apuesta económica. Otro freno para iniciar la implantación del big data es que no existen demasiados científicos de datos o expertos y analistas de negocio que corroboren que el big data es una apuesta segura para cualquier empresa del sector financiero.

Esta escuela de negocios destaca que para afrontar los frenos o barreras que tienen las empresas debe tomarse en cuenta:

- **Estar preparado para la transformación.** Es necesario que los cargos principales de las entidades financieras lideren la transformación, identificando y dando el mando al talento interno, con el fin de que dentro de la empresa exista la misma filosofía de cambio.
- **Decidir qué quiere mejorarse y definir cómo quieren medirse los resultados**. No sería la primera vez que, por un error en el establecimiento de una métrica o KPI, no se lleguen a conocer con certeza los resultados y beneficios obtenidos.
- **Establecer una buena estrategia.** Definir bien los planes de actuación que se van a llevar a cabo es una tarea que debe hacerse transmitiendo las directrices por seguir a todos los empleados, con

el fin de que todo lo que se plantee haga eco en todos los departamentos.

Gary Chropuvka, responsable de estrategias cuantitativas en Goldman Sachs AM, explica:

> Big data requiere un elemento humano que evite que inversionistas y empresas sigan el camino equivocado. El otro reto es asegurarse de contar con los conocimientos adecuados para analizar, almacenar y utilizar los datos en beneficio propio. La conclusión es que esto es sólo el inicio de la revolución de los datos. Si lo ignoramos, nos encontraremos con una desventaja informativa. Big data es algo que está transformando la forma en que interactuamos con las personas y también está transformando a las empresas de todo el mundo.
>
> Todos los sectores del mundo tienen la capacidad de usar big data en su beneficio. El sector de comercio minorista lo ha utilizado para dirigir la publicidad hacia sus clientes y para llegar a comprender mejor sus gustos y preferencias. En el sector agrícola está permitiendo a los agricultores optimizar la producción de sus cosechas. En el sector de servicios financieros las inversiones siempre se han basado en contar con una ventaja informativa.

9. Seguimos mirando a futuro

La evolución del sistema financiero es continua y seguirá siendo impulsada por las innovaciones tecnológicas, los cambios en la demanda de los consumidores y fuertes cambios en la oferta, principalmente derivados de un entorno más competitivo. No obstante, la forma en la que las entidades del sector participarán dependerá de su enfoque y estrategia.

El pasado importa y de éste dependerá que asuman el proceso de transformación en el interior y con sus propios recursos o que inviten a los nuevos jugadores del sistema, como las fintechs, que no surgen como consecuencia de la aparición de nuevas tecnologías, sino como emprendedores que aprovecharon las oportunidades surgidas a partir de las innovaciones tecnológicas.

Esta relación plantea un reto fundamental: la regulación vista como un medio para abordar de forma correcta la captación de talento innovador, combatir la amenaza de la ciberseguridad y crear un marco regulatorio efectivo para las nuevas tecnologías.

México está a la vanguardia en regulación. La Ley Fintech es el ejemplo (así nos ven desde fuera) de cómo legislar en el entorno actual; sin embargo, algunas voces han dicho que la regulación secundaria de la ley frena el espíritu de la innovación, mientras que otras aplauden los esfuerzos y participan para que los resultados tengan un enfoque de pluralidad multisectorial, pero ambas saben que con la innovación proviene el riesgo y se requiere una garantía de seguridad.

En esta parte hemos dado un recorrido por los riesgos, su evolución e importancia, dependiendo de los actores y factores que en momentos específicos del tiempo se han tenido. El último apartado nos deja una pregunta: ¿Qué sigue en materia de riesgos y cuál es el papel de la regulación en un mundo de innovación que fue posible por la desregulación?

TERCERA PARTE

Nuevos componentes para un desarrollo incluyente

10. Evolución de la arquitectura del sistema financiero

De 1971 a nuestros días, el entorno financiero internacional ha sufrido profundas transformaciones, como la eliminación de la convertibilidad de dólares en oro, la flexibilización de los regímenes cambiarios de un gran número de países, el incremento de la liquidez mundial, y la liberalización y desregulación financiera a escala global.

Desde la mitad de la década de 1970, la desregulación de los mercados financieros, la creación de nuevos instrumentos y los cambios tecnológicos han tenido un impacto mayor y han contribuido a un sistema financiero internacional altamente integrado que ha vinculado las economías nacionales de manera más estrecha e incrementado el capital disponible para los países en desarrollo.

El proceso de liberalización y desregulación, con el sucesivo desmantelamiento de las normativas y de los controles de la actividad financiera, fueron las características de las siguientes décadas que hicieron un alto tras las crisis mexicana (1994-1995) y asiática (1997-1998), que mostraron que sin coordinación macroeconómica, sin requerimientos mínimos de liquidez y solvencia, sin una supervisión y regulación global, y con productos financieros de creciente complejidad, el mercado contaba con un fuerte grado de opacidad y, porqué no, de debilidad.

Ante ese escenario, el resultado inmediato fue la necesidad de fortalecer, modificar o reconstruir el sistema a través de la creación de una nueva arquitectura financiera internacional (NAFI), concebida como la estructura de procedimientos y normas financieros que definen el alcance y las operaciones de los mercados financieros internacionales.

Se trataba de recuperar la confianza de los mercados y evitar incurrir en los mismos errores del pasado, superando los modelos de negocios fallidos, y lograr que el sector público mejorara su capacidad de supervisar y regular un mercado financiero global.

La tarea se estaba haciendo, pero la crisis de 2008 puso de manifiesto que la innovación tecnológica y financiera, que sugería una nueva ingeniería financiera,[1] colocó en primer plano la necesidad de un nuevo marco con determinados parámetros de seguridad sistémica y con una supervisión efectiva. Lo que se requería entonces era:

- Sistemas regulatorios que permitieran prevenir los excesivos riesgos asumidos como práctica habitual por las instituciones financieras en los años recientes.
- Una coordinación reguladora entre países.
- Soluciones globales a partir del diálogo entre bancos centrales, supervisores y reguladores.

Pero la crisis financiera de 2008 trajo otra crisis consigo: la de desconfianza. "Un resultado de la crisis global de 2008 fue la pérdida de confianza de la sociedad en el sistema financiero. El principal problema radica en una aparente contradicción: los intermedia-

[1] La ingeniería financiera tiene como objeto de estudio el diseño, desarrollo e implementación de instrumentos y procesos financieros innovadores, apoyada en herramientas matemáticas, estadísticas, de simulación y computación, para la gestión óptima del riesgo y la toma de decisiones financieras.

rios financieros mantienen la base de clientes, pero la confianza de éstos en el sistema mismo ha decrecido de manera sensible".[2]

En medio de esa crisis de confianza, la tecnología emergió abruptamente y, con ello, lo hicieron también nuevos actores en el escenario financiero internacional. Los efectos negativos de la crisis sobre los sistemas financieros y las economías nacionales fueron el marco para la expansión de las empresas fintech a partir de 2009 (aunque es hasta 2014 cuando se registran las tasas de crecimiento más altas de esta actividad tanto en las economías desarrolladas como en las emergentes).

La crisis de 2008, así como el surgimiento y apuntalamiento de las fintechs hizo que se buscara una agenda de principios en el sistema bancario global —ya muy diferente al que se fue conformando en la década de los años setenta— que considerara las condiciones del entorno, la industria global (con sus interrelaciones y riesgos), las presiones regulatorias globales, el cambio en la demanda de los servicios y productos (características de los clientes y nuevas necesidades), jugadores, tecnología y el efecto fintech.

Partiendo de lo anterior, a nivel país, el Grupo Asesor del CEEY (2017) generó un diagnóstico y propuestas para mejorar el funcionamiento e independencia del sistema financiero mexicano.[3] Partieron de dos preguntas: ¿Qué tendencias determinan los pasos siguientes en la evolución del sistema financiero y su arquitectura? y ¿qué tendencias ayudarán a lograr un empuje que transforme la arquitectura del sistema?

El CEEY considera que la arquitectura del sistema financiero va más allá de la estructura jurídica y de las figuras del sistema financiero, pues lo relevante es identificar las funciones y las interrelaciones entre todas las partes que se mueven en el siguiente escenario:

- Proceso de consolidación desde 2004 que permitió nuevos intermediarios y proyectó más fusiones y adquisiciones.
- Empresas no financieras, cadenas de *retailers* y de telecomunicaciones con un papel cada vez más relevante en la operación del sistema financiero.
- Cambios regulatorios constantes con miras a mejorar la supervisión y la adaptación a los estándares internacionales.

> Las condiciones sugieren que la arquitectura seguirá transformándose. Si bien hay un grupo de aproximadamente siete bancos comerciales grandes y un conjunto de grupos financieros relativamente estables, existe un universo muy variado de intermediarios que se encuentran en transformación continua. Las nuevas consolidaciones, el incremento en el costo de la franquicia bancaria por reglas más onerosas de capital y de liquidez, así como los costos regulatorios son variables que modifican día a día la industria financiera. Asimismo, la innovación tecnológica en el ecosistema de pagos, en el financiamiento a los micronegocios y en la contratación de seguros, por citar algunos

[2] *El sistema financiero mexicano. Diagnóstico y recomendaciones*, México, Centro de Estudios Espinosa Yglesias, 2017.

[3] El trabajo es el resultado de nueve sesiones de discusión del grupo que el CEEY organizó y que se llevaron a cabo entre noviembre de 2013 y mayo de 2015. En estas discusiones participaron tanto miembros permanentes del grupo como invitados especiales, según el tema que se iba a tratar. El documento busca tener un espíritu plural, desde distintos enfoques y componentes del sistema, así como una visión integral de su arquitectura.

ejemplos, han de tener su respectivo efecto (CEEY, 2017).

En el tabla Factores para la configuración del Sistema Financiero se muestran tres columnas que marcan los elementos que determinan la configuración del sistema financiero a partir de su influencia y factor determinante. Si hiciéramos un ejercicio combinando las columnas con las casillas, por ejemplo: factor determinante riesgos externos e internos (3/2) con presiones regulatorias globales (1/4), podríamos tener regulación financiera (1/5).

Lo que este ejercicio nos da es la interrelación de factores y la posibilidad de ver qué elementos pueden ser los determinantes en una coyuntura específica y, por lo tanto, qué debe considerarse para dar respuestas eficaces en el marco de la configuración de una nueva arquitectura financiera a partir de cinco condicionantes: uso de la tecnología, participantes, productos y servicios, situaciones que se tienen que evitar (riesgos) y reglas para interactuar.

Factores para la configuración del Sistema Financiero

	1	*2*	*3*
1	Elemento	Influencia	Factor determinante
2	Condiciones del entorno	En economías como la mexicana, los intermediarios financieros necesitarán hacer ajustes ante el escenario de riesgos de mediano plazo: caída en el precio del petróleo y de otros *commoditties*, normalización de la política monetaria de la Reserva Federal, fortalecimiento del dólar y depreciación de la moneda local. Para ello, será importante vigilar el balance de las empresas deudoras, así como la vulnerabilidad financiera de los hogares. Con base en ello, habrá que tomar medidas para prevenir riesgos en la salud del sistema financiero.	Riesgos externos e internos.
3	La industria global	Una tendencia global de la industria financiera es la entrada de oferentes de servicios financieros distintos de la banca; en algunos casos no son intermediarios y se encuentran fuera del sistema y de su regulación. La contracción del financiamiento global posterior a 2008 abrió ventanas de oportunidad a intermediarios no bancarios en el mundo y éstos han crecido y abastecido a los mercados.	Empresas no financieras. Intermediarios no bancarios. Alcance regulatorio.
4	Presiones regulatorias globales	En el ámbito global, la implementación de Basilea III, así como las nuevas regulaciones derivadas de la crisis de 2008, como la Dodd Frank, las reglas de prevención de lavado de dinero, de-risking, *know your costumer*, conforman un entorno en el cual se percibe sobrerregulación y aversión al riesgo por parte de muchos intermediarios establecidos. Lo anterior afecta las posibilidades de mayor inclusión.	Regulación y riesgos.
5	Regulación	Cambios legislativos *vs.* funcionamiento institucional.	Flexibilidad para atender las nuevas condiciones.

	1	*2*	*3*
6	El cambio en la demanda	El cambio demográfico ha transformado la demanda para el sector financiero; los usuarios de tecnología tienen alto nivel de exigencia, además de preferencias de consumo distinta a generaciones previas y fuentes de ingresos no estables, entre otras. Además, los hábitos de consumo han cambiado.	Inclusión financiera. Customización de los servicios.
	Fintech	Las nuevas formas de innovación pretenden ser disruptivas no sólo para crear un nuevo servicio, sino para modificar las expectativas de los usuarios, porque la tecnología es más interactiva y ofrece al usuario más participación en los servicios que requiere. A nivel global, no queda clara la trayectoria de la innovación, y tampoco existe una taxonomía definitiva sobre lo que en este ámbito será lo más relevante. Tampoco es del todo diáfano cuáles habrán de ser las tecnologías dominantes. Lo que es un hecho es que la innovación está creando mayores presiones competitivas sobre los intermediarios establecidos.	Más intermediarios (jugadores). Innovación permanente. Presiones en la industria.
7	Estructura	La estructura del sistema está constituida por dos fuerzas que apuntan en direcciones distintas. Por un lado, se encuentran los intermediarios que necesitan cubrir segmentos que el mercado ha desatendido; por el otro, el hecho de que la licencia bancaria sea menos onerosa para facilitar la operación de bancos de distinta escala.	Cantidad y calidad de los participantes.
8	Alcance de los intermediarios financieros	La banca de desarrollo y los fondos y fideicomisos de fomento han tenido un efecto importante en la arquitectura de los mercados de ahorro y crédito. La banca de desarrollo juega un papel relevante en el fondeo de bancos pequeños y de intermediarios no bancarios. Por su parte, las Sofomes podrían sobrevivir sólo con líneas de crédito de la banca de desarrollo. En proyectos de bursatilización son necesarias las líneas de fondeo de la banca de desarrollo.	Vínculo público y privado.

Fuente: elaboración propia con información de *El sistema financiero mexicano. Diagnóstico y recomendaciones*, México, CEEY, 2007.

En otros apartados ya hemos abordado para el sistema en general el aspecto tecnológico, los viejos y nuevos participantes y las situaciones que tienen que evitarse (riesgos). En las siguientes páginas nos abocaremos a una parte de los nuevos participantes, es decir, a las fintechs, así como a los productos y servicios que se están incorporando a partir de estas empresas de tecnología financiera que están requiriendo reglas para interactuar, tomando en cuenta el desarrollo tecnológico y las situaciones que tienen que evitarse.

Por lo tanto, retomaremos aspectos básicos de la Ley Fintech (abordada a profundidad en el libro *Fintech: Vientos del cambio. Normatividad Bancaria*, México, Grañén Po-

rrúa, 2019) para dar cabida a los lineamientos que se incorporan en 2020, lo que también puede darnos elementos para considerar en nuestra visión (la que vamos construyendo con las nuevas realidades) de la arquitectura del sistema financiero.

11. Fintech: incorporación, marco, avance, expectativas

Desde el punto de vista de Fintech Radar México, la promulgación de la Ley Fintech, el 9 de marzo de 2018, y la posterior publicación de las primeras disposiciones secundarias, el 10 de septiembre del mismo año, han contribuido a un crecimiento neto de 18 por ciento en el número de *startups* existentes desde su última medición, publicada a finales de julio de 2018. Fintech Radar México apuntó que, si bien la espera de estas disposiciones generó incertidumbre sobre las medidas que deberán acatarse, en particular por las empresas de fondos de pago electrónico y de financiamiento colectivo, el ecosistema fintech mexicano observó un crecimiento que lo ubica en el primer puesto en Latinoamérica.

De acuerdo con el informe "Fintech en América Latina 2018: crecimiento y consolidación,[4] la regulación tiene importancia en el desarrollo del ecosistema. Según sus datos, 9 por ciento considera que no se necesita una regulación específica, mientras que 35 por ciento, que sí es necesario y 35 por ciento, que la regulación actual es adecuada. Según el informe, estos datos reflejan el progreso alcanzado en ciertas jurisdicciones en materia de regulación y resaltan avances logrados gracias al diálogo entre reguladores y la industria para propiciar la búsqueda de un marco favorable para la innovación.

En México, de acuerdo con la Comisión Federal de Competencia Económica (Cofece), la motivación de la regulación de las fintechs tiene como objetivo contribuir a la inclusión financiera, aumentar la calidad y creación de nuevos productos y servicios, tener flexibilidad que permita la innovación, contribuir a la reducción de costos de los productos y servicios, otorgar certeza jurídica a los inversionistas (favorecer la inversión en el sector), proteger al consumidor de fraude, asegurar estabilidad del sistema financiero y prevenir el lavado de dinero.

BBVA Research, en su informe "Situación Regulación Financiera 1T19",[5] indicó que 2019 sería el año en el que las autoridades deberían pasar a la acción e implementar una respuesta global para los retos de esta nueva era. Detalló que la importancia de la regulación fintech no entiende de fronteras. "En Europa, Estados Unidos, América Latina, en todo el mundo se pretende aprovechar las oportunidades que ofrece la digitalización para avanzar en materia de inclusión financiera".

BBVA Research (2019) apuntó que México es pionero en temas de regulación y que algunos bancos e instituciones financieras no bancarias están empezando a explotar las oportunidades que representa este nicho de mercado. "El marco regulatorio le ha dado certeza a los grupos financieros y están dispuestos a invertir en este segmento, algunos bancos ya han decidido que prefieren tener al mundo fitech como un aliado y no como un competidor", se mencionó

[4] Banco Interamericano de Desarrollo (BID) y Finnovista, noviembre de 2018.

[5] "Regulación 'fintech': tendencias de una nueva era", enero de 2019, disponible en <https://www.bbva.com/es/regulacion-fintech-tendencias-de-una-nueva-era/>.

en el informe, en el que se plantean denominadores comunes, como los relacionados con la tecnología, aunque existan contextos y situaciones completamente distintas en los países y regiones.

La situación de México fue expuesta en el reporte "Termómetro Fintech: Los retos de la regulación".[6] Desde varias características, como capital, empleo, índice de maduración e impacto de la regulación, el reporte plantea una radiografía de las empresas de tecnología financiera en el país:

- El volumen anual de operación de fintech equivale a 68,409 millones de pesos con 4.7 millones de usuarios registrados.[7]
- El ecosistema fintech en México es liderado por un pequeño grupo de emprendedores que han alcanzado una mayor escala. De las *startups*, 70 por ciento han levantado capital y deuda en los últimos cinco años, equivalentes a 629 millones de dólares. Sin embargo, de las 394 *startups* identificadas, sólo ocho concentran 80 por ciento de esos recursos.
- Este ecosistema es responsable de 3,600 empleos directos. Como reflejo de la etapa en la cual se encuentran la mayoría de las empresas, la productividad del sector está muy concentrada en siete empresas que han superado los 100 empleos y que generan 36 por ciento de los empleos del sector, mientras que 56 por ciento se encuentra en empresas con entre uno y 10 empleados, seguido de 22 por ciento que está entre 11 y 25 empleos directos.
- Como resultado del Índice de Maduración del Ecosistema Fintech en México (INFIN), desarrollado por Endeavor, se encontró que las *startups* fintech mexicanas (considerando variables como ventas, empleos, inversión, volumen de operaciones, usuarios activos, mercado y tecnologías utilizadas) se encuentran en una etapa de crecimiento.
- El sector fintech en México está representado, en mayor medida, por emprendedores en una etapa temprana y de crecimiento, ya que la empresa típica del sector tiene tres años de fundación, 105 mil dólares de ingresos anuales, sólo nueve empleados y ha levantado 230 mil dólares en capital.
- Los emprendedores manifiestan sobre la Ley Fintech, principalmente, que: habrá fuertes barreras de entrada para las *startups* o nuevos jugadores (28 por ciento), los altos costos asociados al cumplimiento de la ley generarán ineficiencias (22 por ciento), habrá que cumplir un marco regulatorio riguroso (21 por ciento) y, finalmente, 13 por ciento manifiesta estar 100 por ciento conforme con la ley y sus reglamentos, y estar listo para cumplir las disposiciones en septiembre.

De las fintechs consultadas, 57 por ciento manifestó estar sujeto al cumplimiento de las nuevas disposiciones y el costo que esperan es de 35 mil dólares anuales; sin embargo, 21 por ciento de los emprendedores y la mayoría de los entrevistados calculan que el costo regulatorio esté alrededor de los 100 mil dólares (incluidos abogados, consultoría, oficial de cumplimiento certificado, entre otros).

Este resultado se dio debido a que "La Ley Fintech señaló que deberían presentar

[6] Realizado por Endeavor con el apoyo de Google, Finnovista, la Embajada Británica y el Banco Santander, 2019.

[7] El estudio precisa que se llegó a estos datos, que podrían equipararse a la cartera y activos manejados por un banco, por medio de una muestra de 148 fintechs.

su solicitud de autorización en un plazo que no excediera los 12 meses contados a partir de la fecha de entrada en vigor de las disposiciones emitidas por la CNBV y publicadas en el Diario Oficial de la Federación el 10 de septiembre del 2018".

En 2019, la CNBV tenía mapeadas más de 515 fintechs que operaban en México y estimaba que alrededor de 200 deberían cumplir con las nuevas disposiciones, al encontrarse en las categorías de fondo de pago electrónicos (*wallets*), activos virtuales (*cryptocurrencies*) y financiamiento colectivo (*crowdfunding*).

El plazo para la autorización vencía el 25 de septiembre del 2019. La CNBV informó que recibió 85 solicitudes de autorización para operar como Instituciones de Tecnología Financiera, de las cuales 60 solicitaron autorización para operar como Instituciones de Fondos de Pago Electrónico y 25, como instituciones de financiamiento colectivo, por lo que las personas que realizaban actividades de financiamiento colectivo o de fondos de pago electrónico con anterioridad a la entrada en vigor de la Ley Fintech y que presentaron su solicitud de autorización ante la CNBV en el periodo establecido, podrían continuar realizando dichas actividades hasta en tanto se resuelva su solicitud, mientras que las personas que no presentaron su solicitud de autorización al 25 de septiembre, deberán abstenerse de continuar realizando actividades o celebrando nuevas operaciones, y deberán realizar únicamente los actos tendientes a la conclusión o cesión de las operaciones existentes; de lo contrario, serían sujetas a las sanciones penales y administrativas que marca la ley.

Asimismo, las personas interesadas en constituir sociedades de nueva creación para realizar actividades de Instituciones de Tecnología Financiera podrán iniciar su proceso de autorización ante la CNBV en cualquier momento y realizar dichas actividades una vez obtenida la autorización correspondiente.

Estructura y alcance

Los hallazgos del "Termómetro Fintech: Los retos de la regulación" nos remiten al elemento de Estructura referido en el cuadro Factores para la configuración del Sistema Financiero:

> La estructura del sistema está constituida por dos fuerzas que apuntan en direcciones distintas. Por un lado, se encuentran los intermediarios que necesitan cubrir segmentos que el mercado ha desatendido; por el otro, el que la licencia bancaria sea menos onerosa para facilitar la operación de bancos de distinta escala. Las presiones regulatorias y de mercado han resultado en la reducción de Sofomes y de socaps, y la diversidad de figuras ha dificultado la consolidación del sistema.

Por lo tanto, las Instituciones de Tecnología Financiera (ITF) podrían contemplar desde ser una Sofom, sofipo e, incluso, un banco *vs.* ser una ITF de financiamiento colectivo y de fondos de pago electrónico. Esto podría ser posible porque, de acuerdo con el análisis del reporte, "la oferta fintech podría contraerse en 50 por ciento si se toma en cuenta la experiencia previa ocurrida con las Sofomes, cuando entró en vigor la reforma financiera en 2014".

Datos de la CNBV indican que en 2015 había un registro de 3,500 entidades, número que se redujo a más de la mitad (1,560) una vez que se terminó el proceso de depuración, que consistió en la obligación de registrarse o renovar su registro ante la Condusef y cumplir con lo requerido en materia de prevención de lavado de dinero ante la Comisión Nacional Bancaria y de Valores.

Para Enrique Presburger Cherem, presidente regional de la Zona Centro de la Asociación de Sofomes de México (Asofom),[8] esa regulación por sí sola hizo que 70 por ciento de las Sofomes existentes desaparecieran paulatinamente, ya que cumplir con esas disposiciones de la autoridad es complejo y requiere mucha inversión, por lo que las Sofomes chicas no tuvieron la capacidad de hacer esas inversiones regulatorias, explicó.

Desde su perspectiva, podría darse una nueva consolidación, aunque no tan acelerada como la anterior, ya que las 1,600 sofomes que existen actualmente son sólidas, por lo que tal vez de esa cantidad entre 100 y 200 sean absorbidas y compradas por competidores grandes como una manera de hacer crecer su cartera.

El directivo de Asofom indicó que, en el tema de subsistir, se hace relevante que exista un mayor fondeo para este tipo de entidades, las cuales no pueden captar ahorro del público, por lo que tienen que acudir a mecanismos para obtener fondeo para prestar, como banca de desarrollo, bursátiles y fondos internacionales.

Esto nos recuerda el elemento 1 con su influencia:

> Alcance de los intermediarios financieros: La banca de desarrollo y los fondos y fideicomisos de fomento han tenido un efecto importante en la arquitectura de los mercados de ahorro y crédito. La banca de desarrollo juega un papel relevante en el fondeo de bancos pequeños y de intermediarios no bancarios. Por su parte, las sofomes podrían sobrevivir sólo con líneas de crédito de la banca de desarrollo. En proyectos de bursatilización son necesarias las líneas de fondeo de la banca de desarrollo. Otra posibilidad para esa depuración podría ser que las que no puedan acceder a un mayor fondeo posiblemente sean absorbidas por sofomes de mayor tamaño como una estrategia para hacer crecer sus carteras y tener los argumentos suficientes para recibir más fondeo.

Reformas al iniciar el siglo XXI

Los cambios recientes a los mercados financieros se observaron con las reformas ocurridas entre 1995 y 1999, en las que se modificaron la Ley del Banco de México, para atribuirle la facultad de otorgar crédito al gobierno federal, a las Instituciones de Crédito y al Instituto de Protección al Ahorro Bancario (IPAB); la Ley de Instituciones de Crédito, la Ley del Mercado de Valores y la Ley para Regular las Agrupaciones Financieras, en las que se establecieron sucesivos cambios en la regulación del capital social de las instituciones financieras, además de que se creó la Ley de Protección al Ahorro Bancario para garantizar el pago de las obligaciones (depósitos, préstamos y créditos) por parte del IPAB.

Los cambios que se dieron entre 2004 y 2012 mostraron una tendencia a favorecer los flujos financieros de forma regulada y la convergencia del sector con las prácticas de los mercados internacionales, incluida la regulación. En este periodo se modificó paulatinamente un conjunto de leyes en materia financiera que transformaron la organización del sector y las operaciones que realizan; el

[8] Entrevista a Enrique Presburger Cherem, presidente regional de la Zona Centro de la Asociación de Sofomes de México (Asofom), disponible en <https://idconline.mx/corporativo/2019/07/03/podran-sobrevivir-las-sofomes-a-la-4t>.

objetivo fue propiciar la mayor flexibilidad de los grupos financieros y dar prioridad a la adopción de prácticas cautelares para la adecuada administración de riesgos.

La Ley de Instituciones de Crédito del 18 de julio de 2006 modificó sensiblemente la estructura del sector financiero al determinar que, en un plazo de siete años, es decir, para julio de 2013, las operaciones de arrendamiento financiero y factoraje financiero dejaban de ser exclusivas de las instituciones constituidas expresamente para esas actividades, y cualquier persona física o moral podría realizarlas sin autorización de la SHCP. Desde esa fecha quedaron sin autorización las sociedades financieras de objeto limitado (sofoles).

Las sofoles se consideraban entidades de crédito especializadas en algún sector, que en su mayoría se concentraban en el financiamiento hipotecario, automotriz y de maquinaria industrial; entre marzo de 2001 y junio de 2013, la CNBV registró 110 sofoles; para junio de 2013, solamente permanecían como tales dos empresas. En sustitución de las sofoles se estructuraron las Sociedades Financieras de Objeto Múltiple (sofomes), no reguladas y reguladas (en este último caso, cuando mantienen vínculos patrimoniales con grupos financieros o Instituciones de Crédito); sus facultades se encuentran reglamentadas en la Ley General de Organizaciones y Actividades Auxiliares del Crédito.

Además de las sofomes, a partir de las reformas a la Ley de Ahorro y Crédito Popular del 3 de agosto de 2009, se originaron las Sociedades Financieras Populares (sofipos), las sociedades financieras comunitarias (soficos) y los organismos de integración rural. Asimismo, se crearon dos nuevas leyes para el mayor control de las instituciones financieras: la Ley de Uniones de Crédito (el 20 de agosto de 2008) y la Ley para Regular las Actividades de las Sociedades Cooperativas de Ahorro y Préstamo (el 21 de agosto de 2009).

Los resultados más visibles se observan con los cambios en la composición de las instituciones del sector; en diciembre de 2004, los 25 grupos financieros existentes se integraban en su mayoría por bancos, arrendadoras financieras, empresas de factoraje financiero, casas de bolsa, sociedades operadoras de sociedades de inversión y sofoles; en cambio, en diciembre de 2013, los 22 grupos financieros se constituyen principalmente por bancos, aseguradoras, administradoras de fondos para el retiro (afores) y casas de bolsa.

En 2014, con la reforma a la legislación financiera (32 leyes y la expedición de una nueva ley) se realizaron modificaciones tendientes a establecer las condiciones para las operaciones de crédito, para la integración efectiva del sector a través de la subcontratación de servicios financieros y mediante mayores controles en la exposición a riesgos, así como para la adopción de estrategias que promuevan la educación financiera y la inclusión financiera, lo que trajo cambios en la composición del capital social de las entidades financieras, la nueva estructura del sector, las modificaciones en los sistemas de ahorro para el retiro, las facilidades otorgadas para los flujos de inversión y la adopción de medidas prudenciales, así como las medidas para la educación y la inclusión financiera.

Oficialmente, esta reforma persigue los siguientes objetivos: mejorar las condiciones del acceso al crédito y ampliar la oferta de recursos para la actividad productiva, regular las nuevas operaciones de las instituciones financieras, adoptar mayores reglas prudenciales ante riesgos e incentivar estrategias para favorecer la inclusión financiera y la educación financiera.

Para otorgar mayor certidumbre y protección a los usuarios de servicios financieros, se introdujeron reformas a la Ley de

Protección y Defensa al Usuario de Servicios Financieros, por las que se crea el Buró Nacional de Entidades Financieras; por este medio, se pretende informar a los usuarios sobre los riesgos al contratar servicios financieros, ofrecer comparativos del desempeño de las instituciones financieras sobre sus indicadores de sanciones, transparencia, cláusulas abusivas, ventas atadas (o condicionadas) y reclamaciones; y emitir recomendaciones a la entidades del sector e informar sobre éstas al público. También se crea el Sistema Arbitral en Materia Financiera; por este medio, las instituciones financieras inscritas (voluntariamente) pueden proporcionar facilidades a los usuarios para resolver controversias relacionadas con la prestación de sus servicios.

Con finalidades de prevención y regulación del sector financiero, y mediante modificaciones a la Ley de la Comisión Nacional Bancaria y de Valores, se reforzaron las atribuciones del organismo, en particular respecto a:

- Supervisión, control y sanción de las entidades financieras.
- Certificación de profesionales y auditores externos.
- Autorización para la constitución y operación de nuevas entidades financieras.
- Investigación para detectar operaciones con recursos de procedencia ilícita.
- Registro de centros cambiarios y transmisores de dinero.
- Autorización de programas de autocorrección sobre riesgos.
- Determinación de los índices de capitalización mínimos para las Instituciones de Crédito.
- Vigilancia sobre la liquidez y solvencia en las entidades financieras.

La reforma financiera de 2014 se enfocó hacia una mayor inclusión financiera y promoción de la educación financiera, por medio del Consejo Nacional de Inclusión Financiera —cuyas funciones son establecer los lineamientos de la Política Nacional de Inclusión Financiera y sus metas, proponer programas y criterios en materia federal, regional, estatal y municipal, y coordinar sus acciones con otras entidades públicas— y el Comité de Educación Financiera con los objetivos de preparar la Estrategia Nacional de Educación Financiera, y las acciones, políticas y programas para su operación.

Después de la Reforma Financiera de 2014, el cambio más significativo ha sido con la Ley Fintech. En Normatividad Bancaria 2015 (Editorial Pearson), se abordaron los cambios de la Reforma de 2014 y sus implicaciones, con una mirada histórica y a la vez prospectiva, a parir de las acciones posteriores a la publicación de la reforma.

¿En el camino correcto?

El reporte Termómetro Fintech (2019) cita el evento "Fintech Summit 2019", organizado por Google México, en el que los emprendedores que participaron concordaron que la Ley Fintech representa un "arma de doble filo", argumentando que el tono del gobierno sobre ella ha ido cambiando. Según ellos, el "espíritu" con el que la regulación fue creada y sustentada (promover la innovación e inclusión financiera) ha ido desapareciendo con las disposiciones secundarias y las circulares, dando pie a una gran carga regulatoria que muchas empresas no van a poder cumplir, e inhibiendo, por lo tanto, la innovación.

Lo que comenzó como una respuesta a la crisis financiera de 2008, así como a las limitaciones que ofrece la banca tradicional, ha hecho que las fintechs se presenten como una opción

más accesible y rápida que está promoviendo un cambio sin retorno, en el que las pequeñas y medianas empresas pueden obtener los beneficios en el corto plazo que siempre han buscado y así lograr una mayor inclusión financiera.

Las fintechs han encontrado en México un terreno fértil, toda vez que las opciones de productos financieros benefician a empresas que antes no tenían acceso y posicionan a nuestro país como líder en América Latina; sin embargo, su universo está en constante movimiento.

Aunque hoy México es el país de América Latina con un mayor desarrollo fintech, la regulación aprobada en 2018 podría frenar el crecimiento, como plantea la investigación de Endeavor México, Santander, la Embajada Británica, Finnovista y Google, pero, a la vez, consolidar el ecosistema por la depuración que podría hacerse para crecer con bases firmes.

Hay que tener claro que la Ley Fintech en realidad es una ley de ITF para empresas de giros específicos (monedas virtuales, *crowdfunding* y medios de pago); todos los demás servicios financieros pueden ser tecnificados y convertir a la empresa en una empresa fintech en cualquiera de sus estructuras regulatorias.

12. Contexto: antes y después de la Ley Fintech

El 1 de marzo de 2018, la Cámara de Diputados aprobó en lo general y en lo particular el dictamen que expide la Ley para Regular las Instituciones de Tecnología Financiera, o Ley Fintech. La ley está conformada por 145 artículos divididos en siete títulos y tiene por objeto regular los servicios financieros que prestan las Instituciones de Tecnología Financiera (ITF), así como su organización, operación y funcionamiento.

Partió de cinco principios: fomentar la inclusión financiera en todo el país, proteger al consumidor, dar estabilidad financiera, promover la sana competencia, así como prevenir y mitigar el riesgo de lavado de dinero y de financiamiento al terrorismo. En esta parte se presentan el panorama y los condicionantes que fueron considerados en el marco de esos principios para la presentación de la ley; también se expone el contexto inmediato a su aprobación.

La intención es mostrar de dónde surgió la legislación para entender el alcance planteado, su contexto nacional (e internacional si tomamos en cuenta las partes anteriores) y las acciones que se han hecho ya con una Ley Fintech como referente, como las disposiciones (y su porqué) del Banco de México en cuanto a los activos virtuales, las disposiciones de carácter general que habrán de aprobarse en 2020, la relativas a las Interfaces de Programación de Aplicaciones informáticas estandarizadas y las aplicables a las Instituciones de Fondos de Pago Electrónico.

Inclusión financiera

De acuerdo con la Encuesta Nacional de Inclusión Financiera,[9] de 2012 a 2015 se incluyó financieramente a 12.7 millones de adultos; esto significó que la población que posee al menos un producto financiero pasó de 39 a 52 millones; es decir, anualmente se incorporaron en promedio casi cuatro millones de adultos al sistema financiero formal en el periodo referido.

[9] Encuesta Nacional de Inclusión Financiera 8, 2017, disponible en <http://www.cnbv.gob.mx/Inclusi%C3%B3n/Documents/Reportes%20de%20IF/Reporte%20de%20Inclusion%20Financiera%207.pdf>, consultado el 28 de noviembre de 2019.

El diagnóstico general revela que se ha incrementado la inclusión financiera, tanto por parte del acceso como de la demanda. Los indicadores de acceso son el número de sucursales, cajeros automáticos o terminales punto de venta, entre otros.

La inclusión financiera se ha definido como el acceso a servicios financieros (crédito, ahorro, seguros, servicios de pago y transferencias) formales y de calidad, y su uso por parte de hogares y empresas, bajo un marco de estabilidad financiera para el sistema y los usuarios. Los objetivos que se le han encomendado apoyan el desarrollo económico.

En la edición 2017 de *Normatividad Bancaria. Inclusión Financiera y Desarrollo*,[10] se abordó el tema que, desde la perspectiva del Center for Global Development, tiene las siguientes contribuciones:

- Facilitar el sistema de pagos y transacciones (central en economías modernas).
- Permitir que familias y empresas tomen decisiones intertemporales (y no sólo de corto plazo) para incentivar el ahorro y eliminar la restricción del autofinanciamiento, lo que genera incentivos para inversiones productivas.
- Permitir mejorar el manejo de riesgos a las poblaciones de bajo ingreso (seguro de salud, microseguros que protegen contra desastres naturales que afectan las cosechas, las propiedades y otras fuentes de ingreso y riqueza).

El tema se abordó porque ha aumentado su importancia en la agenda global para el crecimiento sostenible de largo plazo, debido a la mayor evidencia sobre los nexos que existen entre la inclusión financiera y las oportunidades para reducir la vulnerabilidad de los hogares de menores ingresos y la desigualdad de los países, así como del potencial que ofrecen nuevas tecnologías y modelos de negocio en el mercado para superar los obstáculos que han restringido el acceso a los servicios financieros y su uso para la mayor parte de la población.[11]

En la Encuesta Nacional de Inclusión Financiera (ENIF 2017), se retoman los ejes de la Política Nacional de Inclusión Financiera, de la cual, para efecto de esta obra, retomamos el *Eje 2: Uso de innovaciones tecnológicas para la inclusión financiera*, cuyo objetivo es aprovechar las innovaciones tecnológicas para ampliar el uso de los productos y servicios financieros dentro de un marco regulatorio que brinde seguridad a todos los participantes del sistema financiero. Los elementos que componen este eje son:

1. Revisión permanente del marco regulatorio para permitir la entrada de innovaciones tecnológicas, procurando la estabilidad y seguridad del sistema financiero.
2. Aprovechamiento del acceso a las nuevas tecnologías que permite la reforma en telecomunicaciones para conectar a la población actualmente excluida del sistema financiero.
3. Establecimiento de mecanismos de coordinación entre autoridades, gremios de los sectores financiero y emprendedor de aplicaciones tecnológicas financieras (fintech) para fomentar el desarrollo de soluciones de inclusión fi-

[10] *Normatividad Bancaria. Incusión Financiera y Desarrollo*, México, Grañén Porrúa, 2017.

[11] Fernando de Olloqui, Gabriela Andrade y Diego Herrera, "Inclusión financiera en América Latina y el Caribe. Coyuntura actual y desafíos para los próximos años", documento para discusión núm. IDP-DP385, Banco Interamericano de Desarrollo, junio de 2015.

nanciera, viables y seguras para el mercado mexicano.
4. Promoción de mecanismos que reduzcan el uso de efectivo, como banca móvil, cartera electrónica, remesas digitales, entre otros, así como la entrada de nuevos modelos de negocio como el *blockchain*, considerando medidas de regulación y supervisión que fortalezcan la seguridad informática (ciberseguridad) en su adopción.
5. Coordinación con la SCT, el Ifetel y empresas de telecomunicaciones para ampliar la oferta de servicios financieros en zonas objetivo mediante teléfonos móviles.
6. Desarrollo de una plataforma abierta para facilitar la interconectividad de los servicios financieros digitales.
7. Establecimiento de programas de financiamiento con la banca de desarrollo para apoyar a los intermediarios financieros en la adopción de nuevas tecnologías.

La ENIF 2017 demuestra que, de junio de 2015 a junio de 2016, la infraestructura financiera del país creció 17.8 por ciento, conformada por 16,546 sucursales, lo que implicó un crecimiento menor a 1 por ciento; ofrece cobertura en 50 por ciento de municipios donde habitan 92 por ciento de los adultos del país; 38,285 corresponsales bancarios, lo que representó una variación de 16.1 por ciento respecto al mismo periodo —dados los cambios en los reportes de corresponsales—, con al menos un corresponsal en 65 por ciento de municipios del país, donde vive 95 por ciento de los adultos; el número de cajeros ascendió a 47,743, lo que significó un incremento de 7.5 por ciento, con una cobertura de 57 por ciento de municipios, donde habita 94 por ciento de adultos; y el número de terminales punto de venta (TPV) pasó de 751,669 a 893,244 para los mismos periodos de referencia, lo que lo apuntala como el canal que más creció en ese último año, donde en 68 por ciento de municipios hay al menos una TPV; en dichos municipios vive 96 por ciento de los adultos.

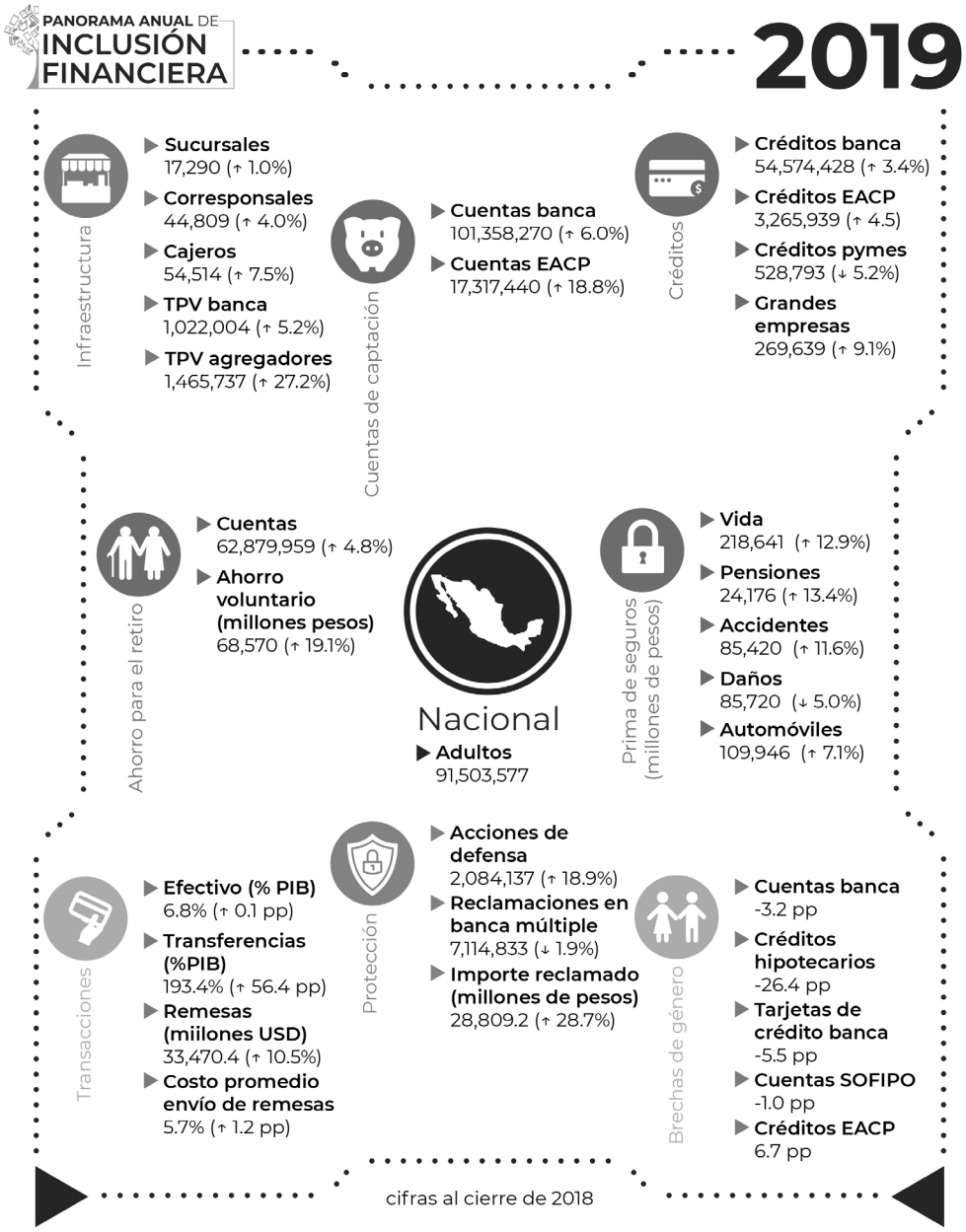
Este aumento de la infraestructura financiera, sobre todo de las TPV que representó el canal con mayor crecimiento (18.8 por ciento), nos sirve como parámetro para la introducción de empresas fintech. Por ejemplo, en este sector se encuentra Clip (la solución para aceptar pagos con tarjetas de crédito y débito en dispositivos móviles), que está conectada a más de 18 mil puntos de venta en todo México.

Por lo que respecta a la banca electrónica, su uso está por debajo del potencial esperado. De acuerdo con datos de la ENIF 2017, existen 29 millones de adultos que tienen un teléfono celular, pero que no tienen una cuenta. Un estudio de McKinsey Global Institute[12] indica que un mayor uso de servicios financieros digitales podría aumentar el PIB de México en 90 mil millones de dólares para el año 2056.

La encuesta también se enfocó en los retos, en los cuales se establece que, si bien México ha avanzado en materia de inclusión financiera, aún tiene pendientes en infraestructura financiera, adquisición y uso limitado de los productos y servicios financieros, falta de conocimiento del sistema financiero y falta de información para medir el impacto de acciones de inclusión financiera, por lo que debe expandirse la infraestructura y la oferta de productos y servicios financieros a una mayor parte de la población, ya que la infraestructura y la oferta se concentran en las zonas urbanas y en las cabeceras municipales.

[12] Citado en la ENIF 2017.

GRÁFICO 3.



Fuente: Panorama anual de Inclusión Financiera 2019. CNBV.

CUADRO 10.
Principales indicadores

Indicador	Dic 2016	Dic 2017	Dic 2018
Infraestructura			
Puntos de acceso (Puntos de acceso en donde se pueden hacer retiros o depósitos por cada 10,000 adultos)	12.0	12.4	13.0
Cobertura de infraestructura por unidad administrativa (Porcentaje de municipios con al menos un punto de acceso)	73.3%	75.4%	76.6%
Cobertura de infraestructura a nivel demográfico (Porcentaje de la población adulta que habita en un municipio con al menos un punto de acceso)	97.8%	98.1%	98.2%
Cobertura georreferenciada (Porcentaje de la población que habita en localidades[1] en un radio de 4km alrededor de al menos un punto de acceso)	N/A	87.0%	87.3%
Tenencia de productos			
Productos de captación (Número de contratos de captación por cada 10 mil adultos)	12,858	12,212	12,970
Productos de crédito (Número de contratos de crédito por cada 10 mil adultos)	6,069	6,197	6,321
Cuentas de ahorro para el retiro (Número de cuentas de cada trabajador que son administradas por las Afore por cada 10,000 adultos)	6,443	6,651	6,872
Prima per cápita del mercado de seguros (Prima per cápita del mercado de seguros en pesos mexicanos. Incluye seguros de accidentes y enfermedades, daños, pensiones y vida)	$ 3,627	$ 3,921	$ 4,200
Frecuencia de uso			
Pagos en comercios a través de TPV (Número de transacciones que se llevan a cabo en las terminales punto de venta de comercios, ya sea con tarjetas de crédito o débito por cada 10,000 adultos en el mes de referencia)	19,508	20,741	25,642
Operaciones en cajeros automáticos (Número de operaciones en cajeros automáticos por cada 10,000 adultos en el mes de referencia)	18,264	22,819	23,380
Transferencias electrónicas (Número de transferencias electrónicas por cada 10,000 adultos en el mes de referencia)	32,106	34,756	35,801
Protección al consumidor			
Acciones de atención de la Condusef (Número de asesorías, controversias, dictámenes, arbitrajes y solicitudes de defensoría que la Condusef realiza por cada 10,000 adultos)	187	194	228

[1] Se consideran aquellas localidades con más de 20 habitantes

Fuente: Panorama anual de Inclusión Financiera 2019. CNBV.

Como resultado del II Foro Internacional de Inclusión Financiera, realizado en junio de 2016, se planteó que la regulación no debía inhibir la innovación, por lo que los reguladores debían comprender la innovación y reformar la regulación, si fuese el caso, de acuerdo con los nuevos paradigmas.

En este sentido, la tecnología representa un potencial importante para ampliar y profun-

> dizar la inclusión financiera, especialmente en las áreas rurales y para la atención de grupos tradicionalmente excluidos. Ello contribuirá a fomentar el uso de nuevos canales de acceso y la introducción de nuevos productos que satisfagan las necesidades del mercado. Por otra parte, la educación financiera debe contribuir a una inclusión de calidad, más profunda. No sólo se trata de que una mayor proporción de la población tenga acceso a servicios financieros, sino de que tenga acceso a instrumentos útiles y que le den un mejor uso, y responsable, para contribuir a un mayor bienestar social y financiero.[13]

El panorama de 2019 puede apreciarse en el gráfico y el cuadro. En el cuadro, puede verse el avance en el tema. Para el autor es importante tener los datos de 2017, ya que, como se mencionó, son el contexto en el que se dio la Ley Fintech, y muy útiles para ver el avance que se registra en 2019 en el marco de un debate sobre una nueva regulación, la divulgación del tema en los medios de comunicación, el aumento en el número de participantes en el sistema financiero mexicano, así como una mayor oferta de productos y servicios, ya sea por los nuevos participantes, por los tradicionales o por una combinación de ambos en el marco general de la transformación digital.

Protección al consumidor

Según la ENIF 2017, el número de acciones de defensa, al cierre del primer semestre de 2016, se incrementaron 10 por ciento respecto al cierre del primer semestre de 2015, al pasar de 775 mil a poco más de 850 mil. Asimismo, el indicador demográfico aumentó 8 por ciento, alcanzando 95.7 acciones de defensa por cada 10 mil adultos.

Del total de acciones de defensa, 85 por ciento se relacionan con asesorías y consultas. Los principales motivos de las asesorías son: emisión del reporte de crédito especial, orientación sobre el funcionamiento de productos y servicios financieros, servicios que ofrece la Condusef, funcionamiento de productos y servicios no financieros, y consumos no reconocidos, entre otros. El restante 15 por ciento tiene que ver con reclamaciones presentadas por los usuarios en contra de alguna institución financiera.

Las acciones de defensa que se presentan ante la Condusef corresponden, en su mayoría, a sociedades de información crediticia (SIC), de usuarios que solicitan asesoría en la emisión de su reporte de crédito especial; bancos, con asuntos principalmente en materia de tarjeta de crédito o débito; el resto les corresponde a aseguradoras, afores, base de datos nacional del sistema de ahorro para el retiro (Procesar), sofomes reguladas y no reguladas, y a otros, que incluye el sector bursátil, fianzas, entidades de ahorro y crédito popular (EACP), organizaciones y actividades auxiliares del crédito (OAAC) y banca de desarrollo, entre otros.

De acuerdo con el Boletín de Sanciones de la CNBV,[14] durante el primer semestre de 2017, se sancionó a 4,242 conductas a través de 3,858 resoluciones de sanción. De dichas conductas, destacan los incumplimientos en la entrega de información en tiempo y forma, informalidades y carencias en los re-

[13] Conclusiones del II Foro Internacional de Inclusión Financiera.

[14] Boletín núm. 10, enero-junio de 2017, disponible en <http://www.cnbv.gob.mx/CNBV/Sanciones/Boletin_de_Sanciones_ene-jun_2017.pdf>, consultado el 28 de noviembre de 2017.

portes de operaciones relevantes y de operaciones con divisas, así como la detección de fallas y deficiencias en los controles para la identificación de clientes; dichas conductas son recurrentes en gran parte de los sectores supervisados. Por monto, las 10 principales conductas suman 83.8 por ciento de las multas[15] impuestas, destacando las violaciones a las disposiciones en materia de prevención de lavado de dinero (PLD), las fallas en procesos internos y la detección de operaciones no permitidas o sin autorización. Estos tres rubros concentran 53.6 por ciento de las multas impuestas durante el primer semestre del año.[16]

En el "Panorama Anual de Inclusión Financiera 2019" (CNBV, 2019), en el apartado de Protección al consumidor, se expone que, de 2017 a 2018, el número de acciones de defensa de la Condusef se incrementó 19 por ciento, es decir, 330 mil acciones más, mientras que el número de asesorías se incrementó 20 por ciento y las reclamaciones, 12 por ciento. De las acciones de defensa, 54 por ciento fueron asesorías técnico-jurídicas de información básica, las cuales ayudan al usuario a entender el tipo de producto o servicio que adquirió, las características y forma de operación de éstos, así como los derechos y obligaciones que adquiere.

GRÁFICA 10.

Instituciones financieras que supervisó la Condusef en 2018	Número de acciones de defensa en 2018	Acciones de defensa por cada 10 mil adultos en 2018	Crecimiento en el último año (2018 vs 2017)
3,004	2,084,137	228	19%

■ Evolución histórica de las acciones de defensa

Fuente: Anuario Estadístico Condusef, 2018

La Comisión Nacional Bancaria y de Valores (CNBV), en el periodo de enero a diciembre de 2018, reportó 7'114,833 reclamaciones por un monto de 28,809.2 millones de pesos. Con respecto al mismo periodo del año anterior, se presentaron 136,466 reclamaciones menos, mientras que el monto reclamado aumentó 6,420.1 millones de pe-

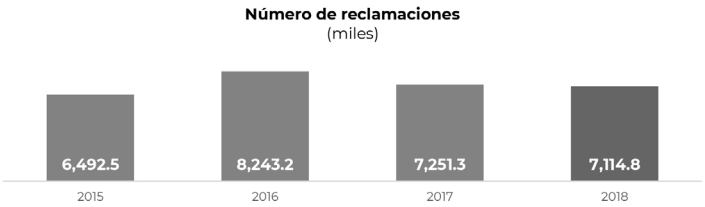
[15] La presunción y/o detección de conductas infractoras da inicio a procedimientos de sanción que pueden concluir en multas, amonestaciones, cancelaciones de registros, inhabilitaciones, suspensión de operaciones o bien, en revocaciones de las autorizaciones para operar.

[16] De los 23 sectores que resultaron sancionados durante el primer semestre del año, los primeros cinco —sofom ENR, centros cambiarios, instituciones de banca múltiple, socap y uniones de crédito— concentran 95.5 por ciento de las multas y amonestaciones impuestas en número. Las Sofom ENR ocupan el primer lugar, con 1,723 multas y amonestaciones a 704 instituciones, seguidas de 1,632 a 478 centros cambiarios y 163 a 42 instituciones de banca múltiple.

GRÁFICA 11.

Número de reclamaciones en 2018	Porcentaje de reclamaciones concluidas a favor del cliente en 2018	Importe reclamado en 2018 (millones de pesos)	Porcentaje del importe de reclamaciones concluidas abonado al cliente en 2018
7,114,833	**74%**	**28,809.2**	**45%**

■ Evolución del número de reclamaciones



Fuente: CNBV, 2015-2018

sos. En favor del cliente se resolvieron seis de cada 10 reclamaciones presentadas, esto es, 10,294.9 millones de pesos abonados al usuario. Las tarjetas de débito concentraron 56 por ciento de las reclamaciones concluidas, por lo que resultaron favorables para el cliente tres de cada cuatro, por lo que 5,481.5 millones de pesos fueron abonados al cliente. La institución con mayor número de reclamaciones fue BBVA Bancomer, con 1'181,674 reclamaciones concluidas, de las cuales, 58 por ciento resultaron favorables para el cliente.

Si bien, la ley se aprobó en marzo y entró en vigor en septiembre, los datos que se presentan (los disponibles en el momento de la elaboración de este trabajo) se dan en un contexto diferente al que determinó el actuar antes de 2018. De ahí la importancia de tenerlos presentes para considerar su evolución, tomando en cuenta los elementos que se suman ya con la ley en pleno uso.

Estabilidad financiera

La nueva realidad impone tener el foco en la estabilidad. Como hemos visto en apartados anteriores, la inclusión de nuevos productos, servicios, actores, tecnología, etcétera ha influido en el entorno financiero, cambiando las reglas y redefiniendo prioridades, por ejemplo, en los riesgos.

De hecho, aunque continúen vigentes las definiciones de estabilidad financiera, los argumentos han variado, si no del todo, sí por los elementos actuales de los que ya el Consejo de Estabilidad Financiera, el Fondo Monetario Internacional y el Banco Mundial daban cuenta en octubre de 2011 en un informe sobre estabilidad financiera "con temas de particular interés para las economías emergentes".

Estos organismos internacionales consideraban la creciente proliferación y desarrollo de instituciones financieras ("que prestan y toman depósitos a muy pequeña escala a personas y pequeñas-medianas empresas"), su rápido crecimiento, la estrecha conexión con el resto del sistema financiero (en especial los bancos), además de un marco regulatorio inadecuado y unos instrumentos de supervisión y capacidad limitados, situaciones que "pueden tener consecuencias muy adversas en la estabilidad financiera de estas economías".

En 2013, el Banco Mundial (2013), en un estudio sobre estrategias de inclusión fi-

nanciera,[17] explicó cómo las estrategias de inclusión financiera no debían perder de vista la estabilidad financiera, la integridad y el comportamiento de mercado, debido a que los nuevos actores comenzaban a aumentar su participación, pero en un marco regulatorio inexistente o mucho más laxo que las instituciones bancarias. Ya se tenía muy en cuenta que algunas políticas de inclusión financiera demasiado audaces —las hipotecas subprime para convertir en dueñas de sus casas a las familias— podrían tener efectos muy negativos, al presentarse tensiones entre la estabilidad financiera y un mayor acceso financiero de la población.[18]

B. McLean y J. Nocera (2010) establecieron que, "para garantizar la estabilidad del sistema financiero, no sólo es necesario proveer de un mayor acceso financiero a la población, sino que ésta use los productos y servicios financieros con frecuencia y de forma diversa, porque las fricciones de información relacionadas con la falta de confianza y carencia de conocimientos financieros pueden dar lugar a una autoexclusión de los mercados financieros, aunque se tenga acceso. Entre las medidas que deben acompañar a un mayor acceso y uso de los productos financieros para que éstos no pongan en riesgo la estabilidad, está contar con regulaciones prudenciales y considerar el riesgo sistémico".

Dada la importancia de la estabilidad financiera, desde 2007 el Banco de México publica un reporte sobre el sistema, su estabilidad y sus riesgos. En el "Reporte de Estabilidad Financiera" de diciembre de 2019,[19] reconoció que la economía mexicana sigue enfrentando un entorno complejo, por lo que puso particular atención en cuatro riesgos macrofinancieros que se perciben sobre el sistema financiero: una importante desaceleración del crecimiento global, la adopción de mayores medidas proteccionistas a nivel mundial y crecientes riesgos geopolíticos, volatilidad en los mercados financieros internacionales con recomposición de flujos hacia activos de menor riesgo, y una menor inversión y menor crecimiento en la economía nacional.

(Sin duda, como lo hemos visto en apartados anteriores, los riesgos macrofinancieros con sus peculiaridades han determinado las acciones, incluso el rumbo de los participantes de los sistemas financieros de los países y, por ende, del internacional).

Siguiendo con el reporte del Banco de México, también se analizaron los riesgos cibernéticos e informáticos, de los cuales se apuntó: "Se encuentran dentro de los más relevantes que enfrenta el sistema financiero por la creciente importancia de las tecnologías de información para su operación, aumentando el alcance potencial de este tipo de ataques". El Banco de México considera el análisis de los riesgos que impone el cambio climático a los participantes en el sistema financiero. "Los riesgos relacionados con el clima y el medio ambiente pueden ser una fuente importante de pérdidas para el sistema financiero y, en casos extremos, podrían tener consecuencias sistémicas". De hecho, los riesgos climáticos ya son considerados en el ranking de los riesgos del sector, ocupando un lugar preponderante.

---

[17] Banco Mundial (2013), *Global Financial Development Report 2014*, Washington, D.C., disponible en <http://siteresources.worldbank.org/EXTGLOBALFINREPORT/Resources/8816096-1361888425203/9062080-1364927957721/GFDR-2014_Complete_Report.pdf>, consultado el 27 de abril de 2017.

[18] B. McLean y J. Nocera, *All the Devils Are Here: Unmasking the Men Who Bankrupted the World*, Penguin, 2010.

[19] Véase <https://www.banxico.org.mx/publicaciones-y-prensa/reportes-sobre-el-sistema-financiero/%7BB8B8764-7345-2016-96F1-E1DA4CFF8BBA%7D.pdf>.

La estabilidad financiera, desde todas las ópticas y perspectivas, es determinante en el presente y futuro. Las medidas que se toman al respecto, como hemos visto, van sumando a los nuevos elementos del entorno.

Sana competencia

A la inclusión financiera y estabilidad financiera se suma la competencia, que tiene un gran impacto en logro de los objetivos encaminados al crecimiento de las economías, en las que el sistema financiero es de gran relevancia, no sólo por su contribución directa a la producción, la inversión y el empleo, sino también por el impacto que tiene en el bienestar de los consumidores y en la eficiencia del resto de los sectores de la economía.

En ese contexto, en México, y luego de la aprobación de la Reforma Financiera de 2014, la Comisión Federal de Competencia Económica (Cofece) realizó un trabajo de investigación (julio de 2014) para presentar un diagnóstico sobre las causas por las cuales un mercado pudiera estar funcionando de forma inadecuada, en términos de eficiencia, competencia y bienestar de los consumidores.

Los resultados del estudio[20] de la Cofece para fomentar la competencia y libre concurrencia en cinco aspectos fundamentales detectó cinco áreas de oportunidad:

1. **Evitar desplazamientos o que se impida el acceso a competidores a los mercados financieros.** Recomendaciones orientadas a que la regulación promueva aún más que los agentes compartan y otorguen acceso a las redes e infraestructura a sus competidores y a que todos los participantes del sector puedan acceder a la misma información.
2. **Reducir riesgos de efectos coordinados anticompetitivos entre competidores.** En el sector financiero mexicano, existen condiciones que facilitan la coordinación de los agentes económicos, lo que puede generar efectos anticompetitivos. Estas recomendaciones se encaminan a inhibir estas conductas a fin de lograr reducciones de precios y mejorar la calidad de los servicios.
3. **Reducir barreras a la competencia para quienes ya están en el sector, pero que les cuesta trabajo competir.** Las recomendaciones se centran fundamentalmente en mejoras al marco normativo para incrementar el número de participantes en los mercados.
4. **Eliminar restricciones que hacen que el funcionamiento de los mercados no sea eficiente.** Las recomendaciones en este rubro buscan mejorar la información en los mercados financieros para facilitar la toma de decisiones y perfeccionar la regulación o intervención del Estado a fin de lograr mayor eficiencia en los mercados financieros.
5. **Aumentar la efectividad de investigación y de sanción de la autoridad de competencia sobre posibles conductas violatorias de la Ley Federal de Competencia Económica.**

[20] "Trabajo de investigación y recomendaciones sobre las condiciones de competencia del sector financiero", Cofece, sisponible en <https://www.cofece.mx/cofece/images/banners/sfinanciero/Resumen_Ejecutivo_Trabajo_de_Investigacion_del_Sistema_Financiero.pdf>, consultado el 12 de noviembre de 2017.

Se busca mejorar el monitoreo, la información y el análisis de los mercados para que la Cofece esté en posibilidad de cumplir con eficacia su mandato constitucional en este sector de la economía.

Entre las recomendaciones de la Cofece destacan (para efectos del tema de esta obra):

- Asegurar que las cargas operativas y de supervisión sean proporcionales a cada tipo de institución, entre otros, conforme a su perfil de riesgo.
- Establecer la obligación a los operadores de telecomunicaciones de proveer el servicio de transferencias con teléfonos móviles a través de mensajes cortos a cualquier procesador o intermediario financiero que lo solicite.
- Propiciar el desarrollo y, en su caso, regulación de plataformas electrónicas para inversión de capital y de financiamiento de proyectos productivos, donde se publiquen las necesidades de capital y financiamiento de Mipymes y se reciban ofertas de instituciones financieras que ofrezcan financiamiento y coinversión de sus proyectos.

En 2017, en el marco de la discusión en el Congreso de la Ley para Regular las Instituciones de Tecnología Financiera, la Cofece emitió una serie de opiniones sobre esta regulación. Para fomentar una mayor competencia, pidió a los legisladores evitar una regulación excesiva y no obstaculizar el desarrollo del sector. Argumentó que, si bien la ley busca proteger a los consumidores y la estabilidad del sistema financiero, no debe obstaculizar el desarrollo de las fintechs.

También exhortó a que se estableciera con claridad que los usuarios son dueños de sus datos; por lo tanto, pueden transferirlos a otra institución si es que así lo deciden. De igual forma, sugirió que se obligue a los bancos a ofrecer servicios bancarios a este tipo de instituciones.

Entre las mejoras a la Ley Fintech, derivadas de la opinión emitida por la Cofece, destacan las relacionadas con facilitar a las fintechs el acceso a la información de los usuarios, que actualmente está en posesión de las entidades financieras, por ser ellas quienes históricamente han participado en este mercado. (Este tema se aborda en otro apartado).

En el entorno general del sistema financiero, en 2018 la Cofece inició una investigación para determinar la posible existencia de barreras a la competencia, así como de posibles insumos esenciales en el mercado de sistema de pagos, cuyo procesamiento involucre una cámara de compensación para pagos con tarjetas de crédito o de débito, ya que se encontraron elementos que hacen suponer la falta de condiciones de competencia efectiva en dicho mercado, debido a la posible existencia de barreras a la competencia o insumos esenciales (elemento o conjunto de éstos que resultan indispensables para la producción o prestación de bienes y servicios y tienen la característica de ser insustituibles). "De existir problemas de competencia económica en el mercado investigado, se estaría afectando la bancarización y la inclusión financiera, lo cual resta potencial crecimiento al país".

En el análisis por sectores del Plan Estratégico 2018-2021, la Cofece apuntó que, al cierre del tercer trimestre de 2017, el sector de servicios financieros y seguros representó 4 por ciento del PIB nacional y tuvo un crecimiento de 8.2 por ciento en términos reales con respecto al mismo periodo del año anterior. Sin embargo, al cierre de 2016, 70 por ciento de los activos totales del sector, así como 71 por ciento de los pasivos totales, se

concentraron en cinco competidores principales. Además, el sector presenta retos de inclusión financiera, por lo que requiere de un seguimiento que propicie mejores condiciones de competencia de forma que se disminuyan los precios y se propicie el acceso de la sociedad a productos financieros de calidad.

"Un sistema financiero que opere de manera eficiente y que sea competitivo favorece el flujo de financiamiento a los proyectos más rentables y productivos, amplía y mejora las opciones de los ahorradores y disminuye los costos de transacción en el resto de los sectores de la economía".[21]

Durante el taller "Competencia económica en el marco del Plan Nacional de Desarrollo", la titular de la Cofece, Alejandra Palacios Prieto, cuestionó a autoridades y participantes del sistema financiero respecto a las acciones para que haya competencia. Enfatizó que el proyecto CoDi solamente ataca a un pedazo de lo que es la conformación del sistema financiero, que es el sistema de pagos, pero deja de lado otros aspectos que deben ser abordados para una mayor competencia y beneficios para los usuarios, como el mercado del crédito o aspectos como las comisiones bancarias.[22]

En el 2017, la banca comercial obtuvo 108 mil millones de pesos por cobro de comisiones netas (8 por ciento más que en 2016). En el primer trimestre de 2018 se registraron 85,698 reclamaciones por cobro de comisiones no reconocidas, según la Condusef.

CUADRO 11.
Comisiónes

			Productos con comisiones	Comisiones registradas		Comisiones promedio por producto
		Total	1,299	5,310	100%	4
35 CONECPTOS DE COMISIÓN	ACTIVAS	Crédito Hipotecario	289	1,316	3,073 (58%)	5
		Tarjeta de Crédito	170	1,056		6
		Crédito simple	84	179		2
		Crédito de auto	63	216		3
		Crédito personal	51	117		2
		Crédito en cuenta corriente	46	116		3
		Arrendamiento financiero	15	34		2
		Factoraje financiero	12	19		2
		Otros créditos	10	20		-
	PASIVAS	Depósito	399	1,700	2,059 (39%)	4
		PRLV	76	125		2
		Nómina	30	138		5
		Básicas	28	96		3
	SERVICIOS	Terminal Punto de venta	14	94	178 (3%)	7
		Fideicomisos	4	50		13
		Cajas de seguridad	4	21		5
		Compra -venta divisas	2	11		6
		Administración de valores	2	2		1

Fuente: Condusef.

[21] Véase <https://www.cofece.mx/wp-content/uploads/2018/02/pe_2018-2021.pdf>.

[22] "Tecnología, clave para la inclusión y competencia en el sistema financiero", disponible en <https://www.eleconomista.com.mx/sectorfinanciero/Tecnologia-clave-para-la-inclusion-y-competencia-en-el-sistema-financiero-20190529-0003.html>.

¿Qué sigue en cuanto a la competencia? Un mayor número de participantes, de entrada, plantea opciones; una oferta en cantidad y calidad ofrece alternativas; y un marco para regular la participación estableciendo estándares mínimos y obligaciones da certidumbre. Lo que sigue es, por lo tanto, monitorear que la competencia cumpla con el objetivo primario de inclusión y estabilidad financiera.

Prevención y mitigación del riesgo de lavado de dinero y financiamiento al terrorismo

El lavado de dinero y el financiamiento al terrorismo (LD/FT) pueden menoscabar la integridad de las instituciones y los sistemas financieros, desalentar la inversión extranjera y distorsionar los flujos internacionales de capital. Para evitar estos ilícitos, el Grupo de Acción Financiera sobre el Blanqueo de Capitales (GAFI) elabora normas y recomendaciones de alcance mundial que constituyen un marco básico y de aplicación universal, entre ellas la elaboración de una Evaluación Nacional de Riesgos (ENR), que debe actualizarse cada tres años con los ajustes de los ejercicios anteriores, la evolución de los métodos delictivos y los resultados de las estrategias públicas de prevención y combate contra el LD/FT.

Una ENR permite optimizar el uso de sus recursos y capacidades para privilegiar la atención de las áreas que resultan prioritarias para la seguridad y estabilidad del país, así como dar cumplimiento a lo dispuesto en la Recomendación 1 de los estándares internacionales sobre la lucha contra el LD, FT y FPADM del GAFI, conocidas como las 40 recomendaciones.

Los estándares indican que los países deben identificar y evaluar cuáles son los riesgos que enfrentan en relación con dichas conductas a fin de entenderlos y orientar los recursos nacionales necesarios para su adecuada prevención y mitigación. Asimismo, los países también deben contar con políticas públicas derivadas de un análisis integral de riesgo que parte de la Recomendación 1 del GAFI.

A finales de 2013, la Secretaría de Hacienda y Crédito Público (SHCP) resolvió realizar una ENR. Durante la XXIX Reunión Plenaria del GAFI y el GAFILAT, celebrada del 1 al 3 de noviembre, dichos organismos internacionales coincidieron en que México cuenta con un régimen maduro que incluye un marco legal e institucional adecuado, que se ha fortalecido significativamente en distintas áreas desde que el país fue evaluado por primera vez en 2008.

En 2017, nuestro país tiene el mismo nivel de cumplimiento que Canadá y Estados Unidos en la tabla de posiciones de la evaluación que se llevó a cabo bajo la coordinación del Fondo Monetario Internacional, conforme a las recomendaciones y la metodología de evaluación emitidas por el GAFI. Las áreas de oportunidad identificadas para México deberán ser incorporadas en los planes y programas de trabajo del gobierno federal y de las autoridades involucradas, así como por todos los sectores del sistema financiero regulados en la materia preventiva y por las actividades vulnerables.

El reporte aprobado en la reunión plenaria del GAFI y el GAFILAT concluye que, en México, las autoridades competentes, coordinadas por la SHCP, realizaron una ENR adecuada que les permite conocer cuáles son las principales amenazas, vulnerabilidades y consecuencias en la materia, de acuerdo con la definición que el GAFI

hace de estos conceptos,[23] y que, conforme a este conocimiento, se han adoptado las medidas necesarias para mitigar los riesgos.

En la ENR se identificó el riesgo de los sectores que componen el sistema financiero mexicano:

Sector	
Banca múltiple (las siete con mayor participación de mercado)	Riesgo alto
Casas de Bolsa	
Casas de Cambio	
Banca múltiple-comercial	
Banca múltiple-consumo	Riesgo medio-alto
Centros cambiarios	
Banca múltiple-inversión	
Transmisores de dinero	
Uniones de crédito	
Banca de desarrollo	Riesgo medio
Sociedades Cooperativas de Ahorro y préstamo	
Sociedades Financieras Populares	
Sociedades Operadoras de Inversión	

[23] Amenaza: Es una persona o grupo de personas, objeto o actividad con el potencial de dañar, por ejemplo, el Estado, la sociedad, la economía, etcétera. En el contexto de LD/FT, esto incluye criminales, grupos terroristas y sus facilitadores, sus recursos, así como actividades de LD/FT pasadas, presentes y futuras.

Vulnerabilidad: Comprende aquellas cosas que pueden explotarse por la amenaza o que pueden sustentar o facilitar sus actividades. En el contexto de la evaluación de riesgos de LD/FT, consiste en los factores que representan debilidades en los sistemas, controles o ciertas características de prevención de LD/FT de un país. También pueden incluir características de un sector particular, un producto financiero o tipo de servicio que los hace atractivos para propósitos de LD/FT.

Consecuencias: Se refieren al impacto o daño que el LD o FT puede causar, incluido el efecto de la actividad criminal o terrorista subyacente en los sistemas financieros e instituciones, así como en la economía y la sociedad de manera más general.

Sector	
Aseguradoras	Riesgo medio-bajo
Afores	
Sociedades Distribuidoras de Acciones de Sociedades de Inversión	
Fianzas	
Sofomes No Reguladas	
Almacenes Generales de Depósito	
Sofomes Reguladas	

A partir de la Ley Fintech, habrá que considerar a las ITF e identificar, de acuerdo con los parámetros de la ENR, el nivel de riesgo de éstas, considerando la capacidad de innovación y el grado de vulnerabilidad que implica —precisamente— la innovación.

Razón de ser

Como pudimos ver en los apartados anteriores, todo evoluciona y en los principios mencionados los resultados de las mediciones muestran diferencias, si no significativas sí notables; también pueden apreciarse más acciones con enfoque incluyente y de largo plazo.

En el *cuadro ¿Hacia una nueva arquitectura?*, se muestra el contenido de la ley y se plantea un mapa donde los elementos que lo conforman impactarán en el sistema financiero mexicano, modificando la arquitectura del mismo. Partimos de los "Principios" para mostrar los avances.

En *Fintech: Vientos del cambio. Normatividad bancaria* (Grañen Porrúa, 2019), se desarrollaron los puntos presentados en los apartados "A través de", "Alcance", "Sanciones", "Ente responsable" y "Autorización de modelos novedosos". También se abordaron los puntos del apartado "Reconocimiento", excepto los de la portabilidad de la información financiera de los usuarios a través de API (Interfaces de Programación de Aplicaciones) —debido a que no se contaba con la información; el proyecto de disposiciones se presentó hasta el 9 de diciembre de 2019— y las Disposiciones aplicables a las Instituciones de Fondos de Pago Electrónico —se dispuso del borrador el 22 de enero de 2020—, por lo que en esta obra se presenta para cerrar el círculo.

Además, aborda el tema de los activos virtuales debido a que las disposiciones relativas a éstos, emanadas del Banco de México, se dieron a conocer en marzo de 2019 cuando *Fintech: Vientos del cambio* ya estaba en circulación.

¿Hacia una nueva arquitectura?

Principios	Fomentar la inclusión financiera en todo el país. Protección al consumidor. Estabilidad financiera. Sana competencia. Prevención y mitigación del riesgo de lavado de dinero y financiamiento al terrorismo.
A través de	Innovación impulsada por la disponibilidad de la tecnología. Establecimiento de las condiciones para que las entidades financieras reguladas por ésta y otras leyes financieras puedan desarrollar innovaciones tecnológicas en espacios seguro.
Alcance	Acercar los servicios financieros a personas y sectores que tradicionalmente no han sido parte del sistema financiero, promoviendo una mayor educación financiera y asesoría sobre las nuevas alternativas. Establecer mecanismos de defensa y verificación de estándares mínimos. Establecer los lineamientos para la protección de datos personales, así como la obligación de completa divulgación a clientes e inversionistas del modelo de operación y factores de riesgos que podrían presentar las ITF. Establecer un marco general de autorización y operación supervisada a las ITF, imponiéndoles reglas prudenciales, proporcionales a los riesgos que representen en distintas materias, como son aquéllos financieros, operacionales, de mercado, tecnológicos (ciberseguridad), gobierno corporativo y reglas de contabilidad. Se busca que el mercado de tecnologías financieras se desarrolle con límites y montos máximos de operaciones, con el fin de evitar una desigualdad regulatoria con otros sectores financieros. Se busca un "piso parejo" y una competencia sana y equilibrada. Se permitirá mayor diversidad y nuevos canales de distribución de servicios financieros, así como la reducción de costos y mejora en la prestación de servicios. Se busca el correcto funcionamiento financiero y su integridad, estableciendo el marco regulatorio ya aceptado y probado, con estándares mínimos de identificación del cliente que permita prevenir este tipo de conductas.
Ente responsable	La supervisión del cumplimiento de lo dispuesto en esta ley y las disposiciones que de ella emanen corresponderá a la Comisión Nacional Bancaria y de Valores (CNBV) y al Banco de México (BM), en el ámbito de sus respectivas competencias, en términos de la ley y las demás disposiciones jurídicas aplicables. La Comisión Nacional de Seguros y Fianzas, la Comisión Nacional del Sistema de Ahorro para el Retiro y la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros tendrán las facultades que en el ámbito de sus respectivas competencias les confiera la ley y demás disposiciones jurídicas aplicables. Se crea un Comité Interinstitucional, una instancia colegiada de la CNBV integrada por servidores públicos de la Secretaría, del BM y de la CNBV.

Reconocimiento Se reconocen dos tipos de ITF: Instituciones de financiamiento colectivo (*crowdfunding*[1]): financiamiento colectivo de deuda, financiamiento colectivo de capital y financiamiento colectivo de copropiedad o regalías. Instituciones de fondos de pago electrónico. Realizarán servicios de emisión, administración, redención y transmisión de fondos de pago electrónico (*e-money*). Se propone que las ITF tengan la capacidad de operar con activos virtuales. Se plantea una figura (sandbox) para experimentar antes de legislar. Se permite la portabilidad de la información financiera de los usuarios. A través de API (Interfaces de Programación de Aplicaciones), los usuarios de servicios financieros podrán llevar su información financiera a donde ellos gusten y la podrán compartir con quienes ellos deseen. Esto forzará a las instituciones financieras a competir con base en precio y propuesta de valor, y no en tener a los clientes cautivos en sus plataformas.
Autorización de modelos novedosos Se crea el Grupo de Innovación Financiera

Desde la perspectiva del autor, considerando las tendencias en el ámbito global del sector financiero, la irrupción de la tecnología (que está forzando la transformación digital con todo lo que ésta implica), las innovaciones y los nuevos participantes están marcando la ruta y el tipo de vehículo para que el país pueda continuar su avance en un escenario de posibilidades, que no está exento de retos y riesgos en los que las partes involucradas tienen, a la vez que su razón de ser, una gran responsabilidad en términos de estabilidad e inclusión financiera.

Crowdfunding

Las instituciones de financiamiento colectivo, o crowdfunding, son un fenómeno enmarcado dentro de los movimientos colaborativos, que han adquirido una nueva dimensión gracias a los avances de las nuevas tecnologías. Estas instituciones brindan acceso a nuevas formas de financiamiento a segmentos de la población que normalmente no son atendidas por la entidades financieras y tradicionales. Pueden contemplarse tres formas de crowdfunding:

1. Colectivo de deuda. Son aquéllas en donde la institución pone en contacto directo a inversionistas con solicitantes que requieren de financiamiento, quienes posteriormente retornarán los recursos, generalmente, con el pago de un interés.
2. Colectivo de capital. Facilitan que los inversionistas aporten recursos a través de la institución para obtener participaciones de capital social de personas morales solicitantes que se promueven por este medio para posteriormente ser partícipes de las utilidades de dichas personas morales.
3. Colectivo de copropiedad o regalía. Los inversionistas aportan recursos a un proyecto, obteniendo una participación en un bien o derecho.[24]

[24] Esta figura ha sido regulada en países como Estados Unidos, Canadá, China, España, Italia, Francia, Reino Unido y Nueva Zelanda.

La irrupción del crowdfunding como mecanismo de intermediación financiera constituye un elemento disruptivo en un escenario donde la banca tradicional estaba acostumbrada a estar prácticamente sola. Las plataformas de crowdfunding han crecido de manera exponencial en algunas geografías, intermediando financiamiento a tipos de interés competitivos —acorde con el nivel de riesgo asociado— y, en muchos casos, ofreciendo una gestión del riesgo crediticio razonable dada la escasa información existente.[25] De acuerdo con BBVA Research,[26] las plataformas de crowdfunding financiero:

1. Son un lugar de encuentro y escaparate de proyectos.
2. Intermedian entre los inversores y los solicitantes de financiamiento.
3. Reducen los costos de transacción.
4. Evalúan el riesgo y/o clasifican los proyectos.
5. Gestionan los riesgos a través de la diversificación.
6. Asumen una responsabilidad muy limitada.
7. Están inspiradas en modelos de financiamiento tradicionales.

El notable desarrollo del crowdfunding se ha debido a la conjunción de varias fuerzas:

1. Las movilizaciones de oferta y demanda propiciadas por el escenario de crisis económica que han llevado, por un lado, a los agentes con necesidad de financiamiento a la búsqueda de fuentes alternativas para hacer frente a la escasez de crédito (principalmente para proyectos en sus primeras fases o iniciativas con riesgo elevado) y, por otro lado, a los agentes ahorradores a la búsqueda de rentabilidades superiores a las ofrecidas por el sistema financiero tradicional, en un contexto de bajos tipos de interés en el ámbito global.
2. El despliegue de una infraestructura de telecomunicaciones adecuada y de una mejora destacable en la velocidad de procesamiento de la información en la era digital, mismo que ha permitido, por ejemplo, el desarrollo de interfaces más interactivas y atractivas para el usuario o la posibilidad de aplicar nuevas técnicas analíticas provenientes del big data para mejorar el cálculo de los scorings. Todo esto se ha unido al acceso y uso por parte de una masa suficiente de la población de internet, especialmente de servicios de pagos electrónicos o de la banca on line.
3. Los gaps dejados por la regulación. Dadas las fuerzas del crowdfunding, éste puede desempeñar un papel fundamental como complemento de las fuentes tradicionales de financiamiento, favorecer el nacimiento de iniciativas empresariales y la innovación, contribuyendo en el ámbito económico, a la vez que ofrece altas rentabilidades para el ahorro. No obstante, los riesgos de solvencia y liquidez son potencialmente altos en un mercado donde hay asimetría de información entre demandantes y oferentes de financiamiento, por lo que el reto es cubrir los gaps, tanto de la regulación como de las recomendaciones para la competencia

[25] Crowdfunding *en 360º: alternativa de financiación en la era digital*, Carmen Cuesta, Santiago Fernández de Lis *et al.*, Observatorio Economía Digital, BBVA Research, 2014, sisponible en <https://www.bbvaresearch.com/wp-content/uploads/2015/01/Observatorio_crowdfunding.pdf>, consultado el 13 de diciembre de 2017.

[26] *Idem*.

económica, y continuar con las políticas de educación financiera.

México se ha colocado como uno de los líderes regionales y de acuerdo con la información del noveno Reporte Nacional de Inclusión Financiera, durante el 2017 aproximadamente 8 mil empresas han conseguido financiamiento mediante crowdfunding; esto plantea un crecimiento de 280 por ciento respecto a los datos recolectados en 2015.

13. Reconocimiento: Las bases del cambio

Activos virtuales

Con la ley, las ITF tienen capacidad de operar con activos virtuales, entendidos como las representaciones de un valor digital verificable que no se encuentran emitidos ni respaldados por ningún banco central o entidad financiera, es decir, que no tienen curso legal y que, a pesar de eso, generan unidades para su intercambio debido a su aceptación por el público.[27]

Además, se añade que las ITF podrán constituir depósitos en entidades financieras autorizadas para recibirlos, y que será facultad del Banco de México prever situaciones relacionadas con la transformación o modificación de características de los activos virtuales.

En marzo de 2019, el Banco de México emitió las "Disposiciones de Carácter General" para el manejo de activos virtuales. En ellas, indicó que sólo permitirá que tanto bancos como Instituciones de Tecnología Financiera, reguladas bajo la Ley Fintech, realicen operaciones con activos virtuales de manera interna, sin trasladar el riesgo a sus usuarios.

Entre sus argumentos, el banco central dijo que no busca restringir el uso de tecnologías que pudieran tener un beneficio desde la perspectiva de eficiencia o funcionalidad, siempre y cuando estas tecnologías sean utilizadas en el contexto de la operación interna de las Instituciones de Tecnología Financiera (ITF) y de las Instituciones de Crédito (IC), y esto a su vez no implique un aumento significativo en los riesgos operativos o financieros de las mismas. Es decir, la utilización de tecnología como registros distribuidos, cadena de bloques o incluso los propios activos virtuales en sus procesos internos podría llegar a ser factible, previa autorización del Banco de México, siempre y cuando los riesgos de los activos virtuales no impacten al consumidor final.[28]

Por lo anterior,

> el Banco de México presentó una regulación en la que se establece un mecanismo de solicitudes de autorización en la que se requiere a las instituciones interesadas presentar la forma en que atenderán los riesgos asociados a la operación con activos virtuales en caso de que decidan utilizarlos para su operación interna, sin considerar algún tipo de autorización que implique la operación con activos virtuales de cara al cliente, pues se considera que la provisión de servicios relacionados con activos virtuales al público en general por parte de las

[27] SEGOB, Subsecretaría de Enlace y Acuerdos Legislativos, oficio núm. SELAP/300/2734/17.

[28] "Regulación sobre la operación con activos virtuales por parte de las Instituciones de Tecnología Financiera e Instituciones de Crédito", disponible en <https://www.banxico.org.mx/sistemas-de-pago/6--acciones-regulatorias-po.html>, consultaldo el 26 de enero de 2020.

instituciones financieras no es conveniente y los riesgos asociados a los activos virtuales no deben impactar al usuario final.

El Banco de México aclaró que, actualmente, no hay un régimen de prevención de operaciones con recursos de procedencia ilícita o de financiamiento al terrorismo que aplique a aquellas personas distintas a las entidades financieras que, de manera habitual y profesional, ofrezcan el intercambio de activos virtuales a través de plataformas electrónicas, digitales o similares, que dichas personas administren u operen, facilitando o realizando operaciones de compra o venta de dichos activos propiedad de sus clientes o bien, provean medios para custodiar, almacenar o transferir activos virtuales. No obstante, mediante reformas a la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita, publicadas el 9 de marzo de 2018, estas personas quedarán sujetas al régimen de dicha ley a partir de septiembre de 2019.

Crecimiento y respuesta

Diversos organismos y autoridades han expresado su preocupación por la expansión de los activos virtuales debido a que, si bien pueden ser utilizados de manera legítima, su complejidad y variedad incrementan los riesgos de fraude o de inversiones especulativas, por lo que son una prioridad los mecanismos de divulgación de información sobre los activos virtuales para que los usuarios cuenten con mayores y mejores elementos para la toma de decisiones.

Considerando esta realidad, el Banco de México realizó una investigación sobre el tratamiento internacional sobre los activos virtuales,[29] el cual se resume en los siguientes cuadros:

País	*Pronunciamiento*
Alemania	La Autoridad Federal de Supervisión Financiera catalogó a los activos virtuales como instrumentos financieros, por lo que, en caso de que alguna empresa quiera ofrecer servicios de compra-venta de activos virtuales, requieren una autorización de dicha autoridad.
Francia	La Autoridad de Mercados Financieros y la Autoridad de Supervisión Prudencial emitieron un comunicado conjunto en el que se advierte a los inversionistas acerca de la falta de regulación sobre los activos virtuales, y que éstos no son algún tipo de instrumento financiero.
Reino Unido	No existe una regulación sobre activos virtuales; sin embargo, la compra-venta de bienes y servicios que utilicen activos virtuales son sujetos a impuesto sobre la renta.
Lituania	El Banco Central emitió un comunicado en el que establece que los proveedores de servicios financieros no deberían participar en actividades o proveer servicios asociados con activos virtuales; a su vez, aquellos proveedores de servicios financieros que tengan clientes cuyas actividades estén asociadas con activos virtuales, deben tomar las medidas necesarias para cumplir con la regulación relativa a prevención de lavado de dinero y combate al financiamiento al terrorismo.

[29] Véase <https://www.banxico.org.mx/sistemas-de-pago/5--tratamiento-internaciona.html>.

País	*Pronunciamiento*
Estados Unidos	La Comisión de Intercambio de Futuros catalogó los activos virtuales como un tipo de mercancía según las normas establecidas en el Commodity Exchange Act. Además, establece que, si el comprador no puede confirmar la posesión del activo virtual adquirido en un periodo no mayor a 28 días, la transacción sería considerada como un futuro, debiendo cumplir las reglas establecidas para dichos contratos con el fin de evitar que las instituciones de compra-venta de activos virtuales mantengan posesión de los activos virtuales en sus carteras.
Canadá	De forma similar a Reino Unido, se aplican reglas fiscales en los casos de compra-venta de bienes y servicios por medio de activos virtuales.
Brasil	El Banco Central emitió un comunicado en el que se alerta a los ciudadanos sobre las operaciones con activos virtuales.
Colombia	La Superintendencia Financiera de Colombia emitió un comunicado en el que se alerta a los ciudadanos sobre las operaciones con activos virtuales.
Costa Rica	El Banco Central emitió un comunicado en el que se alerta a los ciudadanos sobre las operaciones con activos virtuales.

Instituciones internacionales

Consejo de Estabilidad Financiera (FSB, por sus siglas en inglés)	Acorde con lo establecido en el reporte del FSB sobre las implicaciones de estabilidad financiera derivadas de fintechs, se considera que en la actualidad, debido al tamaño de mercado relativamente pequeño de los activos virtuales (aproximadamente 700 activos virtuales distintos con una capitalización de mercado de 106 mil millones de dólares a la fecha del reporte) y a las dificultades que presentan los sistemas que soportan dichos activos para escalar el número de operaciones, estos activos no representan un riesgo sistémico y la posibilidad de que puedan alcanzar una importancia sistémica es muy baja. Además, es poco probable que los activos virtuales sustituyan a las monedas nacionales.
Banco Internacional de Pagos (BIS, por sus siglas en inglés)	Según el reporte anual de 2018, dentro de los desafíos clave en la regulación de los activos virtuales se encuentra el combate al lavado de dinero y el financiamiento al terrorismo, en particular gracias al anonimato que provee este tipo de activos en la realización de transacciones. Adicionalmente, el reporte establece que hay una necesidad de establecer reglas que garanticen la protección a los consumidores.
Grupo de Acción Financiera Internacional (FATF, por sus siglas en inglés)	Está realizando un proyecto de modificaciones al marco integral sobre las recomendaciones respecto a las medidas que los países deben implementar para combatir el lavado de dinero y el financiamiento al terrorismo a través del uso de activos virtuales. En particular, se está buscando incluir los activos virtuales y la operación con éstos como actividades que requieren la aplicación de todas las acciones recomendadas, pues representan un activo que facilita la realización de actividades ilícitas.

Tratamiento internacional sobre los activos virtuales

País	*Definición de activo virtual*	*Ley*	*Características*
Japón	Define dos tipos de activos virtuales: Tipo 1: valor propietario: *i)* disponible como medio de pago para la compra o préstamo de bienes o servicios, *ii)* que puede canjearse por moneda de curso legal y *iii)* que puede ser transferido a través de una red de cómputo. Tipo 2: valor propietario que es mutuamente intercambiable con activos virtuales tipo 1, que puede ser transferible a través de una red de cómputo. Existe la posibilidad de que las empresas puedan realizar el servicio de intercambio de activos virtuales. Para lo anterior, las empresas deben obtener una licencia de "Proveedor de Servicios de Intercambio de Monedas Virtuales" (PSIMV).	Ley de Servicios de Pago	Las actividades consideradas en la Ley son: Compra-venta de activos virtuales o el intercambio por otros activos virtuales; administración de activos virtuales de los usuarios. En los casos en los que la administración de activos virtuales de los usuarios no esté relacionada con la compra-venta de activos virtuales, no se requiere autorización como PSIMV. Las políticas de protección al consumidor incluyen estándares prudenciales como un requerimiento de capital mínimo de 90 mil dólares (10 millones de yenes); reglas de transparencia que implican dar información detallada a los usuarios respecto a la compra-venta, detalles de la transacción y comisiones; manuales operativos y organizacionales que incluyan la información del manejo de seguridad, sistemas de control interno y protección de datos y segregación de recursos de los propios. La Ley para la Prevención de Transferencias de Ingresos de Procedencia Ilícita de Japón obliga a los PSIMV a establecer procesos de conocimiento del cliente, llenado de reportes de actividades sospechosas, así como a tener sistemas de control interno. La Agencia de Servicios Financieros de Japón otorgó una licencia a la Asociación Japonesa de Casas de Cambio de Activos Virtuales para operar como un órgano autorregulatorio. La licencia otorgada por el órgano gubernamental permite a la asociación emitir sus propias reglas y sancionar a los miembros que no las cumplan.

País	*Definición de activo virtual*	*Ley*	*Características*
Corea del Sur		Directrices para la prevención de lavado de dinero con activos virtuales	Antes de entrar en vigor las directrices, los bancos ofrecían a los usuarios de las casas de cambio de activos virtuales cuentas especiales en las que podían ingresar y retirar recursos en moneda local para realizar operaciones de compra-venta de activos virtuales. Estas cuentas eran distintas a las de depósito bancarias y requerían menos información para su apertura. Con la directrices, se obliga a los bancos a cambiar este tipo de cuentas por cuentas que sí requieran un proceso estricto de identificación del usuario. Además, los bancos deben monitorear las transacciones de las casas de cambio de activos virtuales y confirmar la fuente de los recursos asociados a transacciones sospechosas. Posteriormente se realizaron modificaciones que establecen que las casas de cambio de activos virtuales deben separar sus recursos operativos de los de sus clientes. Además, obligan a las instituciones financieras a compartir una lista de casas de cambio de activos virtuales domésticas y del exterior, y les requiere reforzar sus canales de monitoreo sobre las transacciones de casas de cambio domésticas a instituciones del exterior para la prevención de evasión de impuestos y lavado de dinero.

País	*Definición de activo virtual*	*Ley*	*Características*
Nueva York	La ley define un activo virtual como cualquier unidad digital que se utiliza como medio de cambio o una forma de valor almacenado de manera digital. Incluye los activos virtuales que tienen un administrador centralizado, aquellos que tienen una administración descentralizada y que pueden ser creados por medio de poder computacional.	BitLicence	Esta regulación se aplica a las entidades que transmiten, mantienen la custodia, realizan compra venta o administran activos virtuales a nombre de terceros. Para poder hacer este tipo de actividades, es necesario obtener una licencia; la regulación contiene las reglas de solicitud de autorización, requerimientos de capital, reglas de custodia y protección de los activos de los usuarios, reglas para la prevención de lavado de dinero, un programa de ciberseguridad y reglas para la protección al consumidor. La regulación obliga a las empresas que custodien activos virtuales de sus clientes a mantener a la par dichos activos. Asimismo, las reglas obligan a las empresas que obtengan la licencia a establecer un programa de prevención de lavado de dinero (PLD) que como mínimo tenga controles internos, políticas y procedimientos para cumplir con la regulación de PLD, así como programas de capacitación para el personal. Respecto a los requisitos de ciberseguridad, se obliga a las empresas a tener un programa basado en cinco puntos principales: identificación de riesgos externos, protección de la información, detección de intrusión a los sistemas, política de respuesta ante un ciberataque, así como una política de recuperación tras ataque. BitLicense incluye la obligación de informar a sus clientes que los activos virtuales no son moneda de curso legal y que no están respaldados por el gobierno, que los cambios a la regulación pueden afectar su uso de manera negativa, que las transacciones son irreversibles, así como sobre la posible pérdida de los recursos a los que los clientes e pueden enfrentarse derivado del hecho de que el valor es altamente volátil.

Las autoridades y los bancos centrales de diferentes partes del mundo siguen escrutando con cautela el mercado de los activos virtuales. El anuncio de la intención de crear Libra, la criptodivisa encabezada por Facebook con tipo de cambio estable y con el potencial de convertirse en un fenómeno global, ha sido el catalizador de un debate que todavía está en marcha.

Una vuelta atrás

La más popular de las monedas virtuales es el bitcoin. Su creador o creadores se ocultan bajo el seudónimo de "Satoshi Nakamoto" y ya ha recibido premios prestigiosos a la innovación financiera y hasta la propuesta para el Nobel de Economía, no aceptada por la Academia debido al anonimato de su creador.

El bitcoin fue diseñado para que se emitan 21 millones de unidades. No está controlado por ningún gobierno o banco central o privado. La identidad de los usuarios que realizan las transacciones no está ligada directamente a la cuenta donde se realizan los fondos. Se sustenta en las cadenas de bloques (*blockchain*) o bases de datos distribuidas que, actuando por consenso como si fuese un notario público, almacenan las transacciones sin posibilidad de modificación o revisión.

La actividad en bitcoins presenta crecimientos exponenciales alentada por aumentos de su precio. En 2009, el año en que el bitcoin fue creado, su precio era de $ 0.001. Durante 2015, ganó popularidad lenta pero firmemente y, durante ese año, el precio comenzó a subir poco a poco. Desde mayo de 2016, el bitcoin se ha ganado la confianza de más personas y su precio ha seguido aumentando. Sin embargo, debe tenerse en cuenta que enfrenta una serie de riesgos, como el de crédito, tecnológico, de mercado y operacional debido a:

1. **Riesgo de crédito**. La validación de una transacción media suele ser de unos 10 minutos y la ausencia de respaldo bancario o institucional exponen a cualquier usuario al incumplimiento de la contraparte sin las habituales garantías financieras que ofrecen los sistemas de pagos internacionales. Adicionalmente, el anonimato de los actores en ciertas operaciones y la imposibilidad de retroceder transacciones sobreexponen a los usuarios ante el riesgo de impago.
2. **Riesgo tecnológico.** Las monedas virtuales son absolutamente dependientes de la tecnología y tienen por delante importantes retos por solventar antes de convertirse en un medio universalmente aceptado.
3. **Riesgo de mercado.** La volatilidad del bitcoin en 2017 ha sido de 79 por ciento, en promedio, por ejemplo.
4. **Riesgos operacionales.** Los errores y la exposición al fraude son elevados por el propio diseño de la moneda virtual y su falta de respaldo institucional.

Definiciones pertinentes

Entrar al mundo de los activos virtuales implica tener un conocimiento del mismo y tener en cuenta las definiciones clave:[30]

[30] "Informe del GAFI. Monedas virtuales, definiciones clave y riesgos potenciales de LA/FT", junio de 2014, disponible en <http://www.gafilat.org/UserFiles/Biblioteca/Doc%20Interes/tipologias%20gafi/MonedasVirtuales(ESP).pdf>, consultado el 18 de diciembre de 2017.

Moneda virtual. Es una representación digital de valor que puede ser comerciada digitalmente y funciona como un medio de cambio y/o una unidad de cuenta y/o un depósito de valor, pero que no tiene curso legal (es decir, que cuando se ofrezca a un acreedor, no es una oferta válida y legal de pago) en ninguna jurisdicción. Ninguna jurisdicción emite o garantiza las monedas virtuales, y cumple con las funciones antes mencionadas por común acuerdo de la comunidad de sus usuarios.

La moneda virtual se distingue del dinero fiduciario (moneda real, dinero real o moneda nacional), porque éste funciona como la moneda y el papel moneda de un país designado, como dinero de curso legal que circula, se utiliza y se acepta como medio de intercambio en el país emisor. Es diferente del dinero electrónico, puesto que éste es una representación digital del dinero fiduciario, usado electrónicamente para transferir el valor denominado en dinero fiduciario. El dinero electrónico funciona como un mecanismo de transferencia digital para el dinero fiduciario, es decir, transfiere electrónicamente un valor que tiene la condición de moneda de curso legal.

Moneda digital. Puede hacer referencia a una representación digital de cualquier moneda virtual (no dinero fiduciario) o de dinero electrónico (dinero fiduciario), y por ello a menudo su uso es intercambiable con el término "moneda virtual".

Las monedas virtuales se dividen en dos tipos básicos: moneda virtual convertible o abierta y no convertible o cerrada. La primera no implica en ningún caso la convertibilidad *ex officio* (por ejemplo, en el caso del patrón oro), sino más bien una convertibilidad *de facto* (por ejemplo, por el hecho de que un mercado exista). Por ello, una moneda virtual es "convertible", siempre y cuando participantes privados las ofrezcan y otros las acepten, ya que la "convertibilidad" no está garantizada en absoluto por ley.

Moneda virtual convertible tiene un valor equivalente en moneda real y puede ser intercambiada una y otra vez por dinero real. Algunos ejemplos incluyen: bitcoin, e-Gold (fuera de uso), Liberty Reserve (fuera de uso), Second Life Linden Dollars y WebMoney.

Moneda virtual no convertible pretende ser específica de un dominio o mundo virtual particular, como los videojuegos de rol multijugador excepcionales en línea (MMORPG, por sus siglas en inglés) y, en virtud de las normas que regulan su uso, no puede cambiarse por dinero real. Algunos ejemplos incluyen: Project Entropia Dollars, Q Coins y World of Warcraft Gold.

Cabe señalar que, aunque en virtud de los términos establecidos por el administrador, una moneda no convertible sólo puede ser transferida oficialmente dentro de un entorno virtual específico y aunque en ningún caso pueda ser convertible, es posible que pueda surgir un mercado negro secundario no oficial que proporcione una oportunidad de intercambiar la moneda virtual no convertible por moneda fiduciaria o por otra moneda virtual. Por lo general, el administrador aplicará sanciones (incluida la terminación de la membresía y/o la confiscación de las restantes monedas virtuales) a aquellos que busquen crear o utilizar un mercado secundario en contra de las reglas de la moneda.

Todas las monedas virtuales no convertibles son centralizadas: por definición, son emitidas por una autoridad central que establece normas que las hacen no convertibles. Por el contrario, las monedas virtuales convertibles pueden ser de cualquiera de los dos subtipos: centralizadas o descentralizadas.

Las **monedas virtuales centralizadas** tienen una autoridad administrativa única

(administrador), es decir, una tercera parte que controla el sistema. Un administrador emite la moneda, establece las normas para su utilización, mantiene un libro de contabilidad central de pago y tiene autoridad para canjear la moneda (retirarla de la circulación). La tasa de cambio de una moneda virtual convertible puede ser variable, es decir, determinada por la oferta y la demanda de la moneda virtual, o fija, es decir, fijada por el administrador según un valor establecido medido en dinero real o por cualquier reserva de valor del mundo real, como el oro o una cesta de divisas.

La gran mayoría de las transacciones de pago en moneda virtual implican monedas virtuales centralizadas, por ejemplo: E-gold (fuera de uso), Liberty Reserve dollars/euros (fuera de uso), Second Life "Linden dollars", PerfectMoney, WebMoney "WM units" y World of Warcraft gold.

Las **monedas virtuales descentralizadas** (también conocidas como criptomonedas) son monedas virtuales de código abierto fundamentadas matemáticamente, que funcionan en una red de pares distribuida, sin autoridad central administradora, de vigilancia o de supervisión. Por ejemplo: bitcoin, LiteCoin y Ripple.

La **criptomoneda** se refiere a una moneda virtual convertible, descentralizada, fundamentada matemáticamente y que está protegida por criptografía, es decir, que incorpora los principios de la criptografía para implementar una economía de la información segura, descentralizada y distribuida. Las criptomonedas se basan en llaves públicas y privadas para transferir el valor de una persona (individuo o entidad) a otra, y debe ser criptográficamente firmado cada vez que se transfiere.

La seguridad, la integridad y la armonía de los libros de contabilidad de la criptomoneda están garantizadas por una red de partes mutuamente desconfiadas (en bitcoin se conocen como mineros) que protegen la red a cambio de la obtención de una tasa distribuida aleatoriamente (en bitcoin, un pequeño número de nuevas unidades de bitcoins llamado "recompensa de bloque" y, en algunos casos, también las tasas por transacción que pagan los usuarios como incentivo para que los mineros incluyan sus transacciones en el siguiente bloque).

Se han definido decenas de especificaciones sobre las criptomonedas; la mayoría se derivan del bitcoin y utilizan un sistema de prueba de trabajo para validar las transacciones y mantener la cadena de bloques. Si bien el bitcoin significó la primera implementación del protocolo de una criptomoneda, hay un creciente interés en el desarrollo de métodos de prueba alternativos y potencialmente más eficientes, como los sistemas basados en la prueba de participación.

El bitcoin, lanzado en 2009, fue la primera moneda virtual convertible descentralizada y la primera criptomoneda. Los bitcoins son unidades de cuenta compuestos de secuencias alfanuméricas únicas que constituyen unidades de moneda y que tienen valor sólo porque usuarios individuales están dispuestos a pagar por ellos. Los bitcoins se comercian digitalmente entre los usuarios, contando con un alto grado de anonimato y pueden cambiarse (comprar o canjear) por dólares estadounidenses, euros y otras monedas fiduciarias o virtuales. Cualquier persona puede descargar el software gratuito de código abierto de un sitio web para enviar, recibir y almacenar bitcoins, así como para monitorear las transacciones de bitcoins. Los usuarios también pueden obtener direcciones de bitcoin, que funcionan como cuentas, en un intercambiador de bitcoin o servicio de monedero en línea.

Las transacciones (flujos de fondos) están públicamente disponibles en un registro de transacciones compartidas e identificadas por la dirección Bitcoin, una secuencia alfanumérica que no está sistemáticamente conectada a un individuo. Por ello, se dice que el bitcoin es "pseudo-anónimo".

API, el panorama

Para promover la competencia en igualdad de condiciones, es fundamental establecer regulaciones sobre la portabilidad y el acceso a datos que sean recíprocos y que no generen asimetrías entre distintos tipos de participantes en el mercado. El artículo 76 de la Ley Fintech obliga a los bancos (y otras entidades financieras) a desarrollar API (Application Programming Interface, es decir, las Interfaces de Programación de Aplicaciones informáticas estandarizadas que intercambien datos) para compartir datos financieros abiertos, datos agregados y datos transaccionales (definidos en la propia ley).

La apertura de los datos y su regulación ha sido considerada por muchos como la parte más relevante, ya que implica para las entidades financieras la obligación de abrir los datos de un cliente a través de una API. Para el consumidor, significa que tendrá una mejor portabilidad de sus datos financieros, es decir, podrá tomar su historial financiero con un banco y llevarlo con otro. Esta posibilidad hará que haya más competencia.

Según un estudio MarketsandMarkets, entre 2019 y 2023 habrá una elevada demanda de API que permitan conectar diversas aplicaciones y dispositivos, por lo que se estima que el crecimiento anual será de 32.9 por ciento, lo que hará que el mercado sea muy diferente al actual en unos cuantos años, ya que, de mover 1,200 millones de dólares en 2018, pasará a 5,100 millones en 2023.

Proyecto de disposiciones relativas a la API

Como se mencionaba, en diciembre de 2019 ya se contaba con el proyecto de Disposiciones de Carácter General relativas a las Interfaces de Programación de Aplicaciones Informáticas Estandarizadas a que hace referencia la Ley para Regular las Instituciones de Tecnología Financiera. Este proyecto se turnaría a las instancias correspondientes a fin de presentarlas para su aprobación en marzo de 2020. Por la importancia que tienen en general, y en particular para los efectos de este trabajo, se transcribe el contenido del documento disponible al 20 de febrero de 2020, a reserva de que el lector tome en cuenta que lo publicado aquí puede tener modificaciones respecto a su publicación definitiva en el *Diario Oficial de la Federación*. En el Anexo 3 se presentan las Disposiciones de carácter general para regular las Instituciones de Tecnología Financiera, aplicables a las Sociedades de Información Crediticia y Cámaras de Compensación en materia de interfaces de programación de aplicaciones informáticas estandarizadas, emitidas por el Banco de México y publicadas en el Diario Oficial de la Federación el 10 de marzo de 2020, como nuestra del interés de cooperación de los involucrados en el tema en beneficio del país.

Capítulo	*Contenido*
CAPÍTULO I	Disposiciones comunes.
CAPÍTULO II	De los solicitantes de datos.
CAPÍTULO III	De los proveedores de datos.
CAPÍTULO IV	De los programas de regularización.
Anexo 1	Lineamiento de seguridad para datos abiertos.

Capítulo	*Contenido*
Anexo 2	Lineamientos de la arquitectura de datos para el intercambio de información de datos abiertos.
Anexo 3	Diccionario de datos abiertos de cajeros automáticos.

Capítulo I
Disposiciones comunes

Artículo 1.- Para efectos de las presentes disposiciones, en adición a las definiciones previstas en la Ley, se entenderá, en singular o plural, por:

I. API, por sus siglas en inglés (*Application Programming Interface)*, a las interfaces de programación de aplicaciones informáticas estandarizadas que posibilitan el intercambio de Datos.
II. Autenticación, al conjunto de técnicas y procedimientos utilizados por el Proveedor de Datos para verificar la identidad de un Solicitante de Datos y su condición para acceder a los Datos disponibles a través de API.
III. Datos, a los datos abiertos a que hace referencia la fracción I del artículo 76 de la Ley.
IV. Evento de Seguridad de la Información, a cualquier suceso, interno o externo, relacionado con Clientes, terceros contratados por los Solicitantes de Datos o Proveedores de Datos, personas o procesos operativos, así como con componentes de la Infraestructura, u otros elementos que almacenen información, entre otros, que pueda suponer una afectación en la confidencialidad, integridad o disponibilidad de la información que dicho Proveedor de Datos o Solicitante de Datos gestione o conozca, o en la propia Infraestructura.
V. Incidente de Seguridad de la Información, al Evento de Seguridad de la Información del Proveedor de Datos cuando se actualice alguno de los siguientes supuestos:

a) Haya comprometido la confidencialidad, integridad o disponibilidad de uno o más componentes de la Infraestructura utilizada por un Solicitante de Datos o Proveedor de Datos, o bien, de los Datos que se envíen o reciban a través de dicha Infraestructura, con un efecto adverso para cualquiera de ellos, o bien, para terceros contratados por el Proveedor de Datos para administrar o desarrollar API, entre otros.
b) Vulnere la Infraestructura, comprometiendo los Datos que procesa, almacena o transmite.
c) Constituya una violación de las políticas y procedimientos de seguridad a que hace referencia el artículo 5 de las presentes disposiciones.
d) Constituya la materialización de un menoscabo, 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 interrupción de los servicios, atentados contra las infraestructuras interconectadas, conocidos como ciberataques.

VI. Infraestructura, a los equipos de cómputo, instalaciones de procesamiento de datos y comunicaciones, equipos y redes de comunicaciones, sistemas operativos, bases de datos, aplicaciones y sistemas que utilizan los Solicitantes de Datos o Proveedores de Datos para soportar la operación de las API.
VII. Ley, a la Ley para Regular las Instituciones de Tecnología Financiera.
VIII. Proveedores de Datos, a las Entidades Financieras, ITF, sociedades autorizadas por la CNBV para operar con Modelos Novedosos y transmisores de dinero que, conforme al primer párrafo del artículo 76 de la Ley, estén obligados a establecer API con el fin de compartir Datos.
IX. Solicitantes de Datos, a las Entidades Financieras, ITF, sociedades autorizadas para operar con Modelos Novedosos, transmisores de dinero y terceros especializados en tecnologías de información.
X. Usuarios, a las personas que utilicen los productos o servicios que ofrezcan los Solicitantes de Datos.

Capítulo II
De los Solicitantes de Datos

Artículo 2.- Los Solicitantes de Datos cuyas API desarrolladas o administradas por éstos cumplan con lo establecido en los Anexos 1, 2 y 3 de las presentes disposiciones, se tendrán por autorizados por la CNBV sin necesidad de declaración alguna, para acceder a los Datos de los distintos Proveedores de Datos a los que solicite su acceso a través de dichas API.

Capítulo III
De los Proveedores de Datos

Artículo 3.- Los Proveedores de Datos en el desarrollo o administración de sus API deberán cumplir con los Anexos 1, 2 y 3 de las presentes disposiciones.

Los Proveedores de Datos publicarán, de forma clara, precisa y en idioma español, en su página de internet o cualquier otro medio de comunicación electrónica, aplicaciones informáticas o digitales, el proceso que deberán seguir los Solicitantes de Datos para acceder a los Datos a través de API y las contraprestaciones que, en su caso, deberán pagar por el intercambio de Datos.

Los términos y condiciones que establezcan los Proveedores de Datos con los Solicitantes de Datos para llevar a cabo el intercambio de Datos a través de API deberán establecer mecanismos y controles que aseguren la confidencialidad e integridad de los Datos en su acceso, procesamiento y almacenamiento por parte de los Solicitantes de Datos.

Artículo 4.- Los Proveedores de Datos deberán contar con una política de seguridad de la información que proteja en todo momento la Infraestructura, propia o de terceros contratados por éstos, así como la confidencialidad e integridad de los Datos que, en su caso, compartan a través de API. La mencionada política de seguridad deberá contener procedimientos continuos, mecanismos y controles, considerando, al menos, lo siguiente:

I. Configuración segura de los componentes tecnológicos de su Infraestructura, incluidos, entre otros, cierre de puertos y servicios, instalación de mecanismos para detección y prevención de virus, códigos maliciosos y detección de intrusos, así como actualizaciones del fabricante.
II. Mecanismos de identificación y autenticación del personal responsable

del manejo de API bajo el principio de mínimo privilegio. Se entenderá como principio de mínimo privilegio la habilitación del acceso únicamente a la información y recursos necesarios para el desarrollo de las funciones propias del personal referido.

III. Cifrado de la información almacenada y de los canales a través de los que se envíen los Datos, así como mecanismos de identificación y autenticación, que cumplan con los Anexos 1 y 2 de las presentes disposiciones.

IV. Procesos de gestión para la atención de Incidentes de Seguridad de la Información que se presenten en la operación de las API, que aseguren la detección, atención y contención, investigación y, en su caso, análisis forense digital, diagnóstico, solución, seguimiento y reporte a la CNBV a que hace referencia el artículo 6 de estas disposiciones.

V. Programa de pruebas de escaneo de vulnerabilidades y amenazas en el acceso y administración de las API, el cual podrá ser realizado por un tercero. El mencionado programa deberá considerar la realización de dichas pruebas al menos una vez cada tres meses, así como con un plan de remediación para las vulnerabilidades críticas detectadas.

VI. Programa de pruebas de penetración, el cual establezca que se realizarán al menos dos pruebas al año sobre sistemas y aplicativos que estén relacionados o conectados con API, o bien, cuando lo ordene la CNBV. Dichas pruebas deberán realizarse por un tercero independiente que cuente con personal con capacidad técnica comprobable mediante certificaciones especializadas de la industria en la materia. Asimismo, deberá contarse con un plan de remediación para las vulnerabilidades críticas detectadas.

VII. Mecanismos de respaldo y procedimientos de recuperación de la información que mitiguen el riesgo de interrupción de la operación.

VIII. Registros de auditoría íntegros, incluidas la información detallada de los accesos o intentos de acceso y la operación o actividad efectuada por el Solicitante de Datos con la información obtenida. La información a que se refiere el presente numeral deberá conservarse por, al menos, un año.

Tratándose de Proveedores de Datos cuyo régimen normativo establezca disposiciones en materia de seguridad de la información, lo previsto en este artículo deberá ser incorporado en las políticas y procedimientos que deban establecer conforme a dicho régimen.

Artículo 5.- Los Proveedores de Datos deberán asegurar que su Infraestructura para compartir Datos por medio de API cumpla con lo siguiente:

I. Contar con una configuración que garantice que el acceso a los Datos compartidos sea solamente de lectura.

II. Que la Infraestructura se encuentre segregada de aquella que soporte cualquier operación y que cuente con mecanismos de seguridad que limiten el acceso desde el servicio de API hacia este último, bajo el principio de mínimo privilegio.

Se entenderá como principio de mínimo privilegio la habilitación del acceso únicamente a la información y recursos necesarios para el desarrollo

de las funciones propias del personal responsable del manejo de API.

III. Cuenten con procedimientos que garanticen la disponibilidad del servicio relacionado con el intercambio de Datos.

IV. Registros de auditoría íntegros, incluidas la información detallada de los accesos o intentos de acceso y la operación o actividad efectuada en la Infraestructura.

Artículo 6.- En los casos en que se presente un Incidente de Seguridad de la Información, los Proveedores de Datos deberán reportarlo a la CNBV de manera inmediata y a través del correo electrónico ciberseguridad-cnbv@cnbv.gob.mx. En dicha notificación deberá indicarse, al menos, la fecha y hora de inicio del Incidente de Seguridad de la Información de que se trate y, en su caso, la indicación de si continúa o ha concluido y su duración; una descripción de dicho incidente, así como una evaluación del mismo.

Artículo 7.- Los Proveedores de Datos, en los casos en que interrumpan el acceso de información por el incumplimiento del Solicitante de Datos a los términos y condiciones pactados para el intercambio de Datos, deberán notificarlo, vía correo electrónico, a la dirección general de la CNBV encargada de su supervisión. En dicha notificación deberán señalarse las razones que justifiquen la interrupción del acceso a la información y los supuestos de incumplimiento a los términos y condiciones pactados, adjuntando la evidencia de tales incumplimientos.

Artículo 8.- Los Proveedores de Datos deberán presentar ante la CNBV, para su autorización, registro y, en su caso, modificación, las contraprestaciones que pretendan cobrar a los Solicitantes de Datos por el intercambio de Datos, debiendo proporcionar, por cada tipo de API, el método, la información y las variables empleadas para determinar las contraprestaciones, así como cualquier otra consideración utilizada en tal determinación.

Los Proveedores de Datos para efectos de realizar el registro de las contraprestaciones deberán presentar la siguiente información:

I. Nombre, denominación o razón social, sin abreviaturas.

II. En su caso, nombre comercial.

III. Registro Federal de Contribuyentes.

IV. Nombre de la API a la cual aplicará la contraprestación.

V. Descripción del método empleado para determinar la contraprestación.

VI. Monto de la contraprestación, en moneda nacional.

VII. Número telefónico de las personas encargadas de implementar la API.

VIII. Correo electrónico de las personas encargadas de implementar la API.

IX. Periodicidad con la que la contraprestación será exigible, o bien, algún otro parámetro utilizado.

El procedimiento para la autorización de las contraprestaciones, así como para su incremento o reducción, se ajustará a lo establecido en el artículo 76 de la Ley.

Capítulo IV

De los programas de regularización

Artículo 9.- Las Entidades Financieras, las ITF, las sociedades autorizadas por la CNBV para operar con Modelos Novedosos y los transmisores de dinero, en el supuesto previsto en el párrafo décimo segundo del artículo 76 de la Ley y al ejercer su derecho de audiencia, podrán presentar, para aprobación de la CNBV, un programa de regularización,

el cual deberá contemplar, cuando menos, los requisitos siguientes:

I. Señalar las acciones que habrán de implementar para observar las obligaciones previstas en las presentes disposiciones que hayan incumplido.
II. Especificar las etapas y plazos de cada una de las acciones por implementar, así como las personas responsables de llevar a cabo tales acciones. En ningún caso la ejecución y cumplimiento del programa de regularización deberá exceder de tres meses contados a partir de su autorización.
III. Las medidas tendientes a prevenir nuevos incumplimientos.

La CNBV tendrá 20 días hábiles, contados a partir de que reciba el programa de regularización respectivo, para resolver al respecto. La CNBV podrá prevenir al interesado, por una sola ocasión y dentro de los 10 días hábiles al plazo que tiene para resolver, de la falta de requisitos en el contenido del programa o para solicitar mayor información; por lo que, en estos casos, se ampliará por cinco días hábiles más, el plazo para que la CNBV resuelva lo conducente.

El interesado tendrá cinco días hábiles contados a partir de que reciba la prevención de la CNBV para atender el requerimiento de información; de lo contrario, la CNBV resolverá con la información con la que cuente.

TRANSITORIO

ÚNICO. - Las presentes disposiciones entrarán en vigor el día siguiente al de su publicación en el *Diario Oficial de la Federación*.

Instituciones de fondos de pago electrónico

La Ley Fintech contempla la regulación de las Instituciones de Fondos de Pago Electrónicos como consecuencia del aumento de esta modalidad de pago en el comercio, ya que ofrece seguridad y aceptación en los negocios que se encuentren afiliados.

Perú, Paraguay, Brasil, Colombia, Uruguay, Kenia y la Unión Europea, entre otras jurisdicciones, han regulado los fondos de pago electrónicos, definiéndolos, en términos similares, como el valor monetario representado por un crédito exigible a su emisor, almacenado en un soporte electrónico o digital, cuyo valor es constante, denominado en la misma moneda y equivalente a los fondos recibidos por el emisor contra la entrega.[31]

En la ley, las Instituciones de Fondos de Pago Electrónico realizarán servicios de emisión, administración, redención y transmisión de fondos de pago electrónico (*e-money*). La ley apunta que deberá entenderse como fondos de pago electrónico el valor monetario emitido a la par contra la recepción de moneda de curso legal, que servirá para hacer pagos y transferencias.

Esta disposición tiene que ver con la creciente proliferación de los pagos a través de internet y, sobre todo, del teléfono móvil, al que se están sumando gigantes tecnológicos, operadoras de telecomunicaciones, fabricantes de móviles, empresas de distribución y *startups*, que están cambiando la fisonomía del sector, condicionada a su vez por dos grandes elementos transversales: la regulación y la seguridad.

La regulación, que tiene un gran impacto en los modelos de negocio, se desarrolla en distintas capas (sectoriales, de canal, de producto, etcétera), pero está

[31] SEGOB, Subsecretaría de Enlace y Acuerdos Legislativos, oficio núm. SELAP/300/2734/17.

muy fragmentada geográficamente. Estados Unidos fue pionero en la aprobación de normas sectoriales (la primera ley data de 1978), pero está más retrasado en la adopción de algunas regulaciones de producto. La seguridad es otro factor clave, en el que intervienen elementos objetivos (hasta qué punto las transacciones son realmente seguras) y también subjetivos (la percepción, cierta o no, de la realidad).[32]

En este apartado, se presenta un cuadro con el contenido del borrador de las disposiciones aplicables a las Instituciones de Fondos de Pago Electrónico a que se refieren los artículos 48 [segundo párrafo], 54 [primer párrafo] y 56 [primer y segundo párrafo] de la Ley para Regular las Instituciones de Tecnología Financiera. En un anexo se presenta todo el documento con la finalidad de ofrecer al lector un panorama de los avances en la materia para continuar con el reto, como en los otros temas, de empatar estas disposiciones con los nuevos participantes y con el contexto que con ellos se está configurando.

CAPÍTULO	*Tema*
CAPÍTULO I	Deposiciones generales.
CAPÍTULO II	De la seguridad de la información. Sección Primera De la infraestructura tecnológica frente a los clientes. Apartado A. De la celebración de contratos a través de canales de instrucción y las operaciones a través de éstos. Apartado B De la autenticación en los canales de instrucción. Apartado C. De los requerimientos de seguridad de información en los canales de instrucción. Sección Segunda De la infraestructura tecnológica en los procesos internos. Sección Tercera Disposiciones generales para la infraestructura tecnológica.
CAPÍTULO III	De la continuidad operativa.
CAPÍTULO IV	Disposiciones comunes de seguridad de información y de continuidad operativa.
CAPÍTULO V	De la contratación de servicios con terceros y comisionistas.
CAPÍTULO VI	De la evaluación a través terceros independientes.

[32] "Los medios de pago, un paisaje en movimiento", informe del Centro del Sector Financiero de PwC e IE Business School, España, 2015.

TRANSITORIOS	
ANEXO 1	Indicadores de seguridad de la información.
ANEXO 2	Requerimientos mínimos para desarrollar el plan de continuidad de negocio.
ANEXO 3	Incidentes en materia de seguridad de la información.
ANEXO 4	Informe de incidentes de seguridad de la información.
ANEXO 5	Reporte en materia de contingencias operativas.
ANEXO 6	Características de terceros independientes.
ANEXO 7	Requerimientos técnicos para realizar operaciones a través de comisionistas.
ANEXO 8	Formato de información de sistemas y aplicativos (F-SA).

La única constante es el cambio

En el transcurso de estas páginas se han mostrado los elementos más relevantes que han dado pauta para la transformación del sistema financiero internacional y, por supuesto, de los sistemas de cada país. En el caso de México, hemos visto cómo nuestra incorporación al mundo global trajo consigo beneficios y también riesgos en una etapa temprana de la globalización, como los referidos a la crisis de 1994-1995. Entre los riesgos están todas las consecuencias de la crisis en los ámbitos económico, social y político; y en los beneficios, la necesidad de establecer medidas macro y microprudenciales para evitar incurrir en riesgos sistémicos.

México ya tenía en cuenta esta lección cuando sucedió la crisis de 2007-2008. El efecto de este episodio fue menor que en otros países. La lección fue que aprendimos del pasado. Y con esa consigna se ha avanzado a la par de la evolución tecnológica que ha traído consigo innovaciones en participantes, productos, servicios y relaciones del sistema financiero que han ido dando forma a una nueva arquitectura, de la cual se ha hecho un esbozo.

México está siendo cuidadoso, pero, a la vez, está a la vanguardia (la Ley Fintech es un buen ejemplo; el país es pionero y referente en este tema). Las lecciones del pasado exigen actuar con rapidez en un mundo en constante cambio. El objetivo de este trabajo ha sido mostrar los elementos del cambio y seguir sumando. Nuestro recorrido por 50 años de regulación y desregulación; estancamiento tecnológico e innovaciones tecnológicas; configuración, desconfiguración y reconfiguración de nuevos participantes; leyes obsoletas y leyes adecuadas a la realidad, no es más que ubicarnos en donde estamos para saber hacia donde queremos llegar con dos grandes objetivos en mente: estabilidad financiera con inclusión para el desarrollo económico.

Anexo I

Panorama de la Ley para regular las Instituciones de Tecnología Financiera

Título	*Tema*	*Capítulos*
Título I	Disposiciones preliminares; del artículo 1 al 10	
Título II	De las ITF y sus operaciones; del artículo 11 al 34	Capítulo I De las instituciones de financiamiento colectivo
		Capítulo II De las Instituciones de Fondos de Pago Electrónico
		Capítulo III De las operaciones con activos virtuales
Título III	Disposiciones generales; del artículo 35 al 79	Capítulo I De la autorización
		Capítulo II De la operación de las ITF
		Capítulo III De la suspensión y la revocación de la autorización para operar como ITF
		Capítulo IV De la inspección, vigilancia e intercambio de información
		Capítulo V Asociaciones gremiales
Título IV	De las autorizaciones temporales y operación con activos virtuales; del artículo 80 al 95	Capítulo I De la autorización de modelos novedosos
		Capítulo II De los modelos novedosos en entidades reguladas
		Capítulo III De la operación de entidades financieras con activos virtuales
		Capítulo IV Otras obligaciones y de la revocación de las autorizaciones temporales
Título V	Grupo de Innovación Financiera; del artículo 93 al 95	
Título VI	Sanciones y delitos; sel artículo 96 al 127	Capítulo I Sanciones administrativas

		Capítulo II Delitos
Título VII	De las notificaciones; del artículo 128 al 139	
Disposiciones transitorias		

Disposiciones transitorias

Primera	La presente ley entrará en vigor el día siguiente al de su publicación en el *Diario Oficial de la Federación*.
Segunda	La Secretaría de Hacienda y Crédito Público tendrá un plazo de seis meses contado a partir de la entrada en vigor de esta ley para emitir las disposiciones de carácter general a que se refiere el artículo 58 de esta ley. Asimismo, contará con un plazo de 12 meses para emitir las disposiciones de carácter general a que se refiere el artículo 82, fracción VI de esta ley.
Tercera	La Comisión Nacional Bancaria y de Valores contará con los plazos que se señalan a continuación contados a partir de la entrada en vigor de esta ley, para emitir las disposiciones de carácter general siguientes: I. Seis meses para emitir las disposiciones de carácter general a que se refieren los artículos 18, fracción I; 36, fracción IV; 39, fracciones VI, XI, XII y XVI; 44; 45; 48, primer párrafo, para las reglas relacionadas con contabilidad y plan de continuidad de negocio; II. Doce meses para emitir las disposiciones de carácter general a que se refieren los artículos 18, fracción IV; 54; 56, segundo párrafo; 57; 73; 82, fracción VI; 89, fracción IV y 116 de la presente ley, y III. Veinticuatro meses para emitir las disposiciones de carácter general a que se refieren los artículos 55 y 76 de esta ley.
Cuarta	La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros tendrá un plazo de 12 meses, contado a partir de la entrada en vigor de esta ley, para la emisión de las disposiciones de carácter general a que se refiere el artículo 57 de esta ley. Asimismo, contará con un plazo de 12 meses para emitir las disposiciones de carácter general a que se refiere el artículo 82, fracción VI de esta ley.
Quinta	La Comisión Nacional del Sistema de Ahorro para el Retiro y la Comisión Nacional de Seguros y Fianzas tendrán los plazos que se señalan a continuación, contados a partir de la entrada en vigor de esta ley, para emitir las disposiciones de carácter general siguientes: I. Doce meses para emitir las disposiciones de carácter general a que se refieren los artículos 82, fracción VI, y 116 de esta ley, y II. Veinticuatro meses para emitir las disposiciones de carácter general a que se refiere el artículo 76 de esta ley.

Sexta	El Banco de México tendrá los plazos que se señalan a continuación, contados a partir de la entrada en vigor de esta ley, para emitir las disposiciones de carácter general siguientes: I. Seis meses para emitir las disposiciones de carácter general a que se refieren los artículos 26 y 44 de esta ley; II. Doce meses para emitir las disposiciones de carácter general a que se refieren los artículos 30; 32; 46; 57; 82, fracción VI y 116 de esta ley, y III. Veinticuatro meses para emitir las disposiciones de carácter general a que se refiere el artículo 76 de esta ley.
Séptima	La Comisión Nacional Bancaria y de Valores y el Banco de México contarán con un plazo de 12 meses para la emisión conjunta de las disposiciones a que se refieren los artículos 48, 54, 56, segundo párrafo de esta ley, así como para celebrar el convenio previsto en el artículo 71 de este ordenamiento.
Octava	Las personas que a la entrada en vigor del presente ordenamiento se encuentren realizando las actividades reguladas en esta ley deberán dar cumplimiento a la obligación de solicitar su autorización ante la Comisión Nacional Bancaria y de Valores en los términos en que se establezca en las disposiciones de carácter general que para tal efecto se emitan, en un plazo que no exceda de 12 meses, contados a partir de la entrada en vigor de estas disposiciones. Dichas personas podrán continuar realizando tales actividades hasta en tanto la Comisión Nacional Bancaria y de Valores resuelva su solicitud; pero hasta en tanto no reciban la autorización respectiva, deberán publicar en su página de internet o medio que utilice, que la autorización para llevar a cabo dicha actividad se encuentra en trámite, por lo que no es una actividad supervisada por las autoridades mexicanas. En caso de que las personas a que se refiere el párrafo anterior no soliciten su autorización en el plazo de 12 meses previsto en dicho párrafo o no la obtengan una vez solicitada, éstas deberán abstenerse de continuar prestando sus servicios para la celebración de nuevas operaciones y deberán realizar únicamente los actos tendientes a la conclusión o cesión de las operaciones existentes reguladas en esta ley, notificando a sus clientes dicha circunstancia y la forma en que se concluirán o cederán las operaciones. Las autoridades competentes procurarán que en los sitios de internet de sociedades que no obtengan o no cuenten con la autorización correspondiente se alerte a los clientes de los riesgos de operar con dichas entidades y buscarán impedir su oferta en territorio nacional, salvo lo dispuesto en el primer párrafo de este artículo.
Novena	Las personas que se encuentren obligadas a establecer Interfaces de Programación de Aplicaciones informáticas estandarizadas deberán dar cumplimiento a esta obligación en los términos que se establezcan en las disposiciones de carácter general que se emitan, en un plazo que no exceda de seis meses, contando a partir de la entrada en vigor de dichas disposiciones.
Décima	A propuesta de la Secretaría de Hacienda y Crédito Público, la Cámara de Diputados deberá destinar recursos en el Presupuesto de Egresos de la Federación para el desarrollo de las facultades que deba ejercer la Comisión Nacional Bancaria y de Valores y la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros conforme a la presente ley, para el establecimiento del área encargada de preparar e implementar el programa y los lineamientos para las sociedades autorizadas para operar con modelos novedosos regulados en la presente ley.
Décima primera	El Grupo de Innovación Financiera deberá celebrar su primera sesión durante los primeros seis meses posteriores a la entrada en vigor de esta ley. En dicha sesión deberán aprobarse las bases que rijan su organización y funcionamiento.

Leyes modificadas
para hacer realidad la Ley Fintech.

ARTÍCULO SEGUNDO.- Se **ADICIONA** la fracción VII al artículo 103 de la Ley de Instituciones de Crédito, para quedar como sigue:

Artículo 103.- …

…

I. a **VI.** …

VII. Las Instituciones de Tecnología Financiera, así como los usuarios de las instituciones de financiamiento colectivo en las operaciones que realicen en dichas instituciones a que se refiere la Ley para Regular las Instituciones de Tecnología Financiera.

…

ARTÍCULO TERCERO.- Se **REFORMA** el artículo 1, fracciones II y VI, y se **ADICIONA** el artículo 277 Bis 1 de la Ley del Mercado de Valores, para quedar como sigue:

Artículo 1.- …

I. ...

II. La oferta e intermediación de valores**, salvo tratándose de títulos ofrecidos a través de las Instituciones de Tecnología Financiera**.

III. a **V.** …

VI. El desarrollo de sistemas de negociación de valores que permitan la realización de operaciones con éstos**, salvo tratándose de los sistemas ofrecidos a través de las Instituciones de Tecnología Financiera**.

VII. a **VIII.** …

Artículo 227 Bis 1.- La Comisión podrá incluir en las disposiciones generales aplicables a los asesores en inversiones, reglas especiales para los servicios automatizados de asesoría y gestión de inversión.

Los asesores en inversiones, además de las obligaciones a que estén sujetos, deberán cumplir, en lo conducente, con lo dispuesto en los artículos 130, 190 Bis y 190 Bis 1 de esta Ley, conforme a lo previsto en dichos artículos.

ARTÍCULO CUARTO.- Se **REFORMAN** los artículos 57, párrafo sexto y 81-A Bis, párrafo primero, y se **ADICIONA** al artículo 81-A Bis, los párrafos tercero, cuarto y quinto, recorriéndose los subsecuentes en su orden de la Ley General de Organizaciones y Actividades Auxiliares del Crédito, para quedar como sigue:

Artículo 57.- …

…

…

…

…

La Comisión Nacional Bancaria y de Valores, en las visitas de inspección y en el ejercicio de facultades de vigilancia que realice a los centros cambiarios, transmisores de dinero y Sociedades Financieras de Objeto Múltiple no reguladas, podrá revisar, verificar, comprobar y evaluar los recursos, obligaciones y patrimonio, así como las operaciones, funcionamiento, y en general, todo lo que deba constar en los libros, registros, sistemas y documentos para verificar el cumplimiento de los preceptos a que se refiere el artículo 95 Bis de esta Ley y las disposiciones de carácter general que de este deriven. **Para el ejercicio de las funciones de vigilancia, la Comisión Nacional Bancaria y de Valores podrá emitir disposiciones de carácter general para determinar la información que periódicamente deban remitir los centros cambiarios, transmisores de dinero y Sociedades Financieras de Objeto Múltiple no reguladas**.

…

…

Artículo 81-A Bis.- Para efectos de lo previsto en la presente Ley y en las disposiciones que de ella emanen, se entenderá

por transmisor de dinero exclusivamente a la sociedad anónima y sociedad de responsabilidad limitada organizada de conformidad con lo dispuesto en la Ley General de Sociedades Mercantiles que, entre otras actividades, y de manera habitual y a cambio del pago de una contraprestación, comisión, beneficio o ganancia, recibe en el territorio nacional derechos o recursos en moneda nacional o **extranjera**, directamente en sus oficinas o por cable, facsímil, servicios de mensajería, medios electrónicos, transferencia electrónica de fondos o por cualquier vía, **con el único objeto de que**, de acuerdo **con** las instrucciones del remisor, los transfiera al extranjero, a otro lugar dentro del territorio nacional o para entregarlos**, en una sola exhibición,** en el lugar en el que sean recibidos, al beneficiario designado. Asimismo, podrán actuar como transmisores de dinero, las dependencias y entidades de la Administración Pública Federal que conforme a las disposiciones que las regulan, lleven a cabo las operaciones de transmisión de derechos o recursos en moneda nacional o extranjera.

…

Las operaciones a que se refiere este artículo no podrán ser realizadas por agentes relacionados ni por terceros contratados por éstos, sin la intervención de los transmisores de dinero. Se entenderá por agente relacionado a la persona física que, en términos de las disposiciones a que se refiere este artículo, por virtud de una relación contractual con un transmisor de dinero, recibe de éste derechos o recursos en moneda nacional o divisas para entregarlos al beneficiario.

Los transmisores de dinero serán responsables del cumplimiento a las obligaciones establecidas en el artículo 95 Bis de esta Ley, así como de aquellas que deriven de las disposiciones de carácter general a que se refiere dicho artículo, respecto de aquellas operaciones que se celebren a través de los agentes relacionados y respecto de los terceros que éste contrate.

En el caso de que los transmisores de dinero pretendan emitir fondos de pago electrónico o instrumentos de pago que almacenen fondos de pago electrónico, deberán constituirse como una institución de fondo de pago electrónico, en términos de las disposiciones establecidas en la Ley para Regular las Instituciones de Tecnología Financiera.

…

…

ARTÍCULO QUINTO.- Se **REFORMAN** los artículos 3, fracciones V Bis, IX, XII, párrafo primero, XIII y XIV; 6, párrafo primero y 49 Bis 2, párrafo primero, así como la denominación de la Sección VIII del Capítulo V, y se **ADICIONAN** los artículos 2, fracción III Bis; 3, fracciones IV Bis, V Ter, XI Bis, XI Ter, XII, párrafo tercero y 49 Bis 2, párrafo tercero de la Ley para la Transparencia y Ordenamiento de los Servicios Financieros, para quedar como sigue:

Artículo 2. …

I. a **III.** …

III Bis. La Ley para Regular las Instituciones de Tecnología Financiera;

IV. a **IX.** …

Artículo 3. …

I. a **IV.** ...

IV Bis. Consorcio: al 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;

V. …

V Bis. Control: a la capacidad de imponer, directa o indirectamente, de-

cisiones en las asambleas generales de accionistas de la sociedad; 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, y 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;

V Ter. Crédito al Consumo: a las siguientes operaciones celebradas por las Entidades: créditos directos, denominados en moneda nacional, extranjera o en UDIS, así como los intereses que generen, otorgados a personas físicas, derivados de operaciones de crédito, préstamo o financiamiento revolvente asociado a una tarjeta, de créditos personales cuyo monto no exceda el equivalente a tres millones de unidades de inversión, de créditos para la adquisición de bienes de consumo duradero y las operaciones de arrendamiento financiero que sean celebradas con personas físicas;

VI. a **VIII.** …

IX. Entidad Financiera: a las Instituciones de Crédito, a las Sociedades Financieras de Objeto Múltiple reguladas y no reguladas, a las Sociedades Financieras Populares, a las sociedades financieras comunitarias, a las Sociedades Cooperativas de Ahorro y préstamo, a las entidades financieras que actúen como fiduciarias en fideicomisos que otorguen crédito, préstamo o financiamiento al público, las uniones de crédito **y las Instituciones de Tecnología Financiera**;

X. a **XI.** …

XI Bis. Grupo de Personas: a las 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 personas que formen parte de un mismo Consorcio o Grupo Empresarial y las personas o conjunto de personas que tengan el Control de dichas sociedades.

XI Ter. Grupo Empresarial: al 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;

XII. Medio de Disposición: a las tarjetas de débito asociadas a depósitos de dinero a la vista; a las tarjetas de crédito emitidas al amparo de un contrato de apertura de crédito; a los cheques; a las órdenes de transferencia de fondos, incluyendo el servicio conocido como domiciliación; cualquier dispositivo, **tarjeta**, o **interfaz** que permita la realización de pagos, transferencias de recursos **o disposición de efectivo cuyas operaciones se procesen por medio de las Redes de Medios de Disposición**, así como aquellos otros que la Comisión Nacional Bancaria y de Valores y el Banco de México, de manera conjunta, reconozcan como tales mediante disposiciones de carácter general.

…

No quedarán comprendidos en esta definición aquellos medios emitidos al amparo de programas de lealtad o recompensa ofrecidos por personas morales a sus clientes, que sólo puedan ser aceptados por dichas personas morales o por sociedades afiliadas a dichos programas a cambio de bienes, servicios o beneficios, siempre

y cuando no puedan ser convertidos a moneda de curso legal en territorio nacional o en cualquier otra jurisdicción y que las personas morales que los ofrezcan cuenten con un listado de las sociedades afiliadas a dichos programas que, en su conjunto, no podrán ser superiores al 20 por ciento del total de los establecimientos mercantiles habilitados para recibirlos, así como los montos por pago anticipado, que sólo puedan ser aceptados por el emisor o cualquiera de las sociedades que pertenezcan a un mismo Consorcio o Grupo Empresarial del emisor, a cambio de bienes, servicios o beneficios, siempre y cuando no puedan ser convertidas a moneda de curso legal en territorio nacional o en cualquier otra jurisdicción;

XII Bis. ...

XIII. Redes de Medios de Disposición: a la serie de acuerdos, protocolos, instrumentos, interfaces, procedimientos, reglas, programas, sistemas, infraestructura y demás elementos relacionados con el uso de Medios de Disposición, y que, conforme al artículo 4 Bis 3, corresponde regular de manera conjunta a la Comisión Nacional Bancaria y de Valores y al Banco de México**, y**

XIV. Sistema de Pagos: a la serie de instrumentos, procedimientos, reglas y sistemas para la transferencia de fondos.

Artículo 6. Las Instituciones de Crédito y las Sociedades Financieras de Objeto Múltiple reguladas**, así como las Instituciones de Tecnología Financiera,** deberán registrar ante el Banco de México las Comisiones que pretendan cobrar por los servicios de pago y créditos que ofrecen al público, así como sus respectivas modificaciones. Dicho registro se realizará con al menos treinta días naturales de anticipación a la entrada en vigor de las nuevas Comisiones **o de las modificaciones a las previamente registradas** cuando impliquen un incremento.

…

…

…

…

…

Sección VIII

Sanciones que corresponde imponer al Banco de México o *a la Comisión Nacional Bancaria y de Valores*

Artículo 49 Bis 2. La Comisión Nacional Bancaria y de Valores sancionará con multa de 5,000 a 20,000 veces la Unidad de Medida y Actualización, a las Entidades **y Participantes en Redes** que infrinjan cualquier disposición de esta Ley o las disposiciones de carácter general que expidan, de manera conjunta la Comisión Nacional Bancaria y de Valores y el Banco de México, en términos de esta Ley en relación con las Redes de Medios de Disposición a que se refiere el artículo 4 Bis 3. En caso de reincidencia, la Comisión Nacional Bancaria y de Valores podrá imponer sanciones equivalentes hasta por el doble de la prevista en este párrafo.

…

En caso de que la Comisión Nacional Bancaria y de Valores o el Banco de México, en ejercicio de sus respectivas facultades, detecte actos u omisiones de las Entidades o Participantes en Redes que pudieran implicar infracciones a las disposiciones que les resulten aplicables en términos de la presente Ley, lo hará del conocimiento de la otra autoridad. Para efectos de lo anterior, la Comisión Nacional Bancaria y de Valores y el Banco de México celebrarán un convenio de colaboración por el que establezcan la forma y términos para darse a conocer lo previsto en el

presente párrafo, así como las medidas que adopten en el ejercicio de sus atribuciones.

ARTÍCULO SEXTO.- Se **REFORMAN** los artículos 2, fracción V, y 28, párrafo primero, de la Ley para Regular las Sociedades de Información Crediticia, para quedar como sigue:

Artículo 2o.- …

I. a **IV.** …

V. Entidad Financiera, aquella autorizada para operar en territorio nacional y que las leyes reconozcan como tal, incluyendo a aquellas a que se refiere el artículo 12 de la Ley para Regular las Agrupaciones Financieras; la banca de desarrollo; los organismos públicos cuya actividad principal sea el otorgamiento de créditos, así como los fideicomisos de fomento económico constituidos por el Gobierno Federal; las uniones de crédito; las Sociedades **Cooperativas** de Ahorro y préstamo, **las sociedades financieras comunitarias, las Instituciones de Tecnología Financiera y**, con excepción de las Sofom E.N.R., continuarán considerándose Entidades Financieras las personas mencionadas, no obstante que se encuentren en proceso de disolución, liquidación o extinción, según corresponda;

VI a **XV.** …

Artículo 28.- Las Sociedades sólo podrán proporcionar información a un Usuario, cuando este cuente con la autorización expresa del Cliente, mediante su firma, en donde conste de manera fehaciente que tiene pleno conocimiento de la naturaleza y alcance de la información que la Sociedad proporcionará al Usuario que así la solicite, del uso que dicho Usuario hará de tal información y del hecho de que éste podrá realizar consultas periódicas de su historial crediticio, durante el tiempo que mantenga relación jurídica con el Cliente. **La firma a que se refiere este párrafo podrá ser recabada de manera autógrafa o por medios electrónicos, en este último caso, siempre que cumpla con los términos y condiciones establecidos por el Banco de México**.

…

…

…

…

…

…

…

…

…

…

ARTÍCULO SÉPTIMO.- Se **REFORMA** el artículo 2, fracción IV, y se **ADICIONA** un párrafo cuarto al artículo 50 Bis, recorriéndose el párrafo subsecuente de la Ley de Protección y Defensa al Usuario de Servicios Financieros, para quedar como sigue:

Artículo 2o.- …

I. a **III.** …

IV. Institución Financiera, en singular o plural, a las sociedades controladoras, Instituciones de Crédito, Sociedades Financieras de Objeto Múltiple, sociedades de información crediticia, casas de bolsa, fondos de inversión, Almacenes Generales de Depósito, uniones de crédito, casas de cambio, instituciones de seguros, sociedades mutualistas de seguros, instituciones de fianzas, administradoras de fondos para el retiro, PENSIONISSSTE, empresas operadoras de la base de datos nacional del sistema de ahorro para el retiro, Instituto del Fondo Nacional para el Consumo de los Trabajadores, Sociedades Cooperativas de Ahorro y préstamo, Sociedades Financieras Populares, sociedades financieras comunitarias, **las Instituciones de Tecnología Financiera**, y cualquiera otra sociedad que requiera de la autorización de la Secretaría de Hacienda y Crédito Público o

de cualesquiera de las Comisiones Nacionales para constituirse y funcionar como tales y ofrecer un producto o servicio financiero a los Usuarios;

V. a **IX.** …

Artículo 50 Bis.- ...

I. a **V.** …

…

…

En el caso de que las Instituciones Financieras no tengan sucursales u oficinas de atención al público, no les serán aplicables las obligaciones previstas en la fracción II del párrafo primero y el párrafo tercero de este artículo. Dichas Instituciones Financieras solamente deberán señalar los datos de contacto de su Unidad Especializada en un lugar visible y de fácil acceso al público general en el medio electrónico que utilicen para ofrecer sus servicios.

…

ARTÍCULO OCTAVO.- Se **REFORMAN** los artículos 3, párrafo primero, y 12, párrafo primero de la Ley para Regular las Agrupaciones Financieras, para quedar como sigue:

Artículo 3o.- Las entidades financieras no deberán utilizar denominaciones iguales o semejantes a las de otras entidades financieras, actuar de manera conjunta, ofrecer servicios complementarios ni, en general, ostentarse en forma alguna como integrantes de Grupos Financieros, salvo cuando se trate de integrantes de Grupos Financieros que se encuentren organizados y funcionen conforme a las disposiciones de la presente Ley. **Las instituciones reguladas en la Ley para Regular las Instituciones de Tecnología Financiera no podrán utilizar denominaciones iguales o semejantes a las de otras entidades financieras, aún y cuando sean integrantes de Grupos Financieros**.

…

Artículo 12.- Los Grupos Financieros a que se refiere la presente Ley estarán compuestos por una Sociedad Controladora y por algunas de las entidades financieras siguientes que sean consideradas integrantes del Grupo Financiero: Almacenes Generales de Depósito, casas de cambio, instituciones de fianzas, instituciones de seguros, casas de bolsa, instituciones de banca múltiple, sociedades operadoras de fondos de inversión, distribuidoras de acciones de fondos de inversión, administradoras de fondos para el retiro, Sociedades Financieras de Objeto Múltiple, Sociedades Financieras Populares, **Instituciones de Tecnología Financiera y las demás entidades financieras susceptibles de ser integrantes de Grupos Financieros en términos de las reglas que emita la Secretaría**.

…

…

…

…

ARTÍCULO NOVENO.- Se **REFORMA** el artículo 3, fracción IV, inciso a) de la Ley de la Comisión Nacional Bancaria y de Valores para quedar como sigue:

Artículo 3.- …

I. a **III.** …

IV. …

a) A las sociedades controladoras **y subcontroladoras** de grupos financieros, Instituciones de Crédito, casas de bolsa, bolsas de valores, **fondos** de inversión, sociedades operadoras de **fondos** de inversión, sociedades distribuidoras de acciones de **fondos** de inversión, Almacenes Generales de Depósito, uniones de crédito, casas de cambio, Sociedades Financieras de Objeto Múltiple reguladas, Sociedades Financieras Populares, instituciones para el depósito de valores, contrapartes centrales, instituciones calificadoras de valores, **Instituciones de Tecnología Financiera,** sociedades de información crediticia,

sociedades financieras comunitarias, sujetas a la supervisión de la Comisión y los organismos de integración financiera rural, así como otras instituciones y fideicomisos públicos que realicen actividades financieras y respecto de los cuales la Comisión ejerza facultades de supervisión, todas ellas constituidas conforme a las leyes mercantiles y financieras.

b) …

V. a **VIII.** …

ARTÍCULO DÉCIMO.- Se **REFORMAN** los artículos 3, fracción VI y 15, fracción I, y se **ADICIONA** la fracción XVI al artículo 17 de la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita, para quedar como sigue:

Artículo 3. …

I. a **V.** …

VI. Entidades Financieras, aquellas reguladas en los artículos 115 de la Ley de Instituciones de Crédito; 87-D, 95 y 95 Bis de la Ley General de Organizaciones y Actividades Auxiliares del Crédito; 129 de la Ley de Uniones de Crédito; 124 de la Ley de Ahorro y Crédito Popular; 71 y 72 de la Ley para Regular las Actividades de las Sociedades Cooperativas de Ahorro y Préstamo; 212 de la Ley del Mercado de Valores; 91 de la Ley de Fondos de Inversión; 108 Bis de la Ley de los Sistemas de Ahorro para el Retiro; 492 de la Ley de Instituciones de Seguros y de Fianzas **y 58 de la Ley para Regular las Instituciones de Tecnología Financiera**;

VII. a **XIV.** …

Artículo 15. …

I. Establecer medidas y procedimientos para prevenir y detectar actos, omisiones u operaciones que pudieran ubicarse en los supuestos previstos en el Capítulo II del Título Vigésimo Tercero del Código Penal Federal, así como para identificar a sus clientes y usuarios; de conformidad con lo establecido en los artículos 115 de la Ley de Instituciones de Crédito; 87-D, 95 y 95 Bis de la Ley General de Organizaciones y Actividades Auxiliares del Crédito; 129 de la Ley de Uniones de Crédito; 124 de la Ley de Ahorro y Crédito Popular; 71 y 72 de la Ley para Regular las Actividades de las Sociedades Cooperativas de Ahorro y Préstamo; 212 de la Ley del Mercado de Valores; 91 de la Ley de Fondos de Inversión; 108 Bis de la Ley de los Sistemas de Ahorro para el Retiro; 492 de la Ley de Instituciones de Seguros y de Fianzas **y 58 de la Ley para Regular las Instituciones de Tecnología Financiera**;

II. a **IV.** …

Artículo 17. …

I. a **XV.** …

XVI. El ofrecimiento habitual y profesional de intercambio de activos virtuales por parte de sujetos distintos a las Entidades Financieras, que se lleven a cabo a través de plataformas electrónicas, digitales o similares, que administren u operen, facilitando o realizando operaciones de compra o venta de dichos activos propiedad de sus clientes o bien, provean medios para custodiar, almacenar, o transferir activos virtuales distintos a los reconocidos por el Banco de México en términos de la Ley para Regular las Instituciones de Tecnología Financiera. Se entenderá como activo virtual toda representación de valor registrada electrónicamente y utilizada entre el público como medio de pago para todo tipo de actos jurídicos y cuya transferencia únicamente puede 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 divisas.

Serán objeto de Aviso ante la Secretaría cuando el monto de la operación de compra o venta que realice cada cliente de quien realice la actividad vulnerable a

que se refiere esta fracción sea por una cantidad igual o superior al equivalente a seiscientas cuarenta y cinco Unidades de Medida y Actualización.

En el evento de que el Banco de México reconozca en términos de la Ley para Regular las Instituciones de Tecnología Financiera activos virtuales, las personas que provean los medios a que se refiere esta fracción deberán obtener las autorizaciones correspondientes en los plazos que señale dicho Banco de México en las disposiciones respectivas.

…

…

DISPOSICIÓN TRANSITORIA

ÚNICO.- La adición de la fracción XVI del artículo 17 a esta Ley entrará en vigor a los dieciocho meses siguientes a la entrada en vigor del presente Decreto.

TRANSITORIO

ÚNICO.- El presente Decreto entrará en vigor el día siguiente de su publicación en el Diario Oficial de la Federación, salvo que en las Disposiciones Transitorias de este Decreto se disponga lo contrario.

ANEXO 2

Borrador de las Disposiciones aplicables a las Instituciones de Fondos de Pago Electrónico

Borrador de las Disposiciones aplicables a las Instituciones de Fondos de Pago Electrónico

Borrador de las Disposiciones aplicables a las Instituciones de Fondos de Pago Electrónico a que se refieren los artículos 48 [segundo párrafo], 54 [primer párrafo] y 56 [primer y segundo párrafo] de la Ley para Regular las Instituciones de Tecnología Financiera.

(Presentado el 22 de enero de 2020 para su discusión en las instancias petinentes).

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1.- Para efectos de las presentes Disposiciones, se entenderá, en singular o plural, además de los términos utilizados en la Ley para Regular las Instituciones de Tecnología Financiera, los siguientes:

Administrador de comisionistas:	a la persona que, en términos del artículo 46 de estas Disposiciones, organiza una red de comisionistas y funge como intermediario entre éstos y la Institución de Fondos de Pago Electrónico, para que dichos comisionistas celebren con los Clientes operaciones y servicios.
Autenticación:	a la verificación de la identidad de (i) un Cliente, con el fin de permitirle la realización de las Operaciones que éste requiera, o bien, (ii) un Usuario de la Infraestructura Tecnológica de la Institución de Fondos de Pago Electrónico de que se trate, con el fin de que aquél pueda acceder, utilizar u operar algún componente de dicha Infraestructura Tecnológica.
Canales de instrucción:	a los equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones que forman parte de la Infraestructura Tecnológica de la Institución de Fondos de Pago Electrónico de que se trate y que, a través de ellos, ésta permite al Cliente realizar Operaciones.

Cifrado:	al mecanismo que deberán utilizar las Instituciones de Fondos de Pago Electrónico para proteger la confidencialidad de la información mediante métodos criptográficos en los que se utilicen algoritmos y llaves de encriptación.
Cómputo en la Nube:	al modelo de servicios de cómputo prestados por un tercero, bajo demanda y en infraestructura compartida, privada o híbrida, independientemente de la ubicación física de la infraestructura tecnológica del tercero, que puede consistir, entre otros, en uno o más de los siguientes esquemas de servicios digitales: de infraestructura como servicio, de plataforma como servicio o de software como servicio.
Contingencia Operativa:	a cualquier evento que dificulte, limite o impida a una Institución de Fondos de Pago Electrónico realizar sus Operaciones o aquellos procesos que pudieran tener una afectación a sus Clientes o a la propia Institución de Fondos de Pago Electrónico.
Cuenta:	a aquella que la Institución de Fondos de Pago Electrónico, de conformidad con el artículo 22, fracción I, de la Ley, abra a nombre de cada uno de sus Clientes en la que, entre otros, realiza los registros de (a) abonos correspondientes a (i) la cantidad de fondos de pago electrónico que aquella emita a favor de éste, contra la recepción de una cantidad de dinero, en moneda nacional o sujeto a la autorización del Banco de México, en moneda extranjera, o (ii) la cantidad de fondos de pago electrónico objeto de las Transferencias de Fondos de Pago Electrónico de que se trate, así como (b) los cargos que correspondan por (i) la disposición de dichos fondos o (ii) la cantidad de fondos de pago electrónico objeto de las Transferencias de Fondos de Pago Electrónico.
Evento de Seguridad de la Información:	a cualquier suceso, interno o externo, relacionado, entre otros, con Clientes, terceros contratados por la Institución de Fondos de Pago Electrónico, personas o procesos operativos, así como con componentes de la Infraestructura Tecnológica, dispositivos, medios físicos u otros elementos que almacenen información, que constituya algún indicio de la afectación en la confidencialidad, integridad o disponibilidad de la información que dicha institución gestione o a la cual tenga acceso en la propia Infraestructura Tecnológica.
Factor de Autenticación:	al mecanismo de Autenticación, basado en las características físicas del Cliente, en dispositivos o información que sólo el Cliente posea o conozca, conforme a lo previsto en el Artículo 5 de las presentes Disposiciones.
Identificador de Cliente:	a la cadena de caracteres alfanuméricos, o la información de un dispositivo o cualquier otra información, que conozca tanto la Institución de Fondos de Pago Electrónico como el Cliente titular de la respectiva Cuenta que ésta administre, que permita identificarlo por medio del Canal de Instrucción de dicha Institución de Fondos de Pago Electrónico. Entre otros, el Identificador de Clientes podrá ser el número de la línea del teléfono móvil que el Cliente cuentahabiente utilice para acceder a los Canales de Instrucción, la dirección de correo electrónico, el número de la Tarjeta u otro identificador único asociado al uso del Canal de Instrucción correspondiente.

Incidente de Seguridad de Información:	a cualquier suceso, interno o externo, relacionado, entre otros, con Clientes, terceros contratados por la Institución de Fondos de Pago Electrónico, personas y procesos operativos, así como con componentes de la Infraestructura Tecnológica, dispositivos, medios físicos, u otros elementos que almacenen información, que: a) Comprometa la confidencialidad, integridad o disponibilidad de uno o más componentes de la Infraestructura Tecnológica con un efecto adverso para la Institución de Fondos de Pago Electrónico, sus Clientes, terceros, proveedores o contrapartes, entre otros. b) Vulnere la Infraestructura Tecnológica de tal forma que comprometa la información que procesa, almacena o transmite. c) Constituya una violación de las políticas y procedimientos de seguridad de la información. d) Constituya la materialización de un menoscabo en la Institución de Fondos de Pago Electrónico, 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 o robo, de una interrupción de las actividades realizadas por la propia institución ocasionada por alguna acción o de atentados contra las infraestructuras interconectadas conocidos como ciberataques.
Información Personal:	a la conjunción del nombre, apellidos y otro elemento de información que permita identificar al Cliente o al receptor de Transferencias, tales como: domicilio, números de teléfono o direcciones de correo electrónico, entre otros.
Información Sensible:	a la conjunción del nombre, apellidos u otro elemento de información que permita identificar al Cliente o al receptor de Transferencias, así como la información de Identificador del Cliente, de las Cuentas, de los números de Tarjetas, de la información de Operaciones previas, información que permita la Autenticación o demás datos de naturaleza financiera.
Mecanismo de Identificación:	al conjunto de técnicas y procedimientos utilizados para verificar la autenticidad de la información y los documentos que las Instituciones de Fondos de Pago Electrónico recaban de sus Clientes, de conformidad con el Artículo 10 de las disposiciones de carácter general a que se refiere el Artículo 58 de la Ley para Regular las Instituciones de Tecnología Financiera.
Órgano de Administración:	al administrador único o al consejo de administración de una Institución de Fondos de Pago Electrónico, según sea el caso.
Plan de Continuidad de Negocio:	al documento que integra el conjunto de estrategias, procedimientos y acciones previamente determinadas por la Institución de Fondos de Pago Electrónico que corresponda, para permitir, ante la ocurrencia de Contingencias Operativas, la continuidad en las Operaciones, actividades o en la realización de los procesos críticos de dicha Institución de Fondos de Pago Electrónico, o bien, su restablecimiento oportuno, así como la mitigación de las afectaciones producto de dichas Contingencias Operativas.

Plan Director de Seguridad:	al documento que integra el conjunto de proyectos determinadas por la Institución de Fondos de Pago Electrónico que corresponda, que deban ser ejecutados a corto, mediano y largo plazos, para establecer una correcta gestión de seguridad de la información y evitar que los Eventos de Seguridad de Información se materialicen en Incidentes de Seguridad de Información.
Política Estratégica de Continuidad de Negocio y de Seguridad de la Información	al documento que integra las estrategias de la Institución de Fondos de Pago Electrónico en materia de continuidad de negocio y seguridad de la información relacionados con su operación, de conformidad con las presentes Disposiciones, sin perjuicio de cualquier otro elemento en materia de administración de riesgos sujeta a las disposiciones de carácter general que, al efecto, emita la CNBV de conformidad con el artículo 48 de la Ley.
Sesión:	al periodo en el cual el Cliente titular de una Cuenta que administre la Institución de Fondos de Pago Electrónico podrá llevar a cabo consultas de saldos o de sus Operaciones realizadas o iniciar aquellas otras, una vez que haya ingresado al Canal de Instrucción con su Identificador del Cliente.
Tarjeta:	al medio de disposición de los fondos de pago electrónico registrados en la Cuenta de que se trate, constituido como el conjunto de datos que, al procesarse mediante sistemas determinados, permiten iniciar una instrucción de cargo a dicha Cuenta, distinta a aquella otra instrucción que se realice para ejecutar una Transferencia.
Tercero Independiente:	al profesionista competente para realizar labores de evaluación sobre el cumplimiento de los requisitos que las Instituciones de Fondos de Pago Electrónico deben cumplir conforme a estas Disposiciones, quien es externo a la Institución de Fondos de Pago Electrónico y que cumple, en lo conducente, con las características y requisitos previstos en el artículo 58 de estas Disposiciones.
Transferencia:	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 u otra entidad ubicada en territorio extranjero que preste servicios de emisión, administración, redención y transmisión de fondos de pago electrónico similares a los que prestan las Instituciones de Fondos de Pago Electrónico en México, en términos de la legislación aplicable, conforme a la cual la primera realiza (i) el abono en una Cuenta 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 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 designada al efecto. Asimismo, 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 Cuenta, 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.

UDI:	a las unidades de cuenta llamadas "Unidades de Inversión" establecidas en el "Decreto por el que se establecen las obligaciones que podrán denominarse en Unidades de Inversión y reforma y adiciona diversas disposiciones del Código Fiscal de la Federación y de la Ley del Impuesto sobre la Renta", publicado en el Diario Oficial de la Federación el 1 de abril de 1995, tal como ése sea modificado o adicionado de tiempo en tiempo.
Usuario de la Infraestructura Tecnológica:	a la persona o componente de la Infraestructura Tecnológica de la Institución de Fondos de Pago Electrónico, que cuente con la autorización respectiva para que acceda, utilice u opere algún componente de ésta. No quedarán comprendidos en esta definición los Clientes de la Institución de Fondos de Pago Electrónico.

CAPÍTULO II
DE LA SEGURIDAD DE LA INFORMACIÓN

Sección Primera
De la Infraestructura Tecnológica frente a los Clientes

Apartado A
De la celebración de contratos a través de Canales de Instrucción y las Operaciones a través de éstos

Artículo 2.- Las Instituciones de Fondos de Pago Electrónico, al pactar la celebración de Operaciones y la prestación de servicios a través de Canales de Instrucción, deberán requerir el consentimiento expreso de sus Clientes para dichos efectos, el cual se podrá obtener a través del proceso de Autenticación referido en el artículo 7 de las presentes Disposiciones. Adicionalmente, en este mismo supuesto, las Instituciones de Fondos de Pago Electrónico deberán:

I. En la contratación respectiva, establecer de manera clara y precisa, lo siguiente:

   a) Las Operaciones y servicios que podrán realizar y proporcionar a través de dichos Canales de Instrucción.
   b) Los mecanismos y procedimientos para la Autenticación del Cliente, así como las responsabilidades de éste y de la Institución de Fondos de Pago Electrónico respecto de la celebración de Operaciones y la prestación de servicios a través del Canal de Instrucción respectivo.
   c) Los mecanismos y procedimientos para la notificación al Cliente de las Operaciones realizadas y servicios prestados por las Instituciones de Fondos de Pago Electrónico a través de los Canales de Instrucción.
   d) Los mecanismos y procedimientos de cancelación de la contratación de servicios, los cuales deberán ser similares a los de la propia contratación, considerando los Canales de Atención al Cliente y Mecanismos de Identificación del Cliente y procedimientos para su Autenticación.
   e) Las restricciones operativas aplicables de acuerdo al Canal de Instrucción de que se trate, de

conformidad con lo previsto en este Capítulo.

II. Informar a sus Clientes, previamente a la contratación, los términos y condiciones para el uso de los Canales de Instrucción, debiendo mantener dicha información disponible para su consulta en cualquier momento.
III. Informar a sus Clientes los riesgos inherentes a la utilización de los Canales de Instrucción respectivos, así como hacer de su conocimiento sugerencias para prevenir la realización de actos no autorizados por ellos o cualesquier otros irregulares o ilegales por los que se puedan llevar a cabo Operaciones referidas a las Cuentas de las que éstos sean titulares.

Artículo 3.- Las Instituciones de Fondos de Pago Electrónico podrán permitir a sus Clientes: (i) la contratación de Operaciones y servicios adicionales a los originalmente convenidos, (ii) modificar los términos y condiciones para la prestación de los servicios anteriormente convenidos, previo consentimiento expreso de sus Clientes, el cual podrá obtenerse por dichas instituciones a través del proceso de Autenticación referido en el Artículo 7 de las presentes Disposiciones, desde el Canal de Instrucción de que se trate, o bien, (iii) contratar el uso de otro Canal de Instrucción, siempre y cuando la Institución de Fondos de Pago Electrónico requiera, para ello, al menos, un Factor de Autenticación.

Artículo 4.- Las Instituciones de Fondos de Pago Electrónico deberán notificar a sus respectivos Clientes, en un periodo no mayor a tres segundos, por los medios pactados con ellos que hayan elegido de entre los ofrecidos por dichas instituciones para tal fin, cuando, a través de Canales de Instrucción, se ejecute cualquiera de las Operaciones o se solicite a las Instituciones de Fondos de Pago Electrónico alguno de los servicios que ofrezcan, en los siguientes casos:

I. Transferencias y entrega de cantidades de dinero derivado del cargo a la Cuenta del Cliente de que se trate;
II. Alta o modificación del medio de notificación al Cliente, en cuyo caso la Institución de Fondos de Pago Electrónico respectiva deberá enviar la notificación a que este artículo se refiere por el medio previamente pactado con el Cliente, así como por el nuevo medio;
III. Contratación de otro servicio provisto a través de Canales de Instrucción o modificación de los términos y condiciones para el uso del servicio previamente contratado, y
IV. Desactivación, reactivación y modificación de los Factores de Autenticación.

Las Instituciones de Fondos de Pago Electrónico estarán exceptuadas de enviar la notificación prevista en el primer párrafo de este artículo, respecto del supuesto referido en la fracción I anterior en caso de que el monto acumulado diario de las Operaciones realizadas conforme a este mismo artículo no supere al equivalente en moneda nacional a 60 UDIS, o bien, cuando, cada una en lo individual no supere el equivalente en moneda nacional a 25 UDIS.

Las Instituciones de Fondos de Pago Electrónico deberán asegurarse de que la notificación que al efecto envíen conforme a este artículo no contenga Información Personal o Información Sensible del Cliente. No obstante, las Instituciones de Fondos de Pago Electrónico deberán habilitar mecanismos para que sus Clientes puedan, a su elección, recibir la información del saldo de la Cuenta en virtud de los servicios prestados a través de los Canales de Instrucción.

Apartado B
De la Autenticación
en los Canales de Instrucción

Artículo 5.- Para efectos de las presentes Disposiciones, los Factores de Autenticación que las Instituciones de Fondos de Pago Electrónico deberán utilizar sólo podrán incluir la información perteneciente a cualquiera de las siguientes categorías:

I. Información que la Institución de Fondos de Pago Electrónico proporciona al Cliente o permite a esta persona generar, bajo el entendido de que solamente dicha persona la conozca, para que la pueda ingresar al sistema autorizado por la Institución de Fondos de Pago Electrónico para iniciar la Operación de que se trate. Los Factores de Autenticación a que se refiere esta fracción deberán cumplir con cualquiera de los siguientes esquemas:

   A. Contraseñas que cumplan, cuando menos, con lo siguiente:

      a) Deberá estar compuesta, al menos, por seis caracteres consecutivos e incluir caracteres alfanuméricos.
      b) En ningún caso, se podrá utilizar como las contraseñas, la información siguiente:

         i. El Identificador de Cliente.
         ii. La denominación o marca comercial de la Institución de Fondos de Pago Electrónico.
         iii. Más de tres caracteres idénticos en forma consecutiva.
         iv. Más de tres caracteres numéricos y alfabéticos en forma secuencial.

   B. Cuestionarios realizados a través de canales electrónicos de mensajería, de centros de atención telefónica o por agentes automatizados, siempre que observen lo siguiente:

      a) Se requieran datos que el Cliente conozca y que las Instituciones de Fondos de Pago Electrónico puedan validar, manteniendo la debida confidencialidad de dicha información.
      b) Se defina un conjunto de preguntas abiertas en cuestionarios de, al menos, tres preguntas y, en el evento de que la respuesta a una de ellas sea incorrecta, se podrá formular una pregunta adicional. En ningún caso, las respuestas a estas preguntas podrán ser datos que se muestren en el Canal de Instrucción ni se encuentren en comunicaciones impresas o electrónicas enviadas por las Instituciones de Fondos de Pago Electrónico a sus Clientes.
      c) Se validen las respuestas proporcionadas por sus Clientes a través de herramientas informáticas, sin que el operador o sistema automatizado pueda consultar o acceder a los datos de Autenticación de los Clientes.

Las Instituciones de Fondos de Pago Electrónico permitirán a sus Clientes cambiar los Factores de Autenticación de esta categoría, cuando estos últimos así lo requieran, en los términos previstos en las presentes disposiciones.

Las Instituciones de Fondos de Pago Electrónico podrán utilizar cuestionarios para desbloquear los Factores de Autenticación que previamente hayan sido bloqueados.

II. Información contenida, recibida o generada por medios o dispositivos electrónicos que sólo posee el Cliente, incluida la obtenida por dispositivos o aplicativos generadores de contraseñas dinámicas que la Institución de Fondos de Pago Electrónico proporcione al Cliente, así como aquella que permita asociar medios o dispositivos electrónicos a un Cliente a través de mecanismos seguros de intercambio de credenciales o llaves criptográficas. Lo anterior quedará sujeto a que la información sea contenida, recibida o generada y cumpla con las características siguientes:

    a) Contar con propiedades que impidan su duplicación o alteración.
    b) Sea información dinámica que no pueda ser utilizada en más de una ocasión con una vigencia que no podrá ser mayor a dos minutos, o sea información dinámica generada para la realización de una operación, así como operaciones subsecuentes sin modificación alguna, en cuyo caso será considerada, para efectos del presente inciso, como un elemento independiente para autenticar las operaciones como autorizadas por el Cliente únicamente para la primera operación en que se utilice.
    c) No sea conocida con anterioridad a su generación y a su uso por los funcionarios, empleados, representantes de la Institución de Fondos de Pago Electrónico o por terceros.

Las Instituciones de Fondos de Pago Electrónico podrán proporcionar a sus Clientes medios o dispositivos que generen Contraseñas dinámicas de un solo uso, las cuales utilicen información de la Operación, mediante la captura de datos, de manera que dicha Contraseña únicamente pueda ser utilizada para la Operación solicitada. En este caso, no será aplicable la vigencia dispuesta en el inciso b) de la presente fracción.

III. Información derivada de características propias del Cliente, tales como aquellas de carácter biométrico, huellas dactilares, geometría de la mano o de la cara, patrones en iris o retina, entre otros. Para el uso de esta información se deberá contar con la previa autorización de la CNBV y del Banco de México.

En todo caso, se considerará que dos o más Factores de Autenticación son independientes si la vulneración de uno de los Factores de Autenticación no compromete la fiabilidad de los demás.

Artículo 6.- Las Instituciones de Fondos de Pago Electrónico podrán solicitar a la CNBV y al Banco de México que autoricen el uso de Factores de Autenticación referidos en las fracciones I y II del artículo anterior con características distintas a las señaladas en dicho artículo, así como la utilización de la información señalada en la fracción III de dicho artículo, siempre que acrediten que la tecnología utilizada, a juicio de ambas Autoridades Financieras, resulta fiable para autenticar a sus Clientes.

La solicitud para obtener la referida autorización deberá contener lo siguiente:

I. La descripción detallada del proceso, el cual deberá ser aprobado por el Órgano de Administración, así como la tecnología empleada en cada parte de éste.
II. La descripción de los medios necesarios para la transmisión y resguardo de la información que garanticen su integridad, la correcta lectura de los datos, la imposibilidad de manipulación, así como su adecuada conservación y disponibilidad.

Para el caso de la fracción III del artículo 5 de estas Disposiciones, la Institución de Fondos de Pago Electrónico que formule la solicitud referida deberá presentar adicionalmente la evidencia recabada de pruebas controladas, obtenida por la misma Institución de Fondos de Pago Electrónico o por una empresa especializada en certificación de tales Factores de Autenticación, con la capacidad de presentar reportes de que la solución tecnológica y los métodos utilizados son efectivos para autenticar a sus Clientes, comparando la eficacia del Factor de Autenticación de que se trate con aquélla de algún otro Factor de Autenticación recabado y procesado de conformidad con los estándares internacionales correspondientes.

Las Instituciones de Fondos de Pago Electrónico deberán contar con mecanismos y procedimientos para asegurar que, en el uso de los Factores de Autenticación a que se refiere la fracción III del artículo 5, la información transmitida para el proceso de Autenticación sea distinta cada vez que sea generada, de forma que en ningún caso se pueda utilizar nuevamente o duplicarse.

Las Instituciones de Fondos de Pago Electrónico deberán presentar las solicitudes y demás información a que se refiere a este artículo al Banco de México y a la CNBV, mediante correo electrónico enviado a la cuenta ifpe@banxico.org.mx y en la oficialía de partes de la CNBV.

Artículo 7.- Las Instituciones de Fondos de Pago Electrónico, a efecto de permitir el acceso a los Canales de Instrucción, deberán llevar a cabo la Autenticación del Cliente. Para realizar la Autenticación, las Instituciones de Fondos de Pago Electrónico deberán recabar y validar al menos:

I. El Identificador de Cliente, y
II. Un Factor de Autenticación.

El Identificador de Cliente deberá ser único para cada Cliente y deberá asociarse a todas las Operaciones realizadas por ellos de que se trate.

Asimismo, las Instituciones de Fondos de Pago Electrónico deberán guardar evidencia de la Autenticación conforme a lo establecido en el artículo 29, fracción IV, de las presentes Disposiciones.

Artículo 8.- Las Instituciones de Fondos de Pago Electrónico deberán solicitar al menos dos Factores de Autenticación independientes en cada ocasión en que se pretenda realizar lo siguiente:

I. Alta y baja de beneficiarios de la Cuenta a que se refiere el artículo 19 de la Ley.
II. Cambios respecto de los Factores de Autenticación.
III. Solicitud de estados de Cuenta.
IV. Alta y modificación del medio de notificación al Cliente.

Las Instituciones de Fondos de Pago Electrónico deberán apegarse a lo establecido en la Circular 12/2018 emitida por el Banco de México para los casos en que sus Clientes no

reconozcan las Operaciones que no hayan sido instruidas con al menos dos Factores de Autenticación independientes.

Para efectos de lo previsto en el presente artículo, las Instituciones de Fondos de Pago Electrónico podrán tomar en cuenta el Factor de Autenticación utilizado para el inicio de Sesión en los Canales de Instrucción de que se trate.

Artículo 9.- Las Instituciones de Fondos de Pago Electrónico deberán contar con políticas y procedimientos para asegurar que, en la generación, entrega, almacenamiento, desbloqueo y restablecimiento de los Factores de Autenticación, únicamente sea el Cliente quien los reciba, active, conozca, desbloquee y restablezca.

Tratándose de contraseñas definidas o generadas por las Instituciones de Fondos de Pago Electrónico durante el restablecimiento de éstas, las propias instituciones deberán prever mecanismos y procedimientos por medio de los cuales el Cliente deba modificarlos inmediatamente después de iniciar la Sesión correspondiente, cuando así sea requerido según el tipo de Canal de Instrucción, y previo a la realización de cualquier Operación, validando que las Contraseñas sean diferentes a las definidas por las propias Instituciones de Fondos de Pago Electrónico.

Apartado C
De los requerimientos de seguridad de información en los Canales de Instrucción

Artículo 10.- Las Instituciones de Fondos de Pago Electrónico deberán establecer mecanismos y procedimientos para que sus Clientes, al acceder a los Canales de Instrucción, puedan reconocer a las propias Instituciones de Fondos de Pago Electrónico, para lo cual dichas instituciones deberán sujetarse a lo siguiente:

I. Proporcionar información personalizada y suficiente para que los Clientes puedan verificar, antes de realizar el procedimiento para su Autenticación, que se trata efectivamente de la Institución de Fondos de Pago Electrónico de la cual se es Cliente. Para ello, las Instituciones de Fondos de Pago Electrónico podrán utilizar la información siguiente:

    a) Aquella que el Cliente respectivo conozca o haya proporcionado a la Institución de Fondos de Pago Electrónico, o bien, que haya convenido con la Institución de Fondos de Pago Electrónico para este fin, tales como nombre, alias, imágenes, entre otros.
    b) Aquella que el Cliente respectivo pueda verificar a través de un medio pactado con la Institución de Fondos de Pago Electrónico para este fin.

II. Una vez que el Cliente acceda al Canal de Instrucción de que se trate, la Institución de Fondos de Pago Electrónico deberá poner a su disposición al menos la siguiente información:

    a) Fecha y hora del último acceso al Canal de Instrucción de que se trate, y
    b) Nombre y apellido del Cliente.

Lo anterior no será aplicable cuando el Cliente utilice Canales de Instrucción que no requieran una interacción previa para la instrucción de Operaciones, tales como las terminales punto de venta.

Artículo 11.- Las Instituciones de Fondos de Pago Electrónico deberán prever lo necesario para que, una vez autenticado el

Cliente en el Canal de Instrucción, la Sesión no pueda ser utilizada por un tercero. Para efectos de lo anterior, las Instituciones de Fondos de Pago Electrónico establecerán, al menos, los mecanismos siguientes:

I. Dar por terminada inmediatamente la Sesión en forma automática e informar al Cliente del motivo en cualquiera de los siguientes casos:

   a) Cuando exista inactividad por más de 5 minutos.
   b) Cuando en el curso de una Sesión, la Institución de Fondos de Pago Electrónico identifique cambios relevantes en los parámetros de comunicación de dicha Sesión, tales como identificación del Canal de Instrucción, rango de direcciones de los protocolos de comunicación, ubicación geográfica, entre otros, que permitan a la institución inferir que pudiera tratarse de un robo de Sesión.

II. Impedir el acceso de forma simultánea en un mismo Canal de Instrucción, mediante la utilización de un mismo Identificador de Cliente y hacerlo del conocimiento del Cliente. Asimismo, las Instituciones de Fondos de Pago Electrónico deberán detectar los intentos de acceder al Canal de Instrucción con información incorrecta y, en su caso, restringir temporalmente el acceso al Canal de Instrucción de que se trate cuando existan tres intentos de acceso fallido.
III. En el evento de que las Instituciones de Fondos de Pago Electrónico ofrezcan servicios de terceros mediante enlaces, deberán comunicar a sus Clientes que, al momento de ingresar a dichos servicios, se ingresará a otro enlace cuya seguridad no depende ni es responsabilidad de dicha Institución de Fondos de Pago Electrónico.

En el caso en que la Institución de Fondos de Pago Electrónico pretenda establecer parámetros distintos a los establecidos en este artículo, deberá obtener previamente la autorización del Banco de México y de la CNBV. Las solicitudes de dichas autorizaciones deberán presentarse mediante correo electrónico que se envíe a la cuenta ifpe@banxico.org.mx y en la oficialía de partes de la CNBV.

Artículo 12.- Las Instituciones de Fondos de Pago Electrónico, en el uso del Identificador de Cliente y los Factores de Autenticación, deberán cumplir con los requisitos siguientes:

I. Contar con los mecanismos necesarios para impedir la lectura o presentación en el Canal de Instrucción, de la información utilizada en los Mecanismos de Identificación y Autenticación proporcionada por el Cliente.
II. Asegurar que cuando se utilicen al menos dos Factores de Autenticación, éstos sean independientes.
III. Contar con procedimientos para restablecer los Factores de Autenticación de tal manera que no se comprometa la Información Personal o Información Sensible del Cliente.
IV. Contar con procedimientos para invalidar los Factores de Autenticación a fin de impedir su uso en un servicio provisto por la Institución de Fondos de Pago Electrónico, cuando un Cliente o la misma institución cancele el uso de dicho servicio o cuando el Cliente respectivo deje de ser Cliente de dicha

Institución de Fondos de Pago Electrónico.

Artículo 13.- Las Instituciones de Fondos de Pago Electrónico únicamente podrán almacenar información relativa a los Factores de Autenticación utilizados por sus Clientes en los Canales de Instrucción cuando dicho almacenamiento se realice bajo protocolos criptográficamente seguros y no sea posible que:

I. Se obtenga la información original de los Factores de Autenticación a partir de la información almacenada.
II. Distintos conjuntos de datos generen la misma información almacenada.

Artículo 14.- Las Instituciones de Fondos de Pago Electrónico deberán establecer procedimientos y mecanismos para que sus Clientes que realicen Operaciones o soliciten los servicios de éstas a través de Canales de Instrucción puedan, en todo momento, desactivar la realización de dichas Operaciones o la solicitud de servicios de forma temporal en caso de requerirlo, así como establecer procedimientos para reactivar el uso cuando los Clientes lo soliciten.

Las Instituciones de Fondos de Pago Electrónico deberán permitir a los Clientes desactivar de manera temporal la realización de las Operaciones y la solicitud de los servicios mencionados en el párrafo anterior, a través de los Canales de Instrucción que al efecto hayan convenido con ellos, solicitando al menos un Factor de Autenticación.

Para la reactivación de la realización de las Operaciones y la solicitud de servicios que las Instituciones de Fondos de Pago Electrónico presten a través de Canales de Instrucción, dichas instituciones deberán permitir a los Clientes utilizar los Canales de Instrucción que convengan para este fin, para lo cual deberán requerir, al menos, un Factor de Autenticación. Las Instituciones de Fondos de Pago Electrónico deberán observar lo señalado en el Artículo 7 de estas Disposiciones para que puedan permitir el acceso al Canal de Instrucción de que se trate una vez que se haya reactivado el servicio.

Sección Segunda
De la Infraestructura Tecnológica en los procesos internos

Artículo 15.- Las Instituciones de Fondos de Pago Electrónico deberán establecer los aspectos de seguridad siguientes, tratándose de componentes de comunicaciones y de cómputo:

I. 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 tráfico autorizado es permitido. En particular, en aquellos segmentos con enlaces al exterior, tales como internet, proveedores, autoridades, otras redes de la Institución de Fondos de Pago Electrónico o matriz y otros terceros, todo ello referido a aquellos servicios definidos como críticos por la propia institución, relacionados, al menos con sistemas de pagos, equipos de Cifrado o autorizadores de Operaciones, entre otros, deberán considerar zonas seguras, incluyendo las denominadas zonas desmilitarizadas (referidas como DMZ, por sus siglas en inglés).
II. Configuración segura de acuerdo con el tipo de componente, considerando, al menos, puertos y servicios, conexiones

entrantes y salientes a otras redes, incluyendo internet, 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.

III. 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, 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 Fondos de Pago Electrónico.

Artículo 16.- Las Instituciones de Fondos de Pago Electrónico deberán cifrar la Información Personal y la Información Sensible recibida, generada, almacenada, procesada o transmitida en la Infraestructura Tecnológica, las imágenes de documentos de identificación expedidos por autoridades oficiales e información biométrica de los Clientes, así como cualquier otra que determinen de acuerdo con sus políticas.

Artículo 17.- Las Instituciones de Fondos de Pago Electrónico deberán contar con procedimientos y mecanismos que permitan estructurar la Información Personal y la Información Sensible almacenada en la Infraestructura Tecnológica, de tal manera que los datos personales de los Clientes no puedan ser relacionados con la información relativa a sus Operaciones, incluyendo, entre otros, los montos, así como los nombres o denominaciones de los receptores o emisores de los pagos realizados por los Clientes. Esta relación sólo podrá ser generada a través de algoritmos de consulta diseñados por la Institución de Fondos de Pago Electrónico que deberán ser ejecutados a demanda cada vez que sea necesario construir esta relación, ya sea por medio de mecanismos manuales o de los sistemas informáticos.

Artículo 18.- Las Instituciones de Fondos de Pago Electrónico deberán cumplir con los requisitos siguientes, respecto de la información relativa a los Factores de Autenticación:

I. Mantener procedimientos de seguridad de información para la custodia, distribución y asignación de los Factores de Autenticación de sus Clientes.
II. Establecer procedimientos y mecanismos con el fin de que la información relativa a los Factores de Autenticación no sea conocida por ninguno de sus funcionarios, empleados o representantes o por algún tercero.
III. Establecer procedimientos y mecanismos que impidan solicitar a sus Clientes, a través de sus funcionarios, empleados, representantes o terceros, la información parcial o completa relativa a los Factores de Autenticación.

Artículo 19.- Las Instituciones de Fondos de Pago Electrónico deberán establecer procedimientos y mecanismos que aseguren que, al desechar o dar de baja componentes de almacenamiento o dispositivos físicos (hardware) de la Infraestructura Tecnológica, la información de los Clientes contenida en dichos componentes o dispositivos sea irrecuperable.

Artículo 20.- Las Instituciones de Fondos de Pago Electrónico estarán obligadas a utilizar herramientas que permitan detectar virus informáticos y códigos maliciosos en la Infraestructura Tecnológica, así como procedimientos que permitan su actualización periódica.

Artículo 21.- Las Instituciones de Fondos de Pago Electrónico deberán realizar, previo al inicio de su operación y al menos cada dos meses, un análisis que permita administrar las vulnerabilidades de seguridad informática derivadas de, entre otros factores, cambios, actualizaciones o errores en la Infraestructura Tecnológica y generar un plan de remediación documentado para atender las vulnerabilidades referidas en dicho análisis de acuerdo con la importancia crítica de éstos, conforme a la clasificación que realice la propia institución.

Artículo 22.- Las Instituciones de Fondos de Pago Electrónico deberán contar con procedimientos y mecanismos para impedir la instalación de cualquier servicio, aplicación o software, salvo los que (i) sean necesarios para la operación de la Institución de Fondos de Pago Electrónico, y (ii) estén autorizados por el oficial en jefe de seguridad de la información de la Institución de Fondos de Pago Electrónico, en cada uno de los elementos de su Infraestructura Tecnológica.

Artículo 23.- Las Instituciones de Fondos de Pago Electrónico deberán establecer procedimientos y mecanismos para restringir el acceso tanto a los puertos físicos de conexión y dispositivos periféricos, como a la infraestructura de cómputo o de telecomunicaciones, utilizados para el resguardo de la información y la operación de la Institución de Fondos de Pago Electrónico.

Artículo 24.- Las Instituciones de Fondos de Pago Electrónico deberán contar con procedimientos y mecanismos de control de acceso a la Infraestructura Tecnológica que sean robustos y seguros, para lo cual deberán cumplir, al menos, con los requisitos siguientes:

I. Controles de acceso lógico a la infraestructura de cómputo y telecomunicaciones, así como a la infraestructura de software, como base de datos, sistemas operativos, contenedores de software y su Infraestructura Tecnológica;
II. Controles para la gestión de Usuarios de la Infraestructura Tecnológica y contraseñas, y
III. Controles que aseguren el seguimiento y monitoreo del acceso a los sistemas utilizados para el almacenamiento de la información de los Clientes, incluyendo auditorías automáticas que permitan la revisión del acceso a nivel individual a la información de los Clientes, las acciones que se realizaron tras el acceso a tal información, los intentos de acceso inválidos, los cambios de Identificación y Autenticación para el acceso de los datos de los Clientes, así como todos los cambios realizados al sistema de almacenamiento.

En el caso de que la Institución de Fondos de Pago Electrónico pretenda utilizar cualquier práctica o estándar distinto que no contenga los elementos antes mencionados, deberá obtener previamente la autorización del Banco de México y de la CNBV. Las Instituciones de Fondos de Pago Electrónico deberán presentar las solicitudes de dichas autorizaciones mediante correo electrónico que envíen a la cuenta ifpe@banxico.org.mx y en la oficialía de partes de la CNBV. La CNBV y el Banco de México podrán divulgar en sus páginas de internet los estándares que cumplen con los requisitos anteriores.

Artículo 25.- Las Instituciones de Fondos de Pago Electrónico deberán establecer

políticas de seguridad de información que su personal esté obligado a observar, que incluya el correcto uso de los recursos utilizados para el almacenamiento de datos de los Clientes, la revisión previa a la contratación de los perfiles del personal que pretenda contratar la Institución de Fondos de Pago Electrónico, así como los procesos de evaluación de riesgos que se realicen por lo menos cada año.

Sección Tercera
Disposiciones Generales para la Infraestructura Tecnológica

Artículo 26.- Las Instituciones de Fondos de Pago Electrónico deberán establecer y documentar políticas y mecanismos para que los Canales de Instrucción sólo utilicen aquellos protocolos de comunicación que garanticen la confidencialidad de la información en la comunicación punto a punto, de conformidad con las mejores prácticas y estándares internacionales de seguridad informática en esta materia, emitidas por el Instituto Nacional de Estándares y Tecnología del Departamento de Comercio del Gobierno (National Institute of Standards and Technology, NIST), el Insitituto SANS y la Fundación OWASP de los Estados Unidos de América. Los mecanismos de cifrado implementados para dichos protocolos de comunicación deberán estar vigentes, no contar con vulnerabilidades conocidas y contemplar que la longitud de las claves de cifrado sea robusta. En caso de que alguna Institución de Fondos de Pago Electrónico pretenda utilizar cualquier práctica o estándar distinto a los señalados anteriormente, deberá obtener previamente autorización del Banco de México y de la CNBV. Para estos efectos, las Instituciones de Fondos de Pago Electrónico deberán presentar las solicitudes a que se refiere a este artículo al Banco de México y a la CNBV, mediante correo electrónico que se envíe a la cuenta ifpe@banxico.org.mx y en la oficialía de partes de la CNBV.

Artículo 27.- Las Instituciones de Fondos de Pago Electrónico deberán contar con medidas de validación para garantizar la autenticidad de las transacciones ejecutadas por los diferentes componentes de la Infraestructura Tecnológica, incluyendo las Operaciones realizadas por los Clientes, considerando, al menos, lo siguiente:

I. La verificación de la veracidad e integridad de la información sin importar que se encuentre estática o en tránsito.
II. La Autenticación entre componentes de la Infraestructura Tecnológica, que aseguren que se ejecutan sólo las solicitudes de servicio legítimas desde su origen y hasta su ejecución y registro.
III. Los protocolos de mensajería, comunicaciones y Cifrado, los cuales deben procurar la integridad y confidencialidad de la información.
IV. La identificación de transacciones previendo que se cuenten con herramientas de monitoreo o medidas de alerta automática para su atención por las áreas operativas correspondientes.
V. 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 artículo deberán establecerse acorde con el grado de riesgo que las Instituciones de Fondos de Pago Electrónico definan para cada tipo de transacción.

Artículo 28.- Las Instituciones de Fondos de Pago Electrónico, para la implementación y el desarrollo de sus sistemas infor-

máticos, ya sea por parte de la propia Institución de Fondos de Pago Electrónico o por medio de una empresa externa especializada en el desarrollo de programas de cómputo contratada por aquella, deberán cumplir con lo siguiente:

I. 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. El proceso de desarrollo deberá implementar aspectos de seguridad de la información, al menos, en las siguientes etapas:

   a) Elaboración de requerimientos.
   b) Diseño del sistema informático.
   c) Desarrollo o adquisición del sistema informático conforme al diseño anterior.
   d) Validación de funcionalidades, propósito, capacidad y calidad del sistema informático.
   e) Pruebas de vulnerabilidades y análisis de código previas a su liberación.
   f) Liberación o instalación del sistema informático.
   g) Control de cambios en el sistema informático.
   h) Destrucción segura de información al término de la vida útil de componentes o sistemas.
   i) En caso de que el software sea desarrollado por una empresa externa especializada, la Institución de Fondos de Pago Electrónico deberá solicitar que el software entregado contenga mecanismos para validar su integridad y autenticidad al momento de instalarlo en su Infraestructura Tecnológica.

II. Los sistemas informáticos deberán considerar las siguientes funcionalidades durante todo su proceso de operación:

   a) Mecanismos de Autenticación entre los diferentes componentes utilizados para la operación de la Institución de Fondos de Pago Electrónico.
   b) El uso de firmas electrónicas para garantizar la integridad y el no repudio de la información operativa de la Institución de Fondos de Pago Electrónico, con independencia de que sea información estática o en tránsito.
   c) Gestión de Usuarios de la Infraestructura Tecnológica y sus privilegios.
   d) Uso de comunicaciones cifradas para la comunicación de los diferentes sistemas informáticos y sus componentes.

III. Revisar de forma estática, al menos a través de herramientas automatizadas, la seguridad del sistema informático cada vez que se realice una actualización de éste.

Artículo 29.- Las Instituciones de Fondos de Pago Electrónico deberán mantener la solidez de su Infraestructura Tecnológica, para lo cual deberán contar con:

Controles que permitan revisar, al menos una vez al año, que los componentes que brindan seguridad a su Infraestructura Tecnológica se encuentren vigentes y, en su caso, actualizar los componentes que ya no se encuentren vigentes;

Procedimientos y herramientas para la detección de la alteración o falsificación de

la información contenida en la Infraestructura Tecnológica;

Registros que permitan vigilar, auditar y rastrear los accesos y actividades realizadas por los diferentes Usuarios de la Infraestructura Tecnológica de los sistemas informáticos con independencia del nivel de privilegios que se establezca para su acceso y el medio o protocolo de comunicación de acceso. Estos registros deberán incluir al menos la siguiente información:

Fecha, hora, minuto y segundo de las actividades realizadas por los Usuarios de la Infraestructura Tecnológica.

Los elementos que permiten identificar al Usuario de la Infraestructura Tecnológica que realiza dichas actividades.

Los datos de identificación del punto de acceso utilizado por el Usuario de la Infraestructura Tecnológica para realizar la operación de que se trate.

Las direcciones de los protocolos de internet o similares, de acuerdo con el medio electrónico utilizado por el Usuario de la Infraestructura Tecnológica.

La información generada deberá ser almacenada de forma segura por un periodo mínimo de ciento ochenta días naturales y contemplar mecanismos para evitar su alteración, así como mantener procedimientos de control interno para su acceso y disponibilidad.

Registros que permitan vigilar, auditar y rastrear los accesos y actividades realizadas por los diferentes Clientes. Estos registros deberán incluir al menos la siguiente información:

a) Fecha, hora, minuto y segundo de las actividades realizadas por los Clientes.
b) Números de las Cuentas involucradas en la Operación, incluyendo aquella Cuenta perteneciente al ordenante de la Operación y, en su caso, la de los receptores, y demás información que permita identificar las Operaciones realizadas por los Clientes o a quienes hayan usado el medio de disposición respectivo.
c) Los datos de identificación del Canal de Instrucción utilizado por el Cliente o por quien haya usado el medio de disposición respectivo para realizar la Operación de que se trate, así como los Factores de Autenticación utilizados para su instrucción.
d) Las direcciones de los protocolos de internet o similares, el número de la línea del teléfono o demás datos, de acuerdo al Canal de Instrucción utilizado por el Cliente o usuario del medio de disposición.

La información generada deberá ser almacenada de forma segura por un periodo mínimo de ciento ochenta días naturales a partir de su generación, mediante mecanismos previamente determinados para evitar su alteración, así como mantener procedimientos de control interno para su acceso y disponibilidad.

Dicha información deberá ser proporcionada a los Clientes o usuarios del medio de disposición que así lo requieran expresamente a la Institución de Fondos de Pago Electrónico mediante sus canales de atención al Cliente, en un plazo que no exceda de 10 días hábiles, siempre que se trate de Operaciones realizadas en las propias Cuentas de los Clientes o usuarios del medio de disposición durante los ciento ochenta días naturales previos al requerimiento de la información de que se trate.

Registros que permitan vigilar, auditar y rastrear todas las operaciones realizadas por los sistemas informáticos, así como bloquear transmisiones que no cumplan con los criterios de seguridad establecidos. Estos registros deberán incluir:

a) Fecha, hora, minuto y segundo de las actividades realizadas por los sistemas informáticos.
b) Los datos de identificación del punto de acceso utilizado por el sistema informático para realizar la operación de que se trate.
c) Las direcciones de los protocolos de internet o similares de acuerdo al medio electrónico utilizado por el sistema informático.
d) La información generada, incluyendo la de otros medios, deberán ser almacenadas de forma segura por un periodo mínimo de ciento ochenta días naturales y contemplar mecanismos para evitar su alteración, así como mantener procedimientos de control interno para su acceso y disponibilidad.

Artículo 30.- Cada Institución de Fondos de Pago Electrónico deberá contar con una Política Estratégica de Continuidad de Negocio y de Seguridad de la Información, la cual deberá ser aprobada por su respectivo Órgano de Administración.

Artículo 31.- Las Instituciones de Fondos de Pago Electrónico deberán contar con un Plan Director de Seguridad, el cual deberá ser aprobado por el director general o, a falta de éste, el administrador único. El Plan Director de Seguridad deberá estar alineado con la estrategia de negocio de la Institución de Fondos de Pago Electrónico y con lo establecido en la Política Estratégica de Continuidad de Negocio y de Seguridad de la Información, así como definir y priorizar los proyectos en materia de seguridad de la información, con el objetivo de reducir la exposición a los riesgos tecnológicos y la materialización de Incidentes de Seguridad de la Información hasta niveles aceptables en los términos que defina, en su caso, el Órgano de Administración, según se trate, a partir de un análisis de la situación actual.

Para la aprobación del Plan Director de Seguridad, el director general o, en su caso, el administrador único, deberán verificar que contenga las iniciativas dirigidas a mejorar los métodos de trabajo existentes y podrá contemplar los controles requeridos conforme a las disposiciones aplicables. Las modificaciones al Plan Director de Seguridad deberán ser aprobadas por el director general o, en su caso, el administrador único.

Tratándose de Instituciones de Fondos de Pago Electrónico que cuenten con director general y consejo de administración, el primero deberá informar a dicho consejo el contenido del Plan Director de Seguridad, o de sus modificaciones, cuando aplique, y contar con evidencia de su aprobación e implementación.

Artículo 32.- Las Instituciones de Fondos de Pago Electrónico deberán implementar procedimientos y mecanismos que deberán seguir para la atención de Incidentes de Seguridad de Información en su Infraestructura Tecnológica que comprendan su identificación, contención y la adecuada recolección y resguardo de evidencias de dichos incidentes.

Artículo 33.- Las Instituciones de Fondos de Pago Electrónico deberán evaluar o auditar, previo al inicio de sus operaciones y al menos cada dos años, la seguridad informática de sus Infraestructuras Tecnológicas. Además, entre los trabajos de dicha evaluación o auditoría en los plazos referidos, las Instituciones de Fondos de Pago Electrónico deberán presentar un reporte al Órgano de Administración, así como al Banco de México y a la CNBV, que especifique el nivel de riesgo informático para la Infraestructura Tecnológica, así como la conformación de un plan de trabajo documentado para

atender las observaciones de criticidad alta y muy alta encontrados en dicha evaluación o auditoría. Tales planes de trabajo deberán incorporarse al Plan Director de Seguridad. El reporte deberá firmarse digitalmente por el director general o, en su caso, el administrador único, y quedar cifrado conforme a lo siguiente:

I. Uso de llaves asimétricas (pública y privada), a fin de garantizar confidencialidad y no repudio, evitando compartir la llave privada;
II. Uso de un certificado digital validado por una autoridad certificadora reconocida o por una entidad de certificación acreditada por la Secretaría de Economía; y
III. Incorporación de firma digital que permita garantizar la integridad de la información proporcionada.

Las Instituciones de Fondos de Pago Electrónico deberán enviar al Banco de México y a la CNBV el reporte a que se refiere este artículo mediante correo electrónico dirigido a la cuenta ifpe@banxico.org.mx y mediante documento o archivo electrónico que presente en la oficialía de partes de la propia CNBV.

Artículo 34.- Las Instituciones de Fondos de Pago Electrónico deberán contratar a una persona moral, con personal que cuente con capacidad técnica comprobable mediante certificaciones de la industria en la materia, para que, al menos, cada dos años, se realicen pruebas de penetración en los diferentes sistemas y aplicativos de la Infraestructura Tecnológica con la finalidad de detectar errores, vulnerabilidades, funcionalidad no autorizada o cualquier código que ponga o pueda poner en riesgo la información y patrimonio de los Clientes y de la propia Institución de Fondos de Pago Electrónico.

La Institución de Fondos de Pago Electrónico deberá enviar al Banco de México y a la CNBV, dentro de los 20 días hábiles a partir de la fecha en que hayan finalizado las pruebas correspondientes, un informe con las conclusiones de éstas, mediante correo electrónico que se envíe a la cuenta ifpe@banxico.org.mx y en la oficialía de partes de la CNBV. El informe deberá firmarse digitalmente por el director general o, en su caso, el administrador único, y ser cifrado conforme a lo dispuesto en el artículo anterior.

En el caso de que, de las pruebas de penetración realizadas, se deriven observaciones de alta o muy alta criticidad, la Institución de Fondos de Pago Electrónico de que se trate deberá presentar al Banco de México y a la CNBV, mediante correo electrónico que se envíe a las cuentas ifpe@banxico.org.mx y en la oficialía de partes de la CNBV, un plan de remediación documentado para subsanar dichas observaciones, en un plazo no mayor a 20 días hábiles de la finalización de las pruebas de penetración. El plan de remediación deberá firmarse digitalmente por el director general o, en su caso, el administrador único, y ser cifrado conforme lo dispuesto en el artículo anterior. La CNBV y el Banco de México podrán efectuar observaciones, en cualquier tiempo, a dicho plan de remediación.

Una vez concluidas las actividades de remediación de las observaciones de alta o muy alta criticidad a que se refiere el párrafo anterior, la Institución de Fondos de Pago Electrónico deberá realizar nuevamente, en un plazo no mayor a dos meses posteriores a la fecha de conclusión de dichas actividades, pruebas de penetración para verificar que se han mitigado dichas vulnerabilidades.

Las Instituciones de Fondos de Pago Electrónico deberán documentar en manuales las metodologías utilizadas para clasificar la criticidad y el riesgo de los hallazgos de

las pruebas de seguridad de la información, incluyendo las de penetración y vulnerabilidades.

Artículo 35.- Las Instituciones de Fondos de Pago Electrónico deberán contar con un miembro de su personal que, entre sus funciones, se desempeñe como oficial en jefe de seguridad de la información, conocido como CISO por sus siglas en inglés (*Chief Information Security Officer)*.

El oficial en jefe de seguridad de la información deberá ser designado por el director general o, en su caso, por el administrador único, y no deberá tener conflictos de interés respecto del responsable de las funciones de auditoría y tecnologías de la información de la Institución de Fondos de Pago Electrónico. Asimismo, no podrá realizar las funciones relacionadas con la operación de la seguridad de la información de la propia Institución de Fondos de Pago Electrónico.

Las funciones del oficial en jefe de seguridad de la información podrán ser realizadas por un tercero, siempre que se ajuste a lo señalado en el presente artículo.

El oficial en jefe de seguridad de la información podrá apoyarse, para el ejercicio de sus funciones en representantes de las diferentes unidades de negocio.

Las Instituciones de Fondos de Pago Electrónico podrán designar como oficial en jefe de seguridad de la información al director general, o en su caso al administrador único, durante un plazo máximo de doce meses contados a partir de la fecha en que obtengan la autorización para actuar como tales.

Artículo 36.- El oficial en jefe de seguridad de la información de la Institución de Fondos de Pago Electrónico deberá, al menos:

I. Participar en la definición, verificar y ser responsable de la implementación y continuo cumplimiento de las políticas y procedimientos de seguridad de la información señalados en las presentes Disposiciones.

II. Elaborar el Plan Director de Seguridad, el cual deberá contener, por cada proyecto que se defina, nombre del proyecto, objetivo, alcance, fechas de inicio y fin, áreas involucradas y la inversión proyectada. El plan a que se refiere la presente fracción deberá revisarse y actualizarse, al menos, anualmente.

III. Verificar, al menos anualmente, la definición de los perfiles de acceso a la Infraestructura Tecnológica de la Institución de Fondos de Pago Electrónico, ya sea propia o provista por terceros, de acuerdo con los perfiles de puestos (segregación funcional), incluyendo aquellos con altos privilegios, tales como administración de sistemas operativos, bases de datos y aplicativos.

IV. Asegurarse, al menos anualmente, o antes en caso de presentarse un Incidente de Seguridad de la Información, de la correcta asignación de los perfiles de acceso a los Usuarios de la Infraestructura Tecnológica. La función a que se refiere esta fracción podrá realizarse mediante muestras representativas y aleatorias.

Asimismo, será responsable de la autorización temporal de los accesos por excepción, tales como los de Usuarios de la Infraestructura Tecnológica de ambientes de desarrollo con accesos a ambientes de producción, accesos por eventos de contingencia o cualquier otro acceso privilegiado que no corresponda con la política determinada por la Institución de Fondos de Pago Electrónico. Igualmente, deberá contar con un registro que contenga el nombre del Usuario

de la Infraestructura Tecnológica, aplicación asociada, ambiente, motivo de la excepción y fecha de inicio y de fin de la asignación.

V. Aprobar y verificar el cumplimiento de las medidas que se hayan adoptado para subsanar deficiencias detectadas con motivo de las funciones a que se refieren las fracciones III y IV de este artículo, así como de los hallazgos, tanto de auditoría interna como externa relacionada con la Infraestructura Tecnológica y de seguridad de la información.

VI. Gestionar las alertas de seguridad de la información comunicadas por la CNBV u otros medios, así como los Incidentes de Seguridad de la Información, considerando las etapas de identificación, protección, detección, respuesta y recuperación.

VII. Presidir en la Institución de Fondos de Pago Electrónico, el equipo para la detección y respuesta de Incidentes de Seguridad de la Información.

VIII. Informar al Órgano de Administración o, en caso de contar con un comité de auditoría y un comité de riesgos a éstos, en la sesión inmediata siguiente, según resulte aplicable, a la verificación del Incidente de Seguridad de la Información, respecto de las acciones tomadas y del seguimiento a las medidas para prevenir o evitar que se presenten nuevamente los mencionados incidentes.

IX. Verificar que se implementen programas anuales de capacitación dirigidos a todo el personal, así como de concientización en materia de seguridad de la información hacia los Clientes incluyendo, en su caso, a terceros que les presten servicios, en los que se contemplen, entre otros aspectos, los roles y responsabilidades que los Usuarios de Infraestructura Tecnológica tengan al respecto.

X. Presentar mensualmente al director general o, en su caso, al administrador único, el informe de gestión en materia de seguridad de la información. Este reporte deberá efectuarse al comité de auditoría y al comité de riesgos o, en ausencia de éstos, al consejo de administración de la Institución de Fondos de Pago Electrónico.

XI. Considerar, al menos, los indicadores de riesgo en materia de seguridad de la información establecidos en el Anexo 1 de estas Disposiciones, e informar del resultado de la evaluación de dichos indicadores al Órgano de Administración y, en su caso, al comité de auditoría o comité de riesgos.

XII. Responder a los requerimientos formulados por las autoridades y al interior de la Institución de Fondos de Pago Electrónico en materia de seguridad de la información.

Las Instituciones de Fondos de Pago Electrónico deberán asegurarse de que el oficial en jefe de seguridad de la información tenga a su disposición los registros de las personas que cuenten con acceso a la información relacionada con las operaciones en las que interviene la propia Institución de Fondos de Pago Electrónico, incluyendo aquellas que se encuentren en el extranjero y de los Usuarios de la Infraestructura Tecnológica que cuenten con altos privilegios, tales como administración de sistemas operativos, bases de datos y aplicativos, así como de sus prestadores de servicios.

Las Instituciones de Fondos de Pago Electrónico que pertenezcan a un grupo financiero sujeto a la supervisión de la CNBV, o bien, que formen parte de Consorcios

o Grupos Empresariales que cuenten con una entidad financiera sujeta a la supervisión de la propia CNBV, podrán asignar las funciones del oficial en jefe de seguridad de la información, a la persona que desempeñe dichas actividades en la entidad financiera supervisada por la CNBV, siempre y cuando dicha persona cumpla con lo establecido en el artículo 35 de estas disposiciones.

CAPÍTULO III
DE LA CONTINUIDAD OPERATIVA

Artículo 37.- Las Instituciones de Fondos de Pago Electrónico deberán contar con un Plan de Continuidad de Negocio que cumpla con los requerimientos mínimos establecidos en el Anexo 2 de las presentes Disposiciones, el cual deberá de estar alineado con la Política Estratégica de Continuidad de Negocio y de Seguridad de la Información.

El Plan de Continuidad de Negocio deberá ser aprobado por el director general o, en su caso, el administrador único, debiendo verificar que contenga las iniciativas dirigidas a mejorar los métodos de trabajo existentes, conforme a las presentes disposiciones. Las modificaciones al Plan de Continuidad de Negocio deberán ser aprobadas por el director general o, en su caso, el administrador único, siendo responsabilidad del director general ajustarse a los principios establecidos por el consejo de administración en el manual de continuidad de negocio y seguridad de la información.

Tratándose de Instituciones de Fondos de Pago Electrónico que cuenten con director general y consejo de administración, el primero deberá informar a dicho consejo el contenido del Plan de Continuidad de Negocio, o de sus modificaciones, y contar con evidencia de su aprobación e implementación.

Artículo 38.- Cada Institución de Fondos de Pago Electrónico deberá contar con los mecanismos necesarios para la continuidad operativa y la administración de Contingencias Operativas de la propia institución, que incluyan su identificación, evaluación, monitoreo y mitigación**.**

Artículo 39.- Las Instituciones de Fondos de Pago Electrónico deberán contar con metodologías para estimar los impactos cuantitativos y cualitativos de las posibles Contingencias Operativas que, en términos de estas disposiciones, determine el responsable de la administración de Contingencias Operativas para su utilización en el análisis a que hace referencia el Anexo 2. El Órgano de Administración de cada Institución de Fondos de Pago Electrónico deberá aprobar dichas metodologías, sin perjuicio de las facultades del director general para realizar las modificaciones al Plan de Continuidad de Negocio, de conformidad con los principios establecidos por el respectivo Órgano de Administración en la Política Estratégica de Continuidad de Negocio y Seguridad de la Información.

Artículo 40.- El Órgano de Administración de la Institución de Fondos de Pago Electrónico que corresponda deberá designar a una persona que funja como responsable de la administración de Contingencias Operativas, que cuente con conocimientos en la materia, quien podrá ser la misma persona designada como administrador integral de riesgos de conformidad con las disposiciones de carácter general que emita la CNBV. El responsable de la administración de Contingencias Operativas podrá auxiliarse de otras áreas de la propia Institución de Fondos de Pago Electrónico o de terceros contratados al efecto que sean especialistas en la materia. Dicha persona tendrá, como mínimo, las funciones siguientes:

I. Elaborar, revisar y, en su caso, actualizar el Plan de Continuidad de Negocio.
II. Evaluar, por lo menos una vez al año, el alcance y efectividad, así como el cumplimiento de los requerimientos mínimos establecidos en el Anexo 2 de las presentes Disposiciones, el Plan de Continuidad de Negocio establecido, e informar los resultados de dicha evaluación al Órgano de Administración y a las áreas responsables de los procesos operativos críticos, identificando, en su caso, los ajustes necesarios para su actualización, fortalecimiento y cumplimiento. En caso de que la Institución de Fondos de Pago Electrónico cuente con un comité de auditoría, las funciones previstas en esta fracción serán realizadas por dicho comité.
III. Realizar las pruebas del funcionamiento y suficiencia del Plan de Continuidad de Negocio e informar al Órgano de Administración, cuando menos una vez al año, sobre los resultados de dichas pruebas.
IV. Definir y presentar al Órgano de Administración la metodología para la administración de Contingencias Operativas, en los términos establecidos en las disposiciones correspondientes a la administración de eventos operativos. Para efectos de lo anterior, el responsable de la administración de eventos operativos podrá auxiliarse de otras áreas de la propia Institución de Fondos de Pago Electrónico o de terceros contratados al efecto que sean especialistas en la materia.
V Definir y presentar para aprobación del Órgano de Administración, las metodologías para estimar los impactos cuantitativos y cualitativos de las Contingencias Operativas. Para efectos de lo anterior, el responsable de la administración de Contingencias Operativas podrá auxiliarse de otras áreas de la propia Institución de Fondos de Pago Electrónico o de terceros contratados al efecto que sean especialistas en la materia.
VI. Verificar la efectividad de la metodología para estimar los impactos cuantitativos y cualitativos de las posibles Contingencias Operativas, al menos una vez al año, y en su caso corregir dicha metodología dentro del mismo plazo, comparando sus estimaciones contra las Contingencias Operativas efectivamente observadas y, en su caso, deberán llevar a cabo las correcciones necesarias.

En caso de que las Instituciones de Fondos de Pago Electrónico contraten con terceros los servicios necesarios para soportar su operación, en sustitución de lo previsto en las fracciones II y III del presente artículo, y únicamente respecto de los servicios prestados por dichos terceros, las instituciones deberán contar con la documentación que acredite que tales terceros cuentan con una certificación vigente emitida conforme a estándares internacionales respecto de su capacidad para mantener la continuidad de sus servicios. Lo anterior deberá observarse, sin perjuicio del cumplimiento de lo previsto en el Capítulo V de las presentes Disposiciones.

CAPÍTULO IV
DISPOSICIONES COMUNES DE SEGURIDAD DE INFORMACIÓN Y DE CONTINUIDAD OPERATIVA

Artículo 41 .- Las Instituciones de Fondos de Pago Electrónico deberán llevar un registro en bases de datos de los Eventos de Seguridad de la Información calificados como relevantes, Incidentes de Seguridad de la Información, Contingencias Operativas, fallas o vulnerabilidades detectadas en

la Infraestructura Tecnológica, que incluya, según sea el caso, la información relacionada con la detección de fallas, errores operativos, intentos de ataques informáticos y de aquéllos efectivamente llevados a cabo, así como de pérdida, extracción, alteración, extravío o uso indebido de información de los Usuarios de la Infraestructura Tecnológica o de los Clientes, en donde se contemple la fecha del suceso y una breve descripción de éste, su duración, servicio o el elemento de la Infraestructura Tecnológica afectado, Clientes afectados y montos, así como las medidas correctivas implementadas.

La información de los Eventos de Seguridad de la Información calificados como relevantes e Incidentes de Seguridad de la Información, así como Contingencias Operativas, deberá estar respaldada en los medios que las Instituciones de Fondos de Pago Electrónico determinen y conservarse por, al menos, 10 años.

Artículo 42.- En caso de que se presente un Evento de Seguridad de Información en: (i) los componentes de la Infraestructura Tecnológica de la Institución de Fondos de Pago Electrónico, (ii) los Canales de Instrucción o (iii) la infraestructura tecnológica de cualquier tercero que afecte la operación o la Infraestructura Tecnológica de la Institución de Fondos de Pago Electrónico, o bien, se presente un Incidente de Seguridad de la Información, el director general o, en su caso, el administrador único deberá:

Prever lo necesario para hacer del conocimiento del Banco de México y de la CNBV, de forma inmediata, los Incidentes de Seguridad de la Información, mediante correo electrónico que se envíe a las cuentas ifpe@banxico.org.mx y Ciberseguridad-CNBV@cnbv.gob.mx, o a través de otros medios que el propio Banco de México o la propia CNBV señalen. En dicha notificación se deberá indicar, al menos, la fecha y hora de inicio del Incidente de Seguridad de la Información de que se trate y, en su caso, la indicación de si continúa o ha concluido y su duración; una descripción de dicho evento o incidente, así como una evaluación inicial del impacto o gravedad.

Adicionalmente, las Instituciones de Fondos de Pago Electrónico deberán enviar a las cuentas ifpe@banxico.org.mx y Ciberseguridad-CNBV@cnbv.gob.mx, mencionadas o a través de otros medios que el propio Banco de México o la propia CNBV señalen, dentro de los cinco días hábiles siguientes a la identificación del Incidente de Seguridad de la Información de que se trate, la información que se contiene en los Anexos 3 y 4 de las presentes disposiciones.

En el caso de Eventos de Seguridad de la Información, deberán reportarse a través de los medios señalados en el primer párrafo de esta fracción, sólo aquellos que, de acuerdo con las políticas y procedimientos establecidos por la propia Institución de Fondos de Pago Electrónico, se califiquen como relevantes por tener potencial afectación para la Institución de Fondos de Pago Electrónico, sus Clientes, contrapartes, proveedores u otras entidades del sistema financiero, además de los relacionados con Información Personal o Información Sensible, imágenes de identificaciones oficiales e información de los Factores de Autenticación a los que se refiere la fracción III del artículo 5 de estas disposiciones. Este reporte únicamente deberá contener la fecha y hora de inicio, así como la descripción del evento de que se trate.

Llevar a cabo una investigación inmediata sobre las causas que generaron el Incidente de Seguridad de la Información y establecer un plan de trabajo que describa las acciones a implementar para eliminar o mitigar las vulnerabilidades que propiciaron el mencionado incidente. Dicho plan debe-

rá indicar, al menos, el personal responsable de su diseño, implementación, ejecución y seguimiento, plazos para su ejecución, así como los recursos técnicos, materiales y humanos, y enviarse al Banco de México y a la CNBV en un plazo no mayor a quince días hábiles posteriores a que concluyó el Incidente de Seguridad de la Información.

Cuando el Incidente de Seguridad de la Información se refiera a que la Información Personal o Información Sensible que se encuentre en custodia de la Institución de Fondos de Pago Electrónico o de terceros que le presten servicios, fue extraída, extraviada, eliminada, alterada, o bien, las Instituciones de Fondos de Pago Electrónico sospechen de la realización de algún acto que involucre accesos no autorizados a dicha información, el director general o, en su caso, el administrador único o la persona que alguno de éstos designe, deberá notificar a los Clientes la posible pérdida, extracción, alteración, extravío o acceso no autorizado a su información, dentro de las siguientes veinticuatro horas a que ocurrió el Incidente de Seguridad de la Información o a que se tuvo conocimiento de éste, a través de los medios de notificación que el Cliente haya señalado para tal efecto, a fin de prevenirlo de los riesgos derivados del mal uso de la información que haya sido extraída, extraviada, eliminada o alterada, debiendo informarle las medidas que deberá tomar y, en su caso, efectuar la reposición de los medios de disposición que correspondan o la sustitución de Factores de Autenticación necesarios. La notificación deberá incluir, al menos, la naturaleza, fecha y hora de inicio del evento, duración y, en caso de existir, delimitar y señalar las afectaciones individuales a cada Cliente. La evidencia de esta notificación deberá incluirse en el resultado de la investigación señalada en el párrafo anterior.

Artículo 43.- Las Instituciones de Fondos de Pago Electrónico deberán hacer del conocimiento del Banco de México y la CNBV las Contingencias Operativas que se presenten en cualquiera de los canales de atención al público o al interior de la propia Institución de Fondos de Pago Electrónico, mediante correo electrónico que se envíe a las cuentas ifpe@banxico.org.mx, contingencias@cnbv.gob.mx y supervisionfintech@cnbv.gob.mx o a través de otros medios que el propio Banco de México o la propia CNBV dispongan, debiéndose generar un acuse de recibo electrónico. Lo anterior, siempre que estas interrupciones que tengan una duración de, al menos, 30 minutos.

La notificación señalada en el párrafo anterior deberá efectuarse dentro de los 60 minutos siguientes a que la Contingencia Operativa de que se trate haya tenido lugar, debiendo incluir la fecha y hora de inicio de la Contingencia Operativa; la indicación de si continúa o, en su caso, si ha concluido y su duración; los procesos, sistemas y canales afectados; una descripción del evento que se haya registrado, y una evaluación inicial del impacto o gravedad.

Asimismo, en caso de que se presente una Contingencia Operativa, la Institución de Fondos de Pago Electrónico de que se trate deberá realizar una investigación inmediata sobre las causas que generaron el evento, y enviar los resultados de la investigación al Banco de México y a la CNBV en un plazo no mayor a cinco días hábiles conforme a las especificaciones del Anexo 5 de las presentes Disposiciones.

Por su parte, en caso de que, producto de una Contingencia Operativa, se afecten uno o a más Canales de Instrucción, la Institución de Fondos de Pago Electrónico de que se trate deberá hacer de conocimiento a sus Clientes o usuarios del medio de dispo-

sición, en un plazo no mayor a cinco segundos de la intermitencia o imposibilidad del uso de éstos a través de los medios de notificación pactados con ellos y deberá mantener evidencia de ello. Adicionalmente, la Institución de Fondos de Pago Electrónico deberá poner a disposición de sus Clientes o usuarios del medio de disposición, la información relativa a la Contingencia Operativa de que se trate, incluyendo, al menos, la naturaleza, fecha y hora de inicio del evento, duración y, en caso de existir, delimitar y señalar las afectaciones individuales a cada Cliente o usuario del medio de disposición, en un plazo máximo de veinticuatro horas de la materialización del evento.

En su caso, el director general o administrador único será el responsable de llevar a cabo lo previsto en el presente artículo.

CAPÍTULO V
DE LA CONTRATACIÓN DE SERVICIOS CON TERCEROS Y COMISIONISTAS

Artículo 44.- Las Instituciones de Fondos de Pago Electrónico requerirán autorización del Banco de México y la CNBV para contratar la prestación de servicios con cualquier tercero que cumplan con las siguientes características:

I. Los servicios que dicho tercero preste que impliquen la transmisión, almacenamiento, procesamiento, resguardo o custodia de Información Personal o Información Sensible, imágenes de documentos de identificación expedidos por autoridades oficiales o información biométrica de los Clientes, siempre y cuando el tercero de que se trate tenga privilegios de acceso para conocer dicha información o a la información de configuración de seguridad, o bien, a la administración de control de accesos;
II. Realice procesos en el extranjero relacionados con la contabilidad o tesorería; o
III. Funja como el proveedor primario de aquellos servicios cuya interrupción, parcial o permanente, imposibilite a la Institución de Fondos de Pago Electrónico la emisión, administración, redención o transmisión de fondos de pago electrónico, conforme a los actos a los que refieren las fracciones II, III, IV y V del Artículo 22 de la Ley.

Las Instituciones de Fondos de Pago Electrónico únicamente podrán contratar los servicios referidos en las fracciones anteriores, así como cualquier otro, cuando las personas que proporcionen los servicios respectivos guarden la debida confidencialidad de la información referente a las Operaciones celebradas con sus Clientes, así como la relativa a estos últimos, en caso de tener acceso a ella. En todo caso, las Instituciones de Fondos de Pago Electrónico serán responsables por las violaciones a la confidencialidad de la información bajo su resguardo o de los terceros referidos.

El director general o, en su caso, el administrador único de la Institución de Fondos de Pago Electrónico será responsable de aprobar la contratación de los prestadores de servicios a que se refiere este Capítulo.

Las Instituciones de Fondos de Pago Electrónico deberán mantener los datos de quienes les proporcionen servicios, en el padrón a que se refiere el artículo 52 de las presentes disposiciones.

La autorización a que se refiere este artículo no será necesaria cuando las Instituciones de Fondos de Pago Electrónico contraten a otras entidades financieras sujetas a

disposiciones de carácter general sustancialmente similares a las presentes Disposiciones.

Artículo 45.- Las Instituciones de Fondos de Pago Electrónico deberán presentar al Banco de México y a la CNBV un aviso, con 20 días hábiles de antelación a la contratación de terceros, que contenga los requerimientos a que se refiere el artículo 49 de las presentes Disposiciones, cuando dicho tercero funja como proveedor secundario o de respaldo de aquellos servicios cuya interrupción, parcial o permanente, imposibilitarían a la Institución de Fondos de Pago Electrónico la emisión, administración, redención o transmisión de fondos de pago electrónico, conforme a los actos a los que refieren las fracciones II, III, IV y V del Artículo 22 de la Ley.

El Banco de México y la CNBV, durante el plazo de 20 días hábiles anteriormente referido, podrán requerir a la Institución de Fondos de Pago Electrónico de que se trate que la prestación de dicho servicio no se realice a través del tercero señalado en el aviso a que se refiere el presente Artículo, cuando cualquiera de las dos Autoridades considere que, por los términos y condiciones de contratación del servicio o las políticas y procedimientos de control interno, la Infraestructura Tecnológica o de comunicaciones materia del servicio, dicho tercero no estaría en posibilidad de cumplir con las disposiciones aplicables a la propia Institución de Fondos de Pago Electrónico y, en su caso, pueda verse afectada la estabilidad financiera o continuidad operativa de esta última, a juicio del Banco de México o la CNBV.

Artículo 46.- Las Instituciones de Fondos de Pago Electrónico podrán celebrar contratos de comisión mercantil con terceros que actúen frente al público en general a nombre y por cuenta propia de las respectivas Instituciones de Fondos de Pago Electrónico para la realización de las siguientes operaciones:

I. Retiros de efectivo efectuados por el propio Cliente titular de la cuenta respectiva.
II. Recepción de efectivo para abono en cuentas propias o de terceros.
III. Consultas de saldos y movimientos de cuentas.
IV. Poner en circulación instrumentos para la disposición de fondos de pago electrónico.
V. Apertura de cuentas de fondos de pago electrónico, observando en todo momento lo establecido en las disposiciones de carácter general a que se refiere el artículo 58 de la Ley, emitidas por la Secretaría, o las que las sustituyan.
VI. Transferencias con cargo a cuentas de fondos de pago electrónico, incluidos los pagos de servicios.

Las operaciones previstas en las fracciones anteriores deberán efectuarse en moneda nacional y a nombre y por cuenta propia de la Institución de Fondos de Pago Electrónico. En caso de que la Institución de Fondos de Pago Electrónico pretenda realizar a través de Comisionistas operaciones distintas a las señaladas, deberá solicitar autorización a la CNBV, previo a su realización.

Las Instituciones de Fondos de Pago Electrónico, en la celebración de los contratos a que se refiere este artículo, deberán cuidar en todo momento que los terceros que les proporcionen los servicios guarden la debida confidencialidad de la información referente a las Operaciones celebradas con sus Clientes, así como la relativa a estos últimos, en caso de tener acceso a ella.

El director general o, en su caso, el administrador único de la Institución de Fon-

dos de Pago Electrónico será responsable de aprobar la contratación de Comisionistas.

Artículo 47.- Las Instituciones de Fondos de Pago Electrónico que pretendan celebrar los contratos de comisión mercantil a que se refiere el artículo anterior deberán solicitar autorización a la CNBV. Dicha autorización deberá contener lo siguiente:

I. Plan general de funcionamiento que contenga:

a) Descripción detallada y diagrama de flujo de los procesos de cada una de las operaciones a contratar considerando, en su caso, el proceso de conciliación y liquidación de cada una de ellas, los terceros involucrados y la Infraestructura Tecnológica a utilizar en la Operación de que se trate.

b) Mecanismos que incluyan los controles automatizados que utilizará la Institución de Fondos de Pago Electrónico para evitar que los comisionistas o el Administrador de comisionistas excedan los límites de operación establecidos en el artículo 48.

c) Mecanismos de vigilancia del desempeño del comisionista o del Administrador de comisionistas, que deberán considerar, cuando menos, el cumplimiento de sus obligaciones contractuales.

Para efectos de lo anterior, la Institución de Fondos de Pago Electrónico deberá contar con planes para evaluar y reportar al Órgano de Administración o, en su caso, al comité de auditoría el desempeño de los comisionistas o del Administrador de comisionistas contratados y el cumplimiento de la regulación aplicable relacionada con dicha contratación.

d) Los requerimientos técnicos para realizar operaciones a través de comisionistas, ajustándose a lo señalado en el Anexo 7 de las presentes disposiciones.

Las instituciones de fondos de pagos electrónico deberán solicitar autorización a la CNBV en un plazo no mayor a 20 días hábiles previo a la realización de operaciones adicionales a las manifestadas en el plan general de funcionamiento a que se refiere esta fracción. Asimismo, cuando lleven a cabo reformas a dicho plan que impliquen cambios sustanciales en los términos en los que realizarían las Operaciones con los Clientes o usuarios del medio de disposición, deberán solicitar autorización a la CNBV con por lo menos 20 días hábiles de anticipación a la fecha en que se pretenda que surtan efectos.

II. Proyecto de contrato en el que deberá señalarse la fecha probable de su celebración y los derechos y obligaciones de la Institución de Fondos de Pago Electrónico y del comisionista o del Administrador de comisionistas. Asimismo, dentro del contrato se deberá prever lo siguiente:

a) Las Operaciones que el comisionista o el Administrador de comisionistas realizarán a nombre y por cuenta de la Institución de Fondos de Pago Electrónico.

Tratándose de Operaciones que se realicen a través de Administradores de comisionistas, las Instituciones de Fondos de Pago Electrónico deberán prever en el contrato las Operaciones que el Administrador de comisionistas contratará a nombre de la Institución de Fondos de Pago

Electrónico con los Comisionistas que éste administrará, así como, en su caso, las Operaciones y servicios que realizará el propio Administrador de comisionistas.

b) Los límites que aplicarán a cada una de las Operaciones conforme a las disposiciones aplicables.

c) Los derechos y obligaciones que tendrán tanto la Institución de Fondos de Pago Electrónico como el comisionista o el Administrador de comisionistas, así como las respectivas consecuencias legales y sanciones aplicables en caso de incumplimiento a los términos del contrato.

d) La facultad de la Institución de Fondos de Pago Electrónico para suspender la realización de operaciones o dar por terminado el respectivo contrato, ambas sin responsabilidad, en caso de que el comisionista o el Administrador de comisionistas incumplan la normatividad aplicable, el contrato o presenten cambios en su operación que afecten las condiciones del servicio contratado.

e) Las medidas correctivas que la Institución de Fondos de Pago Electrónico implementaría por el incumplimiento del comisionista o del Administrador de comisionistas a las disposiciones aplicables.

f) La prohibición para el comisionista o Administrador de comisionistas de:

   i. Condicionar la realización de la operación a la adquisición de un producto o servicio.
   ii. Publicitarse o promocionarse de cualquier forma a través de la papelería o en el anverso de los comprobantes que proporcionen a los Clientes a nombre de la Institución de Fondos de Pago Electrónico de que se trate.
   iii. Realizar las Operaciones objeto de la comisión en términos distintos a los pactados con la Institución de Fondos de Pago Electrónico correspondiente.
   iv. Subcontratar los servicios relacionados a la comisión mercantil.
   v. Cobrar comisiones, por cuenta propia, a los Clientes por la prestación de los servicios objeto de la comisión mercantil, o bien recibir diferenciales de precios o tasas respecto de las operaciones en que intervengan.
   vi. Llevar a cabo Operaciones con los Clientes a nombre propio.
   vii. Pactar en exclusiva con la Institución de Fondos de Pago Electrónico, la realización de las Operaciones y actividades consistentes en la recepción de pagos de servicios con cargo a cuentas de fondos de pago electrónico.

h) Asimismo, deberá quedar constancia, dentro del contrato, de la aceptación expresa por parte del comisionista o Administrador de comisionistas de las obligaciones siguientes:

   i. Apegarse a lo previsto en el artículo 54 de la Ley.
   ii. Entregar en el desarrollo de la auditoría y a solicitud de la Institución de Fondos de Pago Electrónico, al auditor externo independiente de la propia Institución de Fondos de Pago Electrónico y a la CNBV, los libros, sistemas, registros, manuales y documentos en

general, relacionados con la prestación del servicio de que se trate, así como permitir al auditor externo independiente o al personal de la CNBV el acceso a sus oficinas e instalaciones en general, relacionadas con la prestación del servicio en cuestión.

iii. Informar a la Institución de Fondos de Pago Electrónico respecto de cualquier modificación a su objeto social o cualquier otro cambio que pudiera afectar las operaciones objeto de la contratación, con por lo menos treinta días de anticipación a que suceda dicha modificación o cambio.

iv. Guardar confidencialidad respecto de la información que haya sido recibida, transmitida, procesada o almacenada durante la realización de las operaciones. Asimismo, aceptar que dicha información solamente podrá usarse y explotarse para los fines pactados en el contrato.

v. Manifestar la aceptación de la responsabilidad directa por el uso indebido de la información de la Institución de Fondos de Pago Electrónico y, en su caso, pagar las indemnizaciones por daños y perjuicios causados por cualquier incumplimiento a lo señalado en el inciso anterior.

vi. Cumplir con los términos, condiciones y procesos para garantizar a la Institución de Fondos de Pago Electrónico la transferencia, devolución y eliminación segura de la información sujeta a la comisión contratada cuando el contrato se dé por terminado.

vii. Prevenir el uso indebido de los factores de autenticación de los Clientes y empleados que operen el servicio contratado.

viii. Medidas que deberá instrumentar la Institución de Fondos de Pago Electrónico para apegarse a las disposiciones de carácter general a que se refiere el artículo 58 de la Ley, emitidas por la Secretaría, o las que las sustituyan.

ix. Capacitar al personal respecto del proceso para realizar Operaciones, el uso de la infraestructura tecnológica del comisionista y la seguridad de la información.

Las Instituciones de Fondos de Pago Electrónico deberán presentar a la CNBV la solicitud de autorización a que se refiere el presente artículo, con una anticipación de por lo menos 20 días hábiles a la fecha en que pretendan realizar la contratación.

Las Instituciones de Fondos de Pago Electrónico podrán facultar a terceros, a través de un mandato o comisión, para que contraten a su vez a un Administrador de comisionistas.

En este caso, las Instituciones de Fondos de Pago Electrónico deberán establecer que corresponderá a los Administradores de comisionistas asegurarse de que los comisionistas que contraten cumplan con lo establecido en el presente artículo, así como el anexo 7 de las presentes disposiciones.

Lo previsto en este artículo es sin perjuicio de la autorización que podrá obtener la Institución de Fondos de Pago Electrónico para que su propio Administrador de comisionistas sea a su vez comisionista.

Artículo 48.- Las Instituciones de Fondos de Pago Electrónico, en la realización de las Operaciones a través de comisionistas a que se refiere el artículo 46 anterior, deberán sujetarse a los límites siguientes:

I. Tratándose de las Operaciones a que se refiere la fracción I del artículo 46 anterior, el límite por comisionista no podrá exceder de un monto diario equivalente en moneda nacional a 1,500 UDIS, por cuenta.
II. Tratándose de las Operaciones a que se refiere la fracción II del artículo 46 anterior, el límite por comisionista no podrá exceder de un monto diario equivalente en moneda nacional a 4,000 UDIS, por cuenta.

Artículo 49.- Las Instituciones de Fondos de Pago Electrónico deberán acompañar a la solicitud de autorización a que se refiere el artículo 44 o, en su caso, al aviso a que se refiere el artículo 45 de las presentes disposiciones, lo siguiente:

I. La descripción detallada y diagramas de flujo de los procesos de los servicios a contratar, considerando las actividades que se pretendan realizar por la Institución de Fondos de Pago Electrónico, así como por el prestador del servicio; las áreas de la propia Institución de Fondos de Pago Electrónico y del tercero que participan en el flujo del servicio; nombre, descripción y funcionalidad de los sistemas que, en su caso, serán contratados para la prestación del servicio, o los sistemas de la Institución de Fondos de Pago Electrónico que serán utilizados por el proveedor respectivo.
II. El proyecto de contrato de prestación de servicios, en el que deberá señalarse la fecha contemplada de su celebración, los derechos y obligaciones de la Institución de Fondos de Pago Electrónico y del tercero, incluyendo la determinación sobre la propiedad intelectual respecto de los diseños, desarrollos o procesos utilizados para la prestación del servicio. Dicho proyecto de contrato deberá ser presentado en idioma español.

Asimismo, deberá quedar constancia, dentro del contrato, de la aceptación expresa por parte del tercero de las obligaciones siguientes:

a) Apegarse a lo previsto en el artículo 54 de la Ley.
b) Entregar en el desarrollo de la auditoría y a solicitud de la Institución de Fondos de Pago Electrónico, al Tercero Independiente de la propia Institución de Fondos de Pago Electrónico, así como al Banco de México y a la CNBV, los libros, sistemas, registros, manuales y documentos en general, relacionados con la prestación del servicio de que se trate. Asimismo, permitir al Tercero Independiente o al personal del Banco de México o de la CNBV el acceso a sus oficinas e instalaciones en general, relacionadas con la prestación del servicio en cuestión.
c) Informar a la Institución de Fondos de Pago Electrónico respecto de cualquier modificación a su objeto social o cualquier otro cambio que pudiera afectar la prestación del servicio objeto de la contratación, con por lo menos treinta días de anticipación a que suceda dicha modificación o cambio.
d) Guardar confidencialidad respecto de la información que haya sido recibida, transmitida, procesada o almacenada durante la prestación de los servicios. Asimismo, aceptar que dicha información solamente podrá

usarse y explotarse para los fines pactados en la prestación del servicio.

e) En caso de que el tercero realice la subcontratación para la prestación parcial o total de alguno de los servicios prestados a las Instituciones de Fondos de Pago Electrónico, deberá notificar a la propia institución respecto de dicha subcontratación; asimismo, establecerá los mecanismos para que el subcontratado cumpla con las obligaciones pactadas y proporcione la información para los efectos del artículo 51 de las presentes disposiciones.

f) Cumplir con los términos, condiciones y procesos para que el tercero garantice a la Institución de Fondos de Pago Electrónico la transferencia, devolución y eliminación segura de la información sujeta al servicio contratado cuando deje de prestarlo.

g) Mantener registros de auditoría íntegros que incluyan la información detallada de los accesos o intentos de acceso y la operación o actividad efectuadas por los Usuarios de la Infraestructura Tecnológica. Dichos registros deberán estar a disposición del personal autorizado de la Institución de Fondos de Pago Electrónico.

h) Contar con controles de acceso a la información de acuerdo con los niveles de acceso y perfiles determinados por la Institución de Fondos de Pago Electrónico.

i) Permitir a la Institución de Fondos de Pago Electrónico realizar las revisiones de seguridad que se señalan en los artículos 21, 33 y 34 de las presentes disposiciones a los servicios contratados, o bien, proporcionar evidencia de la realización de estas revisiones.

III. La siguiente documentación respecto de la Infraestructura Tecnológica:

a) La descripción de los enlaces de comunicación utilizados por la Institución de Fondos de Pago Electrónico para conectarse con el proveedor de servicios, que incluya el nombre del proveedor, el ancho de banda y el tipo de servicio prestado, entre otros.

b) Un diagrama de telecomunicaciones en donde se muestre la conexión existente entre cada uno de los participantes en la prestación del servicio (proveedores, centros de datos, Institución de Fondos de Pago Electrónico, entre otros), incluyendo los esquemas de redundancia.

c) La dirección completa del lugar en donde se realizarán cada uno de los servicios, así como de los centros de datos, primario y secundario, en donde se almacenará y procesará la información. En caso de que el lugar señalado se encuentre en territorio nacional, debe incluirse, por lo menos, calle, número exterior e interior, colonia, alcaldía o municipio, código postal y entidad federativa. Tratándose de un sitio localizado en el extranjero, deberán incluirse datos similares que permitan ubicar con certeza el lugar señalado. Tratándose de servicios de Computo en la Nube, solamente deberán proporcionar lo señalado en el artículo 50 de las presentes disposiciones.

d) En su caso, el esquema de interrelación de aplicaciones o sistemas

objeto de la contratación, incluyendo los sistemas propios de la Institución de Fondos de Pago Electrónico.

e) Los mecanismos de continuidad del servicio contratado.

f) Para los casos en que el tercero mantenga Información Personal e Información Sensible, así como imágenes de identificaciones oficiales del Cliente fuera del territorio nacional, la Institución de Fondos de Pago Electrónico deberá acreditar que dicha información se encuentre cifrada y que los mecanismos y procedimientos para descifrarla estén en posesión del oficial en jefe de seguridad de la información, quien será responsable, en caso de pérdida, de la ejecución de los referidos mecanismos y procedimientos.

IV. Los mecanismos que permitirán a la Institución de Fondos de Pago Electrónico mantener en sus instalaciones los registros detallados de todas las Operaciones que se realicen, así como de sus registros contables al cierre diario. Dichos registros deberán mantenerse en un formato que permita su consulta y uso, con independencia de que el servicio contratado con el tercero no se encuentre disponible.

V. Cuando el tercero tenga privilegios de acceso a las imágenes de identificaciones oficiales o información biométrica de los Clientes, presentar evidencia de los controles que mantendrá para garantizar la confidencialidad, integridad y disponibilidad de esta información.

VI. Descripción de los mecanismos para vigilar el desempeño del tercero contratado y el cumplimiento de sus obligaciones contractuales, incluyendo al menos, las previstas en las presentes disposiciones.

VII. Planes para evaluar y reportar al Órgano de Administración o, en su caso, al comité de auditoría de la Institución de Fondos de Pago Electrónico, según la importancia del servicio contratado, el desempeño del tercero y el cumplimiento de la regulación aplicable relacionada con dicho servicio.

VIII. Evidencia que permita verificar que los terceros tengan e implementen políticas de protección de datos personales y confidencialidad de la información que permitan a la Institución de Fondos de Pago Electrónico cumplir con las disposiciones legales que la rigen en la materia.

Tratándose de servicios que se procesen, proporcionen o ejecuten total o parcialmente fuera de territorio nacional, las Instituciones de Fondos de Pago Electrónico deberán acompañar la documentación que acredite que los terceros residen en países cuyo derecho interno proporciona protección a los datos de las personas, resguardando su debida confidencialidad, o bien, que dichos países mantengan suscritos con México acuerdos internacionales en dicha materia o de intercambio de información entre los organismos supervisores, tratándose de Entidades Financieras. Adicionalmente, las Instituciones de Fondos de Pago Electrónico deberán:

a) Contar con la aprobación del Órgano de Administración respecto a que no habrá impacto en la continuidad de la operación de la Institución de Fondos de Pago Electrónico, con motivo de la distancia geográfica y, en su caso, del lengua-

je que se utilizará en la prestación del servicio.

b) Contar con esquemas de soporte técnico que permitan solucionar problemas e incidencias, con independencia de las diferencias que, en su caso, existan en husos horarios y días hábiles.

Adicionalmente, en el evento de que alguna autoridad del país de origen del tercero a que se refiere esta fracción le requiera información relacionada con los servicios que le presta a la Institución de Fondos de Pago Electrónico, el tercero deberá, tan pronto como sea jurídicamente posible, informar de ello a la referida institución, así como proporcionarle copia de la información que haya entregado a dicha autoridad. En este caso, la Institución de Fondos de Pago Electrónico deberá informar mediante correo electrónico que se envíe a la cuenta ifpe@banxico.org.mx y en la oficialía de partes de la CNBV, de tal situación inmediatamente después de que tenga conocimiento de ello, así como proporcionarle copia de la información referida.

El Banco de México y la CNBV contarán con un plazo de veinticinco días hábiles para resolver respecto de la solicitud de autorización a que se refiere el presente artículo; transcurrido este plazo sin pronunciamiento alguno, se entenderá la resolución en sentido positivo. Cualquier requerimiento de información adicional que realice el Banco de México o la CNBV interrumpirá el plazo señalado en este párrafo.

Artículo 50.- La Institución de Fondos de Pago Electrónico que se ubique en los supuestos previstos en este artículo y contrate con algún tercero la prestación de servicios de Cómputo en la Nube para realizar procesos cuya interrupción, parcial o permanente, imposibiliten a la Institución de Fondos de Pago Electrónico la emisión, administración, redención o transmisión de fondos de pago electrónico, conforme a los actos a los que refieren las fracciones II, III, IV y V del Artículo 22 de la Ley, deberá mantener la capacidad de cómputo y procesamiento necesaria para realizar, al menos, los actos a los que se refiere el presente artículo en territorio nacional, o mantener dicha capacidad a través de un prestador de servicios cuya persona o Grupo de Personas que ejerzan el Control, sean distintos al tercero referido y que estén constituidos y sujetos a jurisdicciones nacionales distintas a aquélla en que se haya constituido y quede sujeto dicho tercero.

Únicamente quedarán obligadas a observar lo dispuesto en el presente artículos las Instituciones de Fondos de Pago Electrónico que se ubiquen en alguno se los supuestos siguientes:

I. Durante un periodo de doce meses calendario consecutivos realicen más de 1.2 millones de Transferencias, o envíen o reciban Transferencias por un monto total superior a 3.6 mil millones de UDIS, o bien,

II. En cualquier momento hayan contado con más de 100 mil cuentas de fondos de pago electrónico que, durante un periodo de doce meses calendario consecutivos, hayan tenido en cualquier momento saldo positivo o que hayan enviado al menos una Transferencia en dicho periodo, o hayan contado con un saldo total en las Cuentas de Fondos de Pago Electrónico que lleven a sus Clientes superior a 300 millones de UDIS.

Las Instituciones de Fondos de Pago Electrónico tendrán un plazo de 180 días naturales contados a partir del primer día del mes

calendario inmediato posterior a aquél en el que se cumpla alguna de las características establecidas en las fracciones I y II del presente Artículo para dar cumplimiento a lo establecido en este Artículo.

Artículo 51.- Las Instituciones de Fondos de Pago Electrónico para la contratación de servicios con terceros que sean objeto de autorización en términos del artículo 44 de estas disposiciones, así como aquellos relacionados con procesos operativos y con administración de bases de datos y sistemas informáticos, deberán dar cumplimiento a lo siguiente:

I. Tratándose de terceros que proporcionen servicios relacionados con procesos operativos y con administración de bases de datos y sistemas informáticos, pactar lo señalado en la fracción II del artículo 47 y conservar el contrato respectivo.
II. Realizar, al menos anualmente, auditorías internas o externas sobre el servicio contratado o contar con evidencia de que el tercero contratado las lleva a cabo.
III. Mantener en sus oficinas principales, al menos, la documentación e información relativa a las evaluaciones, resultados de auditorías y, en su caso, los planes de trabajo que correspondan, así como los reportes de desempeño de los terceros contratados, incluyendo documentación respecto del cumplimiento de lo señalado en la fracción I de este artículo.
IV. Actualizar la descripción o documentación respectiva cuando existan modificaciones que se consideren que tienen un impacto relevante en cuanto al servicio proporcionado o que estén relacionadas con los sistemas, equipos y aplicaciones objeto de la contratación o con sus características técnicas.
V. Respecto de la Infraestructura Tecnológica y seguridad de la información, además de la información determinada en el artículo 49, fracción III, incisos b) y d) de estas disposiciones, contar con la siguiente documentación:

    a) La descripción de las características técnicas de los sistemas, equipos y aplicaciones objeto de la contratación que contenga al menos lo señalado en el Anexo 8 de estas disposiciones.
    b) Aquélla en donde se detallen los mecanismos para asegurar la transmisión y almacenamiento de la información en forma Cifrada, en su caso, incluyendo la versión de los protocolos de Cifrado y componentes de seguridad en la Infraestructura Tecnológica.
    c) La que contenga el detalle del tipo de información de la Institución de Fondos de Pago Electrónico y Clientes, precisando, en su caso, el tipo de Información Personal o Información Sensible que será almacenada por el tercero en sus equipos o instalaciones, o a la que podrá tener acceso, en su caso.
    d) La descripción de los mecanismos de control y vigilancia del acceso a los sistemas informáticos y a la Información Personal o Información Sensible transmitida, almacenada, procesada, resguardada o custodiada en dichos sistemas, así como de las bitácoras, bases de datos y configuraciones de seguridad que se establezcan al efecto.

e) La evidencia de los controles y de los mecanismos de control a que se refiere la fracción V del artículo 49 de estas disposiciones.

VI. Contar con la evidencia a que alude la fracción VIII del artículo 49 anterior.

Artículo 52.- Las Instituciones de Fondos de Pago Electrónico deberán contar con un padrón de todos los prestadores de servicios, incluyendo aquellos proveedores subcontratados por éstos, así como de los Administradores de comisionistas y comisionistas contratados, que contenga, al menos, la siguiente información:

A) Prestadores de servicios:

I. Nombre, denominación o razón social del prestador de servicios.
II. Nombre del representante legal del prestador de servicios.
III. Descripción del servicio contratado con el tercero, incluyendo los datos o información que, en su caso, son almacenados, procesados o transmitidos por éste.
IV. En su caso, información de los sistemas que soportan el servicio contratado con el tercero, que incluya al menos el nombre, versión y función o propósito.
V. En su caso, interfaces con otros sistemas y el propósito de éstas, incluyendo el detalle de la información que intercambia.
VI. Ubicación en donde se realiza el servicio y en donde se encuentra el personal responsable de llevarlo a cabo.
VII. En su caso, ubicación o juridiscción del centro de datos principal en donde se encuentran los equipos de procesamiento del sistema contratado.
VIII. En su caso, ubicación o juridiscción del centro de datos alterno en donde se encuentran los equipos de procesamiento, tratándose de la recuperación del servicio contratado.
IX. En su caso, número y fecha del oficio con el que el Banco de México y la CNBV otorgaron la autorización.

B) Administrador de Comisionistas o Comisionistas:

I. Nombre, denominación o razón social del Comisionista o del Administrador de comisionistas.
II. Nombre del representante legal del Comisionista o del Administrador de comisionistas.
III. Nombre comercial del Comisionista o del Administrador de comisionistas, así como detalle de la modalidad comercial bajo la que opera, ya sea que se trate de una cadena comercial o franquicia.
IV. Número de Establecimientos del Comisionista en los que se realizan las comisiones mercantiles, y de cada uno de ellos su domicilio completo, incluyendo la clave de la localidad geoestadística conforme al Catálogo Único de Claves de Áreas Geoestadísticas Estatales, Municipales, y Localidades del Instituto Nacional de Estadística y Geografía, o el que lo sustituya.
V. Tipo de Operación que realiza el Comisionista a nombre y por cuenta de la Institución de Fondos de Pago Electrónico.
VI. Límites de las Operaciones pactadas con el Comisionista o con el Administrador de comisionistas.
VII. Dispositivos de acceso utilizados para ofrecer los servicios a los Clientes, tales como teléfono móvil, tabletas electrónicas, terminales punto de venta, entre otros.

VIII. En su caso, número de oficio y fecha en la que se otorgó la autorización para la contratación del Comisionista o Administrador de comisionistas.

Las Instituciones de Fondos de Pago Electrónico deberán difundir a través de su página de internet o aplicación, el listado de los módulos o establecimientos que los Comisionistas o el Administrador de comisionistas tengan habilitados para realizar las Operaciones referidas en el artículo 47 de las presentes disposiciones, especificando las Operaciones que se pueden realizar en cada uno de ellos y los montos máximos autorizados por Operación.

Las Instituciones de Fondos de Pago Electrónico deberán mantener actualizados los padrones a que se refiere este artículo.

Artículo 53.- La Institución de Fondos de Pago Electrónico deberá realizar al menos anualmente, por sí misma o a través de un tercero, auditorías que tengan por objeto verificar el grado de cumplimiento de las presentes disposiciones. En su caso, si el Comisionista o Administrador de comisionistas cuenta con resultados de auditoría con el mismo objeto realizados previamente con vigencia máxima de un año, podrán presentarlos a la Institución de Fondos de Pago Electrónico. Sin perjuicio de lo anterior, la CNBV podrá ordenar la realización de auditorías cuando a su juicio existan condiciones de riesgo en materia de operación y seguridad de la información.

Artículo 54.- Las Instituciones de Fondos de Pago Electrónico deberán mantener plenamente identificadas en todo momento las Operaciones que realicen a través del Comisionista o del Administrador de comisionistas de manera independiente de las que realicen a través de sus Plataformas.

Asimismo, las Instituciones de Fondos de Pago Electrónico deberán verificar que los Comisionistas o Administrador de comisionistas informen por cualquier medio a los Clientes de las propias Instituciones de Fondos de Pago Electrónico, que actúan a nombre y por cuenta de la Institución de Fondos de Pago Electrónico de que se trate.

Artículo 55.- Las instituciones de fondos de pagos electrónico responderán en todo momento tanto por el servicio que sus Comisionistas o Administrador de comisonistas proporcionen a los Clientes, aun cuando la realización de las Operaciones correspondientes se lleve a cabo en términos distintos a los pactados, así como por el incumplimiento a las disposiciones en que incurran dichos Comisionistas.

En caso de incumplimiento por parte de los Comisionistas o Administrador de comisonistas a las disposiciones aplicables, las Instituciones de Fondos de Pago Electrónico deberán implementar las medidas correctivas necesarias.

Lo establecido en los dos párrafos anteriores será sin perjuicio de las responsabilidades civiles, administrativas o penales, en que los Comisionistas o Administrador de comisionistas o sus empleados, puedan incurrir por las violaciones de las disposiciones legales aplicables.

Lo señalado en el párrafo anterior deberá establecerse en el contrato que se celebre entre la Institución de Fondos de Pago Electrónico y el Comisionista o el Administrador de comisionistas.

CAPÍTULO VI
DE LA EVALUACIÓN A TRAVÉS DE TERCEROS INDEPENDIENTES

Artículo 56.- Las Instituciones de Fondos de Pago Electrónico deberán contratar los servicios de un Tercero Independiente, para la evaluación del nivel de cumplimiento de los requerimientos de seguridad de infor-

mación, el uso de Canales de Instrucción y continuidad operativa que dichas instituciones deben observar conforme a lo previsto en los capítulos II, III, IV y V de las presentes Disposiciones.

Artículo 57.- La evaluación del nivel de cumplimiento realizado por el Tercero Independiente a que se refiere el artículo anterior deberá realizarse cada dos años.

El informe de la evaluación de cumplimiento deberá ser entregado por el Tercero Independiente al Órgano de Administración de la Institución de Fondos de Pago Electrónico y presentado al comité de auditoría de dicha institución, cuando cuente con éste.

Las Instituciones de Fondos de Pago Electrónico no podrán contratar los servicios de un Tercero Independiente, ni de las personas morales por medio de las cuales presten los servicios respectivos, para obtener la evaluación de cumplimiento a que se refiere este artículo por más de dos periodos de evaluación consecutivos. Sin perjuicio de lo anterior, la Institución de Fondos de Pago Electrónico podrá designar nuevamente al mismo Tercero Independiente o persona moral referida, después de una interrupción mínima de cinco años contados a partir de la última evaluación de cumplimiento que hubiere otorgado respecto de dicha institución.

En el caso que de la evaluación realizada se deriven observaciones que a juicio del Tercero Independiente representen violaciones graves, la Institución de Fondos de Pago Electrónico de que se trate deberá presentar el informe de la evaluación de cumplimiento a su Consejo de Administración dentro de los 20 días hábiles siguientes de finalizada la evaluación por el Tercero Independiente, o en cinco días hábiles en caso de tratarse de Administrador Único.

El mencionado informe deberá entregarse al Banco de México y a la CNBV, mediante correo electrónico que se envíe a la cuenta ifpe@banxico.org.mx y en la oficialía de partes de la CNBV, dentro de un plazo de cinco días hábiles contados a partir de la presentación a su Órgano de Administración de dicho informe. El informe deberá firmarse digitalmente por el director general o, en su caso, el Administrador Único, y ser cifrado conforme a lo dispuesto en el artículo 33.

Además, la Institución de Fondos de Pago Electrónico deberá presentar, mediante correo electrónico que se envíe a la cuenta ifpe@banxico.org.mx y en la oficialía de partes de la CNBV, y dentro de un plazo de 20 días hábiles siguientes a la finalización de la evaluación realizada por el Tercero Independiente, un plan de remediación para subsanar dichas observaciones. El plan de remediación deberá firmarse digitalmente por el director general o, en su caso, el Administrador Único, y ser cifrado de conformidad con lo dispuesto en el artículo 33. La CNBV y el Banco de México podrán efectuar observaciones, en cualquier tiempo, a dicho plan de remediación.

Artículo 58.- Los Terceros Independientes que evalúen el nivel de cumplimiento de las Instituciones de Fondos de Pago Electrónico a las normas contenidas en las presentes Disposiciones, así como las personas morales por medio de las cuales éstos presten los servicios respectivos, deberán ser independientes a la fecha de celebración del contrato de prestación de servicios, durante el desarrollo de la evaluación de cumplimiento y hasta la emisión del reporte de la evaluación de cumplimiento de que se trate y deberán cumplir con lo señalado en el Anexo 6 de las presentes Disposiciones.

TRANSITORIOS

Primero.- Las presentes Disposiciones entrarán en vigor al día siguiente al de su publicación en el *Diario Oficial de la Federación*.

Segundo.- Las Instituciones de Fondos de Pago Electrónico contarán con un plazo de 12 meses, posteriores a la entrada en vigor de este instrumento en el *Diario Oficial de la Federación*, para dar cumplimiento a lo establecido en los artículos 16 y 17.

Tercero.- Las personas a que alude la Disposición Octava Transitoria de la Ley para Regular las Instituciones de Tecnología Financiera y que hayan obtenida su autorización para operar como Institución de Fondos de Pago Electrónico, tendrán un plazo no mayor a seis meses contados a partir de la fecha de entrada en vigor de las presentes Disposiciones, para realizar el análisis a que se refiere el artículo 21 y la evaluación a que se refiere el artículo 33 de las presentes Disposiciones, generar un plan de remediación documentado para atender lo referente a cada artículo, así como para mostrar evidencia de las correcciones realizadas conforme a dicho plan y presentarlo al Banco de México y a la Comisión Nacional Bancaria y de Valores.

ANEXO 1
Indicadores de seguridad de la información

El oficial en jefe de seguridad de la información de la Institución de Fondos de Pago Electrónico, en relación con los indicadores de riesgo en materia de seguridad de la información a que se refiere la fracción XI del artículo 36, de las presentes disposiciones, deberá:

1. Evaluar dichos indicadores, los cuales deberán ajustarse a los umbrales contenidos en este anexo para cada indicador. En caso de definir umbrales diferentes, deberá documentar el motivo.
2. Definir planes de remediación para aquellos riesgos en los que los resultados de la evaluación arrojen valores que se encuentren dentro de los umbrales medios y altos de riesgo establecidos en el presente anexo o, en su caso, aquellos definidos por la Institución de Fondos de Pago Electrónico, siempre que éstos se encuentren en un umbral alto por, al menos, dos periodos consecutivos.
3. Dar mantenimiento continuo, ya sea para agregar, eliminar o actualizar los indicadores clave de riesgo y de desempeño de seguridad de la información ya existentes, los cuales siempre deberán estar alineados a la estrategia de la Institución de Fondos de Pago Electrónico y al Plan Director de Seguridad de la información de ésta.
4. Medir y evaluar su evolución con la periodicidad indicada en las siguientes tablas, o antes en caso de eventos inusuales.
5. En caso de que no apliquen todos los supuestos, indicar que no son aplicables y explicar el motivo.

Tipo	*Definición*	*Subtipo*	*Subclase de eventos*	*Ejemplos*
I. Fraude interno	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente, o bien, soslayar regulaciones, leyes o políticas empresariales (excluidos los eventos de diversidad / discriminación) en las que se encuentra implicada, al menos, una parte interna a la Institución de Fondos de Pago Electrónico.	1.1 Actividades no autorizadas.	Operaciones no reveladas (intencionalmente). Operaciones no autorizadas (con pérdidas pecuniarias). Valoración errónea de posiciones (intencional).	Operaciones no comunicadas, operaciones no autorizadas (con pérdidas pecuniarias), valoración errónea de posiciones y omisión intencional de normativa.
		1.2 Robo y fraude internos.	Fraude / depósitos sin valor. Extorsión / malversación / robo. Apropiación indebida de activos. Destrucción dolosa de activos. Falsificación interna. Contrabando. Apropiación de cuentas, de identidad, entre otros. Incumplimiento / evasión de impuestos (intencional). Cohecho. Abuso de información privilegiada (no a favor de la empresa).	Robo, malversación, apropiación indebida, destrucción de activos, falsificaciones, suplantación de identidad y cohechos, manipulación de cuentas.
		1.3. Seguridad de los sistemas.	Vulneración de sistemas de seguridad. Daños por ataques informáticos. Robo de información (con pérdidas pecuniarias). Utilización inadecuada de claves de acceso y/o niveles de autorización.	Abuso y utilización de información privilegiada o confidencial, alteración de aplicaciones informáticas, robo de contraseñas y accesos informáticos prohibidos.

Tipo	*Definición*	*Subtipo*	*Subclase de eventos*	*Ejemplos*
II. Fraude externo	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte de un tercero.	2.1 Hurto y fraude externos.	Robo / estafa / extorsión /cohecho. Falsificación externa / suplantación de personalidad. Uso y/o divulgación de información privilegiada. Espionaje industrial. Contrabando.	Documentaciones falsificadas o manipuladas (transferencias, etcétera), suplantación de identidad, disposiciones indebidas, monedas falsas, billetes deteriorados o fuera de curso legal, robos en las instalaciones de la IFC y uso indebido de tarjetas robadas o falsificadas.
		2.2 Seguridad de los sistemas.	Vulneración de sistemas de seguridad. Daños por ataques informáticos. Robo de información (con pérdidas pecuniarias). Utilización inadecuada de claves de acceso y/o niveles de autorización.	Acceso informático no autorizado, manipulación de aplicaciones informáticas, daños por ataques informáticos y robo de información.
VI. Incidencias en el negocio y fallos en los sistemas	Pérdidas derivadas de incidencias en el negocio y de fallas en los sistemas.	6.1 Sistemas.	Hardware. Software. Telecomunicaciones. Interrupción / incidencias en el suministro.	Interrupción / incidencias en los suministros y líneas de comunicación, errores en los programas informáticos, fallos en hardware y software, sabotajes, interrupciones del negocio.

ID	*Nombre*	*Descripción*	*Dominio*	*Tipo*	*Subtipo*	*Subclase de Eventos*
KRI0001	Incidentes mediante ataques directos contra los sistemas internos.	Número de incidentes que hayan sido originados por ataques hacia los sistemas internos de la Institución de Fondos de Pago Electrónico, en el periodo establecido.	Ataques lógicos.	II. Fraude externo.	2.2 Seguridad de los sistemas.	2.2.1 Vulneración de sistemas de seguridad.
KRI0002	Casos de fraude en la plataforma.	Porcentaje de casos donde se identifica un fraude, que haya sido originado por ataques hacia la Plataforma.	Ataques lógicos.	II. Fraude externo.	2.2 Seguridad de los sistemas.	2.2.1 Vulneración de sistemas de seguridad.
KRI0003	Equipos de la infraestructura tecnológica de los que se gestiona su configuración de seguridad.	Porcentaje de equipos de infraestructura tecnológica dentro de la plataforma y/o proceso de revisión de estándares de configuración segura, con respecto al total de los equipos de la IFPE durante el periodo establecido.	Cumplimiento.	II. Fraude externo.	2.2 Seguridad de los sistemas.	2.2.1 Vulneración de sistemas de seguridad.

Tipo de indicador	*Periodo*	*Unidad de medi-ción*	*Cálculo*	*Variable X*	*Variable Y*	*Riesgo alto*	*Riesgo medio*	*Riesgo bajo*
Reactivo.	Trimestral.	Cantidad.	Variable X.	Número de casos de incidentes identificados.	-	Más de 1.	Igual a 1.	Igual a 0.
Reactivo.	Mensual.	Porcentual.	(X/Y)*100	Número de casos de fraude en la plataforma.	Número de clientes que usan la plataforma.	Más de .01 por ciento.	Entre 0.005 por ciento y 0.01 por ciento.	
Preventivo.	Mensual.	Porcentual.	(X/Y)*100	Número de equipos dentro de la plataforma o proceso de revisión de estándares de configuración segura.	Número total de equipos.	Menos de 85 por ciento.	Entre 85 por ciento y 95 por ciento.	Más de 95 por ciento.

ID	*Nombre*	*Descripción*	*Dominio*	*Tipo*	*Subtipo*	*Subclase de Eventos*
KRI0004	Nivel de cumplimiento de configuración segura de servidores de los que se gestiona su configuración.	Porcentaje promedio de nivel de cumplimiento de servidores contemplados dentro de la herramienta y/o proceso de revisión de estándares de configuración segura.	Cumplimiento.	II. Fraude externo.	2.2 Seguridad de los sistemas.	2.2.1 Vulneración de sistemas de seguridad.
KRI0005	Usuarios con roles y perfiles inadecuados.	Porcentaje de usuarios con perfiles inadecuados dentro de las aplicaciones de la IFPE, con respecto al total de usuarios en todas las aplicaciones de la Institución de Fondos de Pago Electrónico.	Cumplimiento.	I. Fraude interno	1.3. Seguridad de los sistemas.	Robo de información (con pérdidas pecuniarias). Utilización inadecuada de claves de acceso y/o niveles de autorización.
KRI0006	Aplicaciones sin roles y perfiles.	Porcentaje de aplicaciones las cuales no poseen la capacidad ni el perfilamiento de roles.	Cumplimiento.	I. Fraude interno.	1.3. Seguridad de los sistemas.	1.3.3 Robo de información (con pérdidas pecuniarias).

Tipo de indicador	*Periodo*	*Unidad de medi-ción*	*Cálculo*	*Variable X*	*Variable Y*	*Riesgo alto*	*Riesgo medio*	*Riesgo bajo*
Preventivo.	Mensual.	Promedio porcentual.	Promedio (X)	Por ciento de cumplimiento del estándar de configuración segura de cada uno de los servidores.	-	Menos de 90 por ciento.	Entre 90 por ciento y 95 por ciento.	Más de 95 por ciento.
Correctivo.	Semestral.	Porcentual.	(X/Y)*100	Número de usuarios con perfiles incorrectos, considerando todas las aplicaciones.	Número total de usuarios considerando todas las aplicaciones.	Más de 3 por ciento.	Entre 1 por ciento y 3 por ciento.	Menos de 1 por ciento.
Correctivo.	Trimestral.	Porcentual.	(X/Y)*100.	Número de aplicaciones sin capacidad de	Número total de aplicaciones.	Más de 5 por ciento.	Entre 2 por ciento y 5 por ciento.	Menos de 2 por ciento.

ID	*Nombre*	*Descripción*	*Dominio*	*Tipo*	*Subtipo*	*Subclase de Eventos*
		y permisos, o que dichos perfiles no están implementados, con respecto al total de aplicaciones.				1.3.4 Utilización inadecuada de claves de acceso y/o niveles de autorización.
KRI0007	Incidentes de seguridad de la información en general.	Número total de incidentes reportados durante el periodo establecido referentes a seguridad de la información.	Información.	Aplica a: Fraude interno Fraude externo VI. Incidencias en el negocio y fallos en los sistemas.	Aplican a: 1.3. Seguridad de los sistemas 2.2 Seguridad de los sistemas. 6.1 Sistemas.	Aplican a: Vulneración de sistemas de seguridad Daños por ataques informáticos. Robo de información (con pérdidas pecuniarias). Utilización inadecuada de claves de acceso y/o niveles de autorización.
						2.2.1 Vulneración de sistemas de seguridad.
						2.2.2 Daños por ataques informáticos.
						2.2.3 Robo de información (con pérdidas pecuniarias).
						2.2.4 Utilización inadecuada de claves de acceso y/o niveles de autorización.
						6.1.1Hardware.
						6.1.2 Software.

	Tipo de indicador	*Período*	*Unidad de medición*	*Variable X*	*Variable Y*	*Riesgo alto*	*Riesgo medio*	*Riesgo bajo*	
					perfilamiento o perfilamiento no implementado.				
	Reactivo.	Mensual.	Cantidad.	Variable X.	Número de incidentes de seguridad. de la información	-	Más de 5.	De 2 a 5.	Menos de 2.

ID	*Nombre*	*Descripción*	*Dominio*	*Tipo*	*Subtipo*	*Subclase de Eventos*
						6.1.3 Telecomunicaciones.
						6.1.4 Interrupción / incidencias en el suministro.
KRI0008	Plataformas tecnológicas obsoletas y/o desactualizadas.	Porcentaje de plataformas tecnológicas que se encuentran sobre versiones obsoletas y/o sin soporte por el Fabricante.	Infraestructura.	II. Fraude externo.	2.2 Seguridad de los sistemas.	2.2.1 Vulneración de sistemas de seguridad.
KRI0009	Caídas de sistemas relacionados con los servicios brindados a sus clientes.	Número de caídas de sistemas relacionados con los servicios brindados a sus clientes mayores a 10 minutos.	Infraestructura.	VI. Incidencias en el negocio y fallas en los sistemas.	6.1 Sistemas.	6.1.4 Interrupción / incidencias en el suministro.
KRI0010	Incidentes de seguridad por vulnerabilidades de sistemas provistos por proveedores (terceros).	Porcentaje de incidentes de seguridad causados por vulnerabilidades en sistemas e infraestructura tecnológica provistos por proveedores (terceros) que no pertenezcan a la	Infraestructura.	II. Fraude externo.	2.2 Seguridad de los sistemas.	Vulneración de sistemas de seguridad. Daños por ataques informáticos. Robo de información (con pérdidas pecuniarias).

Tipo de indicador	*Período*	*Unidad de medición*	*Variable X*	*Variable Y*	*Riesgo alto*	*Riesgo medio*	*Riesgo bajo*	
Correctivo.	Semestral	Porcentual.	(X/Y)*10.	Número de plataformas tecnológicas obsoletas.	Total de plataformas tecnológicas.	Más de 5 por ciento.	Entre 2 por ciento y 5 por ciento.	Menos de 2 por ciento
Reactivo.	Mensual.	Cantidad.	Variable X.	Numero de caídas de sistemas.	-	Más de 1.	Igual a 1.	Igual a 0.
Reactivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de incidentes de seguridad de atribuidos a vulnerabilidades en sistemas provistos por	Número total de incidentes de seguridad.	Más de 5 por ciento.	Entre 0.1 por ciento y 5 por ciento.	Menor a 0.1 por ciento.

KRI0011	Vulnerabilidades críticas pendientes de corregir detectadas en las pruebas de hackeo ético.	Número de vulnerabilidades en los sistemas de información que, de acuerdo con las pruebas de hackeo ético, se cataloguen como críticas, las cuales tengan más de un mes de antigüedad a partir de su fecha de detección.	Infraestructura.	II. Fraude externo.	2.2 Seguridad de los sistemas.	2.2.1 Vulneración de sistemas de seguridad.
KRI0012	Indisponibilidad de los sistemas de TI.	Porcentaje promedio del tiempo de indisponibilidad de los sistemas contra el tiempo total del periodo establecido.	Infraestructura.	VI. Incidencias en el negocio y fallas en los sistemas.	6.1 Sistemas.	6.1.4 Interrupción/ incidencias en el suministro.
KRI0013	Incidentes críticos y de alta prioridad en ambientes productivos.	Porcentaje de incidentes calificados como críticos y de alta prioridad en ambientes de producción respecto al total de incidentes en producción.	Infraestructura.	II. Fraude externo.	2.2 Seguridad de los sistemas.	2.2.1 Vulneración de sistemas de seguridad.
KRI0014	Componentes de la infraestructura tecnológica expuestos a internet sin pruebas de hackeo ético y/o análisis de vulnerabilidades.	Porcentaje de los componentes de la infraestructura tecnológica de la organización expuestos a internet, a los cuales no se haya realizado hackeo ético o análisis de vulnerabilidades, con respecto al total de equipos en más de 3 meses.	Infraestructura.	II. Fraude externo.	2.2 Seguridad de los sistemas.	2.2.1 Vulneración de sistemas de seguridad.

Preventivo.	Mensual.	Cantidad.	Variable X.	Número de vulnerabilidades críticas pendientes de corregir con antigüedad de más de un mes.	-	Más de 2.	Entre 1 y 2.	Igual a 0.
Reactivo.	Mensual.	Promedio porcentual.	Promedio(X).	Promedio de tiempo de indisponibilidad de los sistemas de TI.	-	Más de 0.5 por ciento.	Entre 0.25 por ciento y 0.5 por ciento.	Menos de 0.25 por ciento.
Reactivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de incidentes en producción calificados como críticos.	Número total de incidentes en producción.	Mayor o igual a 0.5 por ciento.	Mayor a 0 por ciento y menor 0.5 por ciento.	Igual a 0 por ciento.
Correctivo.	Trimestral.	Porcentual.	(X/Y)*100.	Número de activos expuestos a internet que no hayan realizado pruebas de hackeo ético o análisis de vulnerabilidades.	Número de activos expuestos a internet.	Más de 3 por ciento.	Entre 1 por ciento y 3 por ciento.	Menos de 1 por ciento.

KRI0015	Vulnerabilidades críticas pendientes de corregir detectadas en los analisis de vulnerabilidades	Número de vulnerabilidades en los sistemas de información que, de acuerdo con los análisis de vulnerabilidades se cataloguen como críticas, las cuales, tengan más de un mes de antigüedad a partir de su fecha de detección.	Infraestructura.	II. Fraude sxterno.	2.2 Seguridad de los sistemas.	2.2.1 Vulneración de sistemas de seguridad.
KRI0016	Infraestructura tecnológica obsoleta y/o sin soporte.	Cantidad de equipos e infraestructura tecnológica, que se encuentran en versiones obsoletas o sin soporte, en comparación con toda la infraestructura de IT activa en el periodo establecido.	Infraestructura.	II. Fraude externo.	2.2 Seguridad de los sistemas.	2.2.1 Vulneración de sistemas de seguridad.
KRI0017	Servidores sin solución *antimalware*.	Porcentaje de servidores sin *antimalware* respecto del total de servidores.	*Malware.*	II. Fraude externo.	2.2 Seguridad de los sistemas.	2.2.1 Vulneración de sistemas de seguridad.
KRI0018	Servidores con firmas de *antimalware* desactualizadas.	Porcentaje de servidores con firmas de *antimalware (malware signatures)* desactualizados respecto del total de servidores con *antimalware* en cada IFPE.	*Malware.*	II. Fraude externo.	2.2 Seguridad de los sistemas.	2.2.1 Vulneración de sistemas de seguridad.

Correctivo.	Mensual.	Cantidad.	Variable X.	Número total de vulnerabilidades críticas.	-	Más de 2	Entre 1 y 2	Igual a 0
Correctivo.	Trimestral.	Porcentual.	(X/Y)*100.	Número de equipos e infraestructura obsoleta.	Número total de equipos activos.	Más de 5 por ciento.	Entre 2 por ciento y 5 por ciento.	Menos de 2 por ciento.
Correctivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de servidores sin *antimalware*.	Número total de servidores.	Más de 6 por ciento.	Entre 3 por ciento y 6 por ciento.	Menor a 3 por ciento.
Correctivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de servidores con firmas *antimalware* desactualizadas.	Número total de servidores con *antimalware*.	Más de 6 por ciento	Entre 3 por ciento y 6 por ciento	Menor a 3 por ciento

KRI0019	*Workstations* sin solución *antimalware.*	Porcentaje de *workstations* sin *antimalware* con respecto al total de Equipos.	*Malware.*	II. Fraude externo.	2.2 Seguridad de los sistemas.	2.2.1 Vulneración de sistemas de seguridad.
KRI0020	*Workstations* con firmas de *antimalware* desactualizadas.	Porcentaje de las *workstations* que cuentan con las firmas de antimalware *(malware signatures)* desactualizadas con respecto al total de equipos de cómputo con antimalware instalado.	Malware.	II. Fraude externo.	2.2 Seguridad de los sistemas.	2.2.1 Vulneración de sistemas de seguridad.
KRI0021	Incidentes de seguridad atribuidos a personal de proveedores (terceros).	Porcentaje de incidentes de seguridad relacionados a personal de proveedores (terceros) que no pertenezcan a la nómina de la IFPE, reportadas durante el periodo establecido, con respecto al total de incidentes de seguridad.	Incidentes.	II. Fraude externo.	2.2 Seguridad de los sistemas.	2.2.1 Vulneración de sistemas de seguridad.
KRI0022	Servidores con versiones de sistema operativo obsoletas.	Porcentaje total de servidores con versiones de sistema operativo obsoletas comparado contra número total de servidores.	Software.	II. Fraude externo.	2.2 Seguridad de los sistemas.	2.2.1 Vulneración de sistemas de seguridad.

Correctivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de *workstations sin antimalware.*	Número total de *workstations.*	Más de 8 por ciento.	Entre 4 por ciento y 8 por ciento.	Menor a 4 por ciento.
Correctivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de *workstations* con firmas *antimalware* desactualizadas.	Número de *workstations* con *antimalware.*	Más de 8 por ciento.	Entre 4 por ciento y 8 por ciento.	Menor a 4 por ciento.
Reactivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de incidentes de seguridad relacionados con personal de proveedores (terceros).	Número de incidentes de seguridad total de personal de proveedores (terceros).	Más de 5 por ciento.	Mayor a 0 por ciento y menor 5 por ciento.	Igual a 0 por ciento.
Correctivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de servidores con versiones de sistema operativo obsoletas.	Número total de servidores.	Más de 10 por ciento.	Entre 5 por ciento y 10 por ciento.	Menor a 5 por ciento.

KRI0023	Aplicaciones en producción con cumplimiento parcial o deficiente de los controles de seguridad.	Porcentaje de las aplicaciones en producción con cumplimientos parciales o deficientes, con respecto a las políticas de seguridad establecidas, en cuestiones de seguridad, con respecto al total de aplicaciones.	Software.	II. Fraude externo.	2.2 Seguridad de los sistemas.	2.2.1 Vulneración de sistemas de seguridad.
KRI0024	*Data base managers (DBM)* con versiones de tecnología obsoletas o no soportadas.	Porcentaje de manejadores de *data base managers(DBM),* los cuales son versiones de tecnologías obsoletas o no soportadas por el fabricante, en comparación con el total de *data base managers (DBM)* activos en el periodo establecido.	Software.	II. Fraude externo.	2.2 Seguridad de los sistemas.	2.2.1 Vulneración de sistemas de seguridad.
KRI0025	Aplicaciones obsoletas o no soportadas.	Porcentaje de aplicaciones dentro de la IFC, las cuales se encuentran obsoletas o sin soporte por el fabricante, en relación con todas las aplicaciones activas durante el periodo establecido.	Software.	II. Fraude externo. VI. Incidencias en el negocio y fallos en los sistemas.	2.2 Seguridad de los sistemas. 6.1 Sistemas.	2.2.1 Vulneración de sistemas de seguridad. 6.1.2 Software.
KRI0026	Servidores sin cobertura de parches de seguridad.	Porcentaje de servidores sin los parches de seguridad más recientes, con respecto al total de servidores activos durante el periodo establecido.	Software.	II. Fraude externo.	2.2 Seguridad de los sistemas.	2.2.1 Vulneración de sistemas de seguridad.

Correctivo.	Trimestral.	Porcentual.	(X/Y)*100.	Número de controles de seguridad deficientes en aplicaciones en producción.	Número total de controles de seguridad.	Más de 5 por ciento.	Entre 2 por ciento y 5 por ciento.	Menos de 2 por ciento.
Correctivo.	Trimestral.	Porcentual.	(X/Y)*100.	Número de *data base managers (DBM)* obsoletas o no soportadas.	Número total *data base managers* (DBM).	Más de 10 por ciento.	Entre 5 por ciento y 10 por ciento.	Menos de 5 por ciento.
Correctivo.	Trimestral.	Porcentual.	(X/Y)*100.	Número de aplicaciones obsoletas o no soportadas.	Total de aplicaciones activas.	Más de 5 por ciento.	Entre 2 por ciento y 5 por ciento.	Menos de 2 por ciento.
Correctivo.	Mensual.	Porcentual.	(X/Y)*100.	Número de servidores sin los parches de seguridad más recientes instalados.	Total de servidores.	Más de 5 por ciento.	Entre 2 por ciento y 5 por ciento.	Menos de 2 por ciento.

KRI0027	*Workstations* sin cobertura de parches de seguridad.	Porcentaje de *workstations* sin los de parches de seguridad más recientes indistinto del sistema operativo de que se trate, con respecto al total de *workstations* de la IFPE.	Software.	II. Fraude externo.	2.2 Seguridad de los sistemas.	2.2.1 Vulneración de sistemas de seguridad.
KRI0028	*Data base managers (DBM)* sin cobertura de parches de seguridad.	Porcentaje de *data base managers (DBM)* sin cobertura de los parches de seguridad más recientes, con respecto al total de *data base managers (DBM)* durante el periodo establecido.	Software.	II. Fraude externo.	2.2 Seguridad de los sistemas.	2.2.1 Vulneración de sistemas de seguridad.

Correctivo.	Mensual.	Porcentual.	(X/Y))*100.	Número *workstations* sin los parches de seguridad más recientes instalados totales.	Número de *workstations* totales.	Más de 3 por ciento.	Entre 1 por ciento y 3 por ciento.	Menos de 1 por ciento.
Preventivo.	Trimestral.	Porcentual.	(X/Y)*100.	Número de *data base managers (DBM)* sin cobertura de parches de seguridad.	Número total de *data base managers (DBM).*	Más de 5 por ciento.	Entre 2 por ciento y 5 por ciento.	Menos de 2 por ciento.

ANEXO 2
Requerimientos mínimos para desarrollar el plan de continuidad de negocio

Las Instituciones de Fondos de Pago Electrónico, previo al desarrollo del Plan de Continuidad de Negocio, deberán llevar a cabo:

I. Un análisis de riesgo que:

a) Considere riesgos asociados a los siguientes factores: humanos (incluye fraude, integridad, capacitación), de procesos, tecnológicos y externos (incluidos proveedores externos) conforme a la metodología a que se refiere el artículo 39 de estas disposiciones.
b) Identifique, evalúe, monitoree y mitigue los riesgos relacionados con los procesos operativos y servicios de procesamiento y transmisión de datos contratados con proveedores, así como los relacionados con custodia y resguardo de información de la Institución de Fondos de Pago Electrónico, de sus Clientes.
c) Determine los riesgos derivados de la ubicación geográfica de los centros principales de procesamiento de datos y de operación de los procesos identificados como críticos conforme al análisis de impacto al negocio, para evitar que los centros de procesamiento de datos y de operación alternos estén expuestos en el mismo momento a los mismos riesgos que los principales.
d) Evalúe la necesidad de establecer sitios o servicios alternos de procesamiento de información, así como de operación, los cuales, en su caso, deberán permitir operar en el momento que así se requiera, y no estar sujetos en el mismo momento a los mismos riesgos que el sitio primario.

II. Un análisis de impacto al negocio que:

a) Contenga la totalidad de los servicios y procesos, identificando aquellos que sean críticos y que se consideren indispensables para la continuidad de las operaciones, incluidos los servicios contratados con sus proveedores de servicios.
b) Determine los recursos humanos, logísticos, materiales, de Infraestructura Tecnológica y de cualquier otra naturaleza, mínimos necesarios para mantener y restablecer los servicios y procesos de la Institución de Fondos de Pago Electrónico ante la ocurrencia de una Contingencia Operativa, así como al término de ésta.
c) Elabore escenarios relevantes relativos a las posibles Contingencias Operativas, considerando, entre otros, los siguientes:

i. Desastres naturales y ambientales.
ii. Enfermedades infecciosas.
iii. Ataques cibernéticos o a la actividad informática.
iv. Sabotajes.
v. Terrorismo.
vi. Interrupciones en el suministro de energía.
vii. Fallas o indisponibilidad en la Infraestructura Tecnológica.
viii. Indisponibilidad de recursos humanos, materiales o técnicos.
ix. Interrupciones ocurridas en servicios prestados por terceros.

d) Estime los impactos cuantitativos y cualitativos de las Contingencias Operativas, con base en los escenarios definidos para cada proceso y a través de las metodologías a que se refiere el artículo 39 de estas Disposiciones.
e) Defina la prioridad de recuperación para cada uno de los procesos.
f) Determine el tiempo objetivo de recuperación (conocido como RTO, por sus siglas en inglés), para cada uno de los servicios y procesos. En el caso de los procesos considerados como críticos, el plazo de recuperación no deberá exceder de dos horas.
g) Establezca el punto objetivo de recuperación (conocido como RPO, por sus siglas en inglés), entendido como la máxima pérdida de datos tolerable para cada uno de los servicios y procesos, considerando que la información de aquellas operaciones ya efectuadas no pueda perderse en ningún escenario y que se conozca, de forma oportuna, el estado que tenía cada operación celebrada en el momento en que se presentó la Contingencia Operativa.
h) Identifique y evalúe los riesgos relacionados con los procesos operativos y servicios de procesamiento y transmisión de datos contratados con proveedores, así como los riesgos relacionados con custodia y resguardo de información de la Institución de Fondos de Pago Electrónico.

III. El Plan de Continuidad de Negocio deberá señalar los procesos que tendrán prioridad en la recuperación cuando se presente una Contingencia Operativa, conforme al análisis de impacto a que alude la fracción II anterior del presente anexo.

IV. En el desarrollo del Plan de Continuidad de Negocio se deberán incorporar, al menos, las siguientes acciones:
a) De prevención, que comprenderá al menos la determinación de las actividades y procedimientos relativos a:

i. La reducción de las vulnerabilidades en los procesos y servicios de la Institución de Fondos de Pago Electrónico ante Contingencias Operativas.
ii. La disposición de los recursos humanos, financieros, materiales, técnicos y de Infraestructura Tecnológica necesarios para actuar de manera oportuna ante una Contingencia Operativa.
iii. El establecimiento de un programa anual de pruebas, o bien antes, si ocurre un cambio significativo en la Infraestructura Tecnológica, procesos, productos y servicios, u organización interna de la institución, respecto del funcionamiento y suficiencia del Plan de Continuidad de Negocio que evalúe todas sus etapas y componentes.
iv. Las políticas y procedimientos de capacitación al personal involucrado tanto en los procesos como en el desarrollo del propio plan.
v. Procedimientos de registro, atención, seguimiento y difusión al personal cuyas funciones se vean afectadas por la Contingencia Operativa o estén relacionadas con la ejecución del Plan de Continuidad de Negocio, de los hallazgos, incidencias u observaciones resultantes de las pruebas sobre el funcionamiento y sufi-

ciencia de dicho plan, o bien, de la ejecución del mismo en caso de haberse presentado una Contingencia Operativa.

b) De contingencia, que comprenderá la definición de las acciones y procedimientos de respuesta autorizados para:

   i. Identificar oportunamente la naturaleza de las Contingencias Operativas que afecten los procesos críticos de la Institución de Fondos de Pago Electrónico.
   ii. Contener los efectos de Contingencias Operativas sobre los procesos críticos y favorecer el restablecimiento de la operación a los niveles de funcionamiento requeridos.
   iii. Hacer del conocimiento del Banco de México y la CNBV las Contingencias Operativas, conforme a lo señalado en el artículo 43 de estas Disposiciones.

c) De recuperación, que comprenderá la definición de las acciones y procedimientos a seguir para que los servicios y procesos de las Instituciones de Fondos de Pago Electrónico, ante la materialización de Contingencias Operativas, puedan continuar su operación en un nivel mínimo aceptable, incluidos mecanismos de actualización y conciliación de la información, así como los mecanismos para recuperación en caso de actualizar lo dispuesto en la fracción VII del artículo 49.

d) De restauración, que comprenderá la definición de las acciones y procedimientos para que los servicios y procesos de las Instituciones de Fondos de Pago Electrónico vuelvan a su operación normal después de la ejecución de las acciones de recuperación por la ocurrencia de alguna Contingencia Operativa.

e) De evaluación, que comprenderá lo relativo a la recopilación y análisis de la información relevante sobre el desarrollo de la Contingencia Operativa, y de las acciones y procedimientos seguidos para su prevención, contención, recuperación y restauración a fin de, en su caso, efectuar los ajustes necesarios al Plan de Continuidad de Negocio.

Las Instituciones de Fondos de Pago Electrónico, al definir las diferentes acciones y procedimientos a que hace referencia la presente fracción, deberán en todo momento determinar de manera precisa al personal responsable, así como prever lo relativo a su suplencia o sustitución en caso de que los titulares no se encuentren presentes o disponibles para llevar a cabo lo que el Plan de Continuidad de Negocio establezca.

ANEXO 3
Incidentes en materia de seguridad de la información

I. Información de la Institución de Fondos de Pago Electrónico.

   a) Nombre de la Institución de Fondos de Pago Electrónico.
   b) Nombre completo del oficial en jefe de seguridad de la información, así como su número de teléfono y dirección de correo electrónico.

II. Información detallada del Incidente de Seguridad de la Información.

Descripción del Incidente de Seguridad de la Información			
a)	Fecha y hora en que ocurrió.		
b)	Fecha y hora en que se detectó.		
c)	Duración del incidente.		
d)	¿La información involucrada en el incidente es administrada por terceros?	Sí ( )	No ( )
e)	En caso de ser afirmativo el inciso d), detallar datos del proveedor (nombre, dirección y datos de contacto, correo electrónico, teléfono, entre otros).		

Afectación provocada por el Incidente de Seguridad de la Información			
f)	¿El incidente puede ocasionar una pérdida monetaria para los Clientes o para la propia IFPE?	Sí ( )	No ( )
g)	¿Es viable recuperar de manera directa (gestiones propias) o indirecta (a través de seguros) la posible pérdida monetaria?	Sí ( )	No ( )
h)	¿Se han identificado otros incidentes relacionados con el que se reporta, sea por origen, modo de operación o afectación?	Sí ( )	No ( )

Indicar, en su caso, el tipo de información comprometida con el Incidente de Seguridad de la Información, conforme a las tablas siguientes:

Información personal comprometida del Cliente		
Nombres.	Sí ( )	No ( )
Domicilios.	Sí ( )	No ( )
Números de teléfono.	Sí ( )	No ( )
Direcciones de correo electrónico.	Sí ( )	No ( )
Datos biométricos (huellas dactilares, patrones en iris o retina o reconocimiento facial, entre otros).	Sí ( )	No ( )
Otro(s):		

Información de Cuentas o saldos		
Números de tarjetas, u otros.	Sí ( )	No ( )
Números de Cuenta.	Sí ( )	No ( )
Contraseñas o números de Identificador de Cliente.	Sí ( )	No ( )
Identificadores de Clientes.	Sí ( )	No ( )
Límites.	Sí ( )	No ( )
Saldos.	Sí ( )	No ( )
Otro(s):		

Información de la IFPE		
Claves de acceso.	Sí ( )	No ( )
Configuraciones de seguridad.	Sí ( )	No ( )
Identificación de puertos o servicios.	Sí ( )	No ( )
Direcciones IP de componentes o servicios.	Sí ( )	No ( )
Direcciones IP de componentes internos.	Sí ( )	No ( )
Acceso a segmentos internos de red.	Sí ( )	No ( )
Versiones de software, sistemas operativos o bases de datos.	Sí ( )	No ( )
Identificación de vulnerabilidades.	Sí ( )	No ( )
Otro(s):		

III. Clasificar el Incidente de Seguridad de la Información reportado con base en las siguientes definiciones:

Daño no intencional o accidental, pérdida de información o pérdida de activos		
Información compartida indebidamente.	Sí ( )	No ( )
Errores u omisiones en sistemas o dispositivos.	Sí ( )	No ( )
Errores en procedimientos o controles.	Sí ( )	No ( )

Cambios indebidos a datos.	Sí ( )	No ( )
Extravío de información o dispositivos.	Sí ( )	No ( )
Otro(s):		

Incidentes por fallas o mal funcionamiento

Dispositivos.	Sí ( )	No ( )
Sistemas.	Sí ( )	No ( )
Comunicaciones.	Sí ( )	No ( )
Servicios.	Sí ( )	No ( )
Equipos de terceros.	Sí ( )	No ( )
Cadena de suministros.	Sí ( )	No ( )
Otro(s):		

Incidentes por la interrupción o falta de insumos

Ausencia de personal.	Sí ( )	No ( )
Huelgas.	Sí ( )	No ( )
Energía.	Sí ( )	No ( )
Agua.	Sí ( )	No ( )
Telecomunicaciones.	Sí ( )	No ( )
Otro(s):		

Incidentes por intercepción de datos

Espionaje.	Sí ( )	No ( )
Mensajes.	Sí ( )	No ( )
Wardriving.	Sí ( )	No ( )
Ataques de hombre en medio.	Sí ( )	No ( )
Secuestro de sesiones.	Sí ( )	No ( )
Sniffers.	Sí ( )	No ( )
Robo de mensajería.	Sí ( )	No ( )
Otro(s):		

	Incidentes por actividad maliciosa con el fin de tomar el control, desestabilizar o dañar un sistema informático		
	Robo de identidad.	Sí ( )	No ( )
	Phishing.	Sí ( )	No ( )
	Denegación de servicios (DOS, DDOS).	Sí ( )	No ( )
	Código malicioso (*malware*, troyanos, gusanos, inyección de código, virus, *ransomware*).	Sí ( )	No ( )
	Ingeniería social.	Sí ( )	No ( )
	Vulneración de certificados (suplantación de sitios, certificados falsos).	Sí ( )	No ( )
	Manipulación de hardware (proxies anónimos, skimmers, *sniffers*).	Sí ( )	No ( )
	Alteración de información (suplantación de direccionamiento y tablas de ruteo, DNS *poisoning*, alteración de configuraciones).	Sí ( )	No ( )
	Abuso de aplicaciones de auditoría.	Sí ( )	No ( )
	Ataques de fuerza bruta.	Sí ( )	No ( )
	Abuso de autorizaciones.	Sí ( )	No ( )
	Crimen organizado.	Sí ( )	No ( )
	Hacktivistas.	Si ( )	No ( )
	Gobierno o grupos afines.	Sí ( )	No ( )
	Terroristas.	Sí ( )	No ( )
	Insiders.	Sí ( )	No ( )
	Otro(s):		
	Incidentes originados por aspectos legales		
	Violación de cláusulas contractuales.	Sí ( )	No ( )
	Violación de acuerdos de confidencialidad.	Sí ( )	No ( )
	Decisiones adversas (resoluciones judiciales en la misma jurisdicción o en otras).	Sí ( )	No ( )
	Otro(s):		
Otros (especificar)			

Clasificación del Incidente de Seguridad de la Información, señalar en la tabla siguiente la clasificación en la que se ubica el incidente mediante los conceptos del catálogo que a continuación se señalan:

Tipo	*Subtipo*	*Subclase de Eventos*	
I. Fraude Interno	1.1 Actividades no autorizadas.	Operaciones no reveladas (intencionalmente). Operaciones no autorizadas (con pérdidas pecuniarias). Valoración errónea de posiciones (intencional).	( ) ( ) ( )
	1.2 Robo y fraude internos.	Fraude / depósitos sin valor. Extorsión / malversación / robo. Apropiación indebida de activos. Destrucción dolosa de activos. Falsificación interna. Contrabando. Apropiación de cuentas, de identidad, entre otros. Incumplimiento/evasión de impuestos (intencional). Cohecho. Abuso de información privilegiada (no a favor de la empresa).	( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( )
	1.3. Seguridad de los sistemas.	Vulneración de sistemas de seguridad. Daños por ataques informáticos. Robo de información (con pérdidas pecuniarias). Utilización inadecuada de claves de acceso y/o niveles de autorización.	( ) ( ) ( ) ( ) ( )
II. Fraude externo	2.1 Hurto y fraude externos.	Robo/estafa/extorsión/cohecho. Falsificación externa/suplantación de personalidad. Uso y/o divulgación de información privilegiada. Espionaje industrial. Contrabando.	( ) ( ) ( ) ( ) ( )
	2.2 Seguridad de los sistemas.	Vulneración de sistemas de seguridad. Daños por ataques informáticos. Robo de información (con pérdidas pecuniarias). Utilización inadecuada de claves de acceso y/o niveles de autorización.	( ) ( ) ( ) ( )

Tipo	*Subtipo*	*Subclase de Eventos*	
VI. Incidencias en el negocio y fallos en los sistemas	6.1 Sistemas	Hardware.	( )
		Software.	( )
		Telecomunicaciones.	( )
		Interrupción/incidencias en el suministro.	( )

ANEXO 4
Informe de Incidentes de Seguridad de la Información

I. Información de la Institución de Fondos de Pago Electrónico.

a) Nombre de la Institución de Fondos de Pago Electrónico.
b) Nombre completo del oficial de seguridad de la información, así como su número de teléfono y dirección de correo electrónico.

II. Información detallada del Incidente de Seguridad de la Información.

a) Anexar, en medio digital Cifrado la siguiente información:

- Descripción del Incidente de Seguridad de la Información.
- Números de Cuenta afectadas.
- Estado de las Cuentas afectadas (bloqueada, suspendida, activa).
- Zona de red afectada (internet, red interna, red de administración, entre otras).
- Tipo de sistema afectado (servidor de archivos, servidor web, servicio de correo, base de datos, estaciones de trabajo, ya sea de escritorio o móvil, entre otros).
- Sistema operativo (especificar versión).
- Protocolos o servicios de los componentes impactados.
- Número de componentes de los sistemas de la Institución de Fondos de Pago Electrónico afectados.
- Aplicaciones involucradas (especificar versión).
- Información del dispositivo comprometido, en su caso (marca, versión de software, firmware, entre otros).
- Impacto al servicio (considerando cualquier disrupción) ocasionado por el Incidente de Seguridad de la Información.
- Monto de la pérdida en pesos, en su caso.
- Monto recuperado en pesos, en su caso.
- Estado del Incidente de Seguridad de la información (Resuelto o No resuelto).
- Señalar si el Incidente de Seguridad de la información se ha dado a conocer a alguna autoridad. En caso afirmativo, indicar la autoridad y la fecha.
- Direcciones IP públicas, direcciones de correo electrónico o dominios de donde proviene el ataque.
- El protocolo de comunicación utilizado, en su caso.
- La URL en caso de sitios web involucrados.
- El *malware* o firma detectada.

- Detallar las acciones que se realizaron para mitigar el Incidente de Seguridad de la Información, mencionando las personas responsables de implementar dichas acciones de mitigación.
- Descripción de los resultados de las acciones de mitigación.
- Tiempos de recuperación del incidente.
- Acciones para minimizar el daño en situaciones similares subsecuentes.
- Otra información que considere que deba ser de conocimiento de la CNBV.
- Acciones de comunicación con Clientes para informarles del incidente.

ANEXO 5
Reporte en materia de contingencias operativas

I. Información de la Institución.

- Nombre de la Institución de Fondos de Pago Electrónico.
- Autor del reporte.
- Puesto/área.
- Correo electrónico.
- Teléfono.

II. Información detallada de la Contingencia Operativa.

Descripción de la Contingencia Operativa

a)	Fecha y hora en que ocurrió.		
b)	Fecha y hora en que se detectó.		
c)	Duración de la contingencia operativa.		
d)	Ubicación(es) de la instalación(es) afectada(s) (centro de datos, oficinas).		
e)	Fallas o mal funcionamiento en la Infraestructura Tecnológica que soporta los servicios.	Sí ( )	No ( )
g)	Afectación en los componentes críticos de la Infraestructura Tecnológica que haya tenido como consecuencia la activación total o parcial del Plan de Continuidad de Negocio.	Sí ( )	No ( )
h)	Indicar si el evento se originó de un incidente de ciberseguridad.	Sí ( )	No ( )
i)	Señale el Impacto de los eventos (según la "Escala de Impacto"):	Muy Alto Alto Medio Bajo	
j)	¿La Infraestructura Tecnológica involucrada en la contingencia operativa es administrada por terceros?	Sí ( )	No ( )
k)	En caso de ser afirmativo el inciso j), detallar datos del proveedor y servicios proporcionados		

III. Clasificar la contingencia operativa reportada con base en las siguientes causas que provocaron las contingencias operativas:

Fallas en la Infraestructura Tecnológica que soporta los servicios o Afectación en los componentes críticos de la Infraestructura Tecnológica que haya tenido como consecuencia la activación total o parcial del Plan de Continuidad de Negocio

Fallas o mal funcionamiento		
Dispositivos	Sí ( )	No ( )
Sistemas	Sí ( )	No ( )
Telecomunicaciones	Sí ( )	No ( )
Servicios	Sí ( )	No ( )
Bases de Datos	Sí ( )	No ( )
Equipos de terceros	Sí ( )	No ( )
Otros (especificar):		
Daño no intencional o accidental		
Errores en procedimientos o controles	Sí ( )	No ( )
Mencione los procedimientos o controles		
Cambios indebidos a datos	Sí ( )	No ( )
Otro(s):		
Incidente de ciberseguridad		
Dispositivos	Sí ( )	No ( )
Sistemas	Sí ( )	No ( )
Telecomunicaciones	Sí ( )	No ( )
Servicios	Sí ( )	No ( )
Bases de Datos	Sí ( )	No ( )
Equipos de terceros	Sí ( )	No ( )
Otros (especificar)		

	Afectación por escenarios diferentes a afectaciones en la Infraestructura Tecnológica Interrupción o falta de insumos		
	Manifestaciones	Sí ( )	No ( )
	Huelgas	Sí ( )	No ( )
	Energía	Sí ( )	No ( )
	Agua	Sí ( )	No ( )
Otros (especificar):			
	Desastres naturales o ambientales		
	Terremotos	Sí ( )	No ( )
	Inundaciones	Sí ( )	No ( )
	Huracanes	Sí ( )	No ( )
	Incendios	Sí ( )	No ( )
	Otros (especificar):		
	Cuantificación provocada por la contingencia operativa		
	¿La contingencia operativa ocasionó una pérdida monetaria para los Clientes o para la propia institución?	Sí ( )	No ( )
	Pérdida monetaria	$	
	Número de Clientes afectados		

IV. Informe de la descripción de la contingencia operativa reportada.

a)	Descripción detallada de las causas y diagnóstico de la contingencia operativa (Señalar causa raíz y cómo fue determinada).
b)	Acciones implementadas para solventar los problemas presentados (acciones correctivas) (Señale cronología y descripción de lo realizado).
c)	Indicar los controles que fallaron.

d)	¿Qué acciones preventivas y correctivas se llevarán a cabo para mitigar el riesgo de ocurrencia de una situación similar?
e)	Plan de trabajo para la atención de acciones correctivas que al efecto se elaboró, el cual deberá contener al menos el personal responsable de su diseño, implementación, ejecución y seguimiento, plazos para su ejecución, detalle de las actividades realizadas y por realizar, así como los recursos técnicos, materiales y humanos empleados.
f)	Información adicional (indique todo aquello que considere útil para complementar este informe).

En la fracción III del presente Anexo, deberán describirse las razones que lo motivaron a clasificar el incidente teniendo como base la siguiente "Escala de Impacto":

- "Crítico" (P. ej. interrupción de procesos esenciales del negocio que afectan otros recursos).
- "Alto" (P. ej. interrupción de procesos primarios del negocio).
- "Medio" (P. ej. es posible continuar trabajando usando una solución alterna).
- "Bajo" (P. ej. interrupción de procesos secundarias del negocio).

ANEXO 6
Características de terceros independientes

A. Requisitos de independencia.

Se considerará que no existe independencia cuando el Tercero Independiente o la persona moral por medio de la cual preste sus servicios se ubiquen en alguno de los supuestos siguientes:

I El Tercero Independiente o la persona moral por medio de la cual preste sus servicios ejerza el Control sobre la Institución de Fondos de Pago Electrónico, o sea, su subsidiaria, su asociada, una entidad con la que realiza acuerdos con control conjunto o una persona moral que pertenezca al mismo Grupo Empresarial o Consorcio que la Institución de Fondos de Pago Electrónico.

Los ingresos que perciba el Tercero Independiente o la persona moral por medio de la cual preste sus servicios, provenientes de la Institución de Fondos de Pago Electrónico o, en su caso, de su controladora, subsidiarias, asociadas, entidades con las que realicen acuerdos con control conjunto o las personas morales que pertenezcan al mismo Grupo Empresarial o Consorcio derivados de la prestación de sus servicios, representen en su conjunto 10 por ciento o más de los ingresos totales de dicha persona moral o Tercero Independiente durante el año inmediato anterior a aquél en el que pretenda prestar el servicio.

II. El Tercero Independiente o la persona moral por medio de la cual preste sus servicios, haya sido Cliente o proveedor importante de la Institución de Fondos de Pago Electrónico o, en su caso, de su controladora, subsidiarias, asociadas, entidades con las que realicen acuerdos con control conjunto o personas morales que pertenezcan al

mismo Grupo Empresarial o Consorcio, durante el año inmediato anterior a aquél en el que pretenda prestar el servicio.

Se considera que un Cliente o proveedor es importante cuando sus ventas o compras a la Institución de Fondos de Pago Electrónico o, en su caso, a su controladora, subsidiarias, asociadas, entidades con las que realicen acuerdos con control conjunto o personas morales que pertenezcan al mismo Grupo Empresarial o Consorcio, representen en su conjunto 10 por ciento o más de sus ventas totales o, en su caso, compras totales.

III. El Tercero Independiente o algún socio de la persona moral por medio de la cual preste sus servicios, sean o hayan sido durante el año inmediato anterior a su contratación, consejero, director general o empleado que ocupe un cargo dentro de los dos niveles inmediatos inferiores a este último en la Institución de Fondos de Pago Electrónico, en su controladora, subsidiarias, asociadas, entidades con las que realicen acuerdos con control conjunto o personas morales que pertenezcan al mismo Grupo Empresarial o Consorcio.

IV. En caso de que el Tercero Independiente o algún socio de la persona moral por medio de la cual se presten los servicios, el cónyuge, concubina, concubinario o dependiente económico de las personas físicas anteriores, tengan inversiones en acciones o títulos de deuda emitidos por la Institución de Fondos de Pago Electrónico o, en su caso, por su controladora, subsidiarias, asociadas, entidades con las que realicen acuerdos con control conjunto o personas morales que pertenezcan al mismo Grupo Empresarial o Consorcio, tengan títulos de crédito que representen dichos valores o derivados que los tengan como subyacente, salvo que se trate de depósitos a plazo fijo, incluidos certificados de depósito retirables en días preestablecidos, aceptaciones bancarias o pagarés con rendimiento liquidable al vencimiento, siempre y cuando éstos sean contratados en condiciones de mercado.

Lo previsto en esta fracción no resultará aplicable a:

a) La tenencia en acciones representativas del capital social de fondos de inversión de renta variable y en instrumentos de deuda.
b) La tenencia en acciones representativas del capital social de una sociedad anónima, inscritas en el Registro Nacional de Valores a cargo de la CNBV, a través de fideicomisos constituidos para ese único fin en los que no intervengan en las decisiones de inversión o bien en títulos referidos a índices o canastas de acciones o en títulos de crédito que representen acciones del capital social de dos o más sociedades anónimas emitidos al amparo de fideicomisos.

V. El Tercero Independiente o algún socio de la persona moral por medio de la cual se presten los servicios, el cónyuge, concubina, concubinario o dependiente económico de las personas físicas anteriores, mantengan con la Institución de Fondos de Pago Electrónico o, en su caso, con su controladora, subsidiarias, asociadas, entidades con las que realicen acuerdos con control conjunto o personas mo-

rales que pertenezcan al mismo Grupo Empresarial o Consorcio, deudas por préstamos o créditos de cualquier naturaleza, salvo que se trate de adeudos por tarjeta de crédito, por financiamientos destinados a la compra de bienes de consumo duradero por créditos hipotecarios para adquisición de inmuebles y por créditos personales y de nómina, siempre y cuando sean otorgados en condiciones de mercado.

VI. En caso de que la controladora, subsidiarias, asociadas, entidades con las que realicen acuerdos con control conjunto o personas morales que pertenezcan al mismo Grupo Empresarial o Consorcio que la Institución de Fondos de Pago Electrónico tengan inversiones en la persona moral en la cual preste sus servicios o sea socio el Tercero Independiente que realiza la auditoría.

VII. En caso de que el Tercero Independiente o la persona moral por medio de la cual se presten los servicios proporcione a la Institución de Fondos de Pago Electrónico, adicionalmente al de la evaluación de cumplimiento, cualquiera de los servicios siguientes:

- Consultoría sobre la elaboración de los procesos, procedimientos, políticas y criterios, así como los sistemas con que la Institución de Fondos de Pago Electrónico deba contar para dar cumplimiento a los requisitos a que se refieren las presentes Disposiciones.
- Operación, directa o indirecta, de los sistemas de información financiera, o bien, administración de su red local.
- Supervisión, diseño o implementación de los sistemas informáticos (hardware y software) de la Institución de Fondos de Pago Electrónico, que lleven a cabo actividades para las operaciones que la referida institución realice.
- Supervisión, diseño o implementación de políticas y procedimientos para la seguridad de la información, uso de Canales de Instrucción o continuidad operativa.
- Provisión de servicios relacionados con seguridad de la información, uso de medios electrónicos o continuidad operativa.
- Administración de la Institución de Fondos de Pago Electrónico, temporal o permanente, participando en las decisiones.
- Auditoría interna relativa a la evaluación del nivel de cumplimiento de los requerimientos relativos a seguridad de la información, uso de Canales de Instrucción y continuidad operativa.
- Reclutamiento y selección de personal de la Institución de Fondos de Pago Electrónico para que ocupen cargos de director general o de los dos niveles inmediatos inferiores al de este último, y,
- Cualquier otro servicio que implique o pudiera implicar conflictos de interés respecto al trabajo de evaluación del cumplimiento que se realice.

VIII. Los ingresos que el Tercero Independiente, o la persona moral a través de la cual se preste el servicio, perciba o vaya a percibir por llevar a cabo la evaluación de cumplimiento de la Institución de Fondos de Pago Electrónico dependan del resultado de la propia evaluación o del éxito de cualquier

operación realizada por dicha Institución de Fondos de Pago Electrónico que tenga como sustento la evaluación de cumplimiento.

IX. El Tercero Independiente o la persona moral a través de la cual preste el servicio, tengan Cuentas por cobrar vencidas con la Institución de Fondos de Pago Electrónico por honorarios provenientes de algún servicio que ya se haya prestado a la Institución de Fondos de Pago Electrónico, a la fecha de emisión del informe de evaluación.

B. Selección de la persona moral a través de la cual se prestarán servicios de evaluación del cumplimiento.

La Institución de Fondos de Pago Electrónico deberá seleccionar a una persona moral a través de la cual el Tercero Independiente podrá prestar servicios de evaluación del cumplimiento a las normas contenidas en estas Disposiciones, que deberá cumplir con las características definidas en este anexo.

En caso de estimarlo conveniente, la Institución de Fondos de Pago Electrónico podrá seleccionar personas morales distintas para evaluar el cumplimiento de los requisitos relativos a la seguridad de la información, uso de Canales de Instrucción y a la continuidad operativa.

En caso de que, como resultado de la evaluación de los requisitos de seguridad informática y de continuidad operativa, se identifique que uno o varios puntos se cumplen parcialmente o no se cumplen, cualquier futura evaluación, y en tanto las observaciones no se solventen plenamente, deberá realizarse por la misma persona moral que realizó la primera evaluación.

Únicamente cuando por causas de fuerza mayor no le sea posible a la Institución de Fondos de Pago Electrónico seleccionar a la misma persona moral, ésta podrá seleccionar a una persona moral distinta, para lo cual deberá justificar plenamente sus razones por escrito ante el Banco de México y la CNBV.

C. Contrato de prestación de servicios suscrito entre la Institución de Fondos de Pago Electrónico y la persona moral a través de la cual se prestarán servicios de evaluación del cumplimiento.

La Institución de Fondos de Pago Electrónico deberá establecer un contrato de prestación de servicios con la persona moral en el que definan los términos en los que esta última realizará la evaluación, así como el periodo que comprenderán las actividades. Dicho contrato deberá establecer los siguientes aspectos:

- Que los Terceros Independientes asignados al proyecto cumplan con las características señaladas en este Anexo, así como lo previsto en las presentes Disposiciones.
- Que la entrega de la información entre la Institución de Fondos de Pago Electrónico y la persona moral se realizará en los términos especificados en el presente Anexo.
- Que la información proporcionada por la Institución de Fondos de Pago Electrónico, así como los resultados de la evaluación de cumplimiento, podrá ser requerida directamente a la persona moral por el Banco de México o la CNBV.
- Que la persona moral y los Terceros Independientes se comprometen a:
- Mantener confidencialidad sobre las evidencias recabadas y sobre los resultados obtenidos de la evaluación a la Institución de Fondos de Pago Electrónico sobre el cumplimiento de los requisitos de seguridad informática y de continuidad operativa.

- Mantener confidencialidad sobre los requisitos de seguridad informática y de continuidad operativa.
- Resguardar la información que se produzca como parte de la evaluación en medios restringidos de acceso, que aseguren la integridad y confidencialidad de la misma.

D. Evaluación de cumplimiento de los requisitos relativos a la seguridad de la información, Canales de Instrucción y continuidad operativa.

La evaluación del cumplimiento comprende dos tipos de revisiones:

- Extra-situ – Dictaminación de evidencias documentales que provean las Instituciones de Fondos de Pago Electrónico.
- In-situ – Verificación del cumplimiento de los requisitos mediante visitas a las instalaciones de la Institución de Fondos de Pago Electrónico, basada en las evidencias provistas por ésta.

E. Características de la persona moral y Tercero Independiente a través de la cual se prestarán servicios de evaluación del cumplimiento.

Los Terceros Independientes deberán cumplir con las siguientes características:

I. En materia de seguridad de la información:

a) Contar al menos con alguna de las siguientes certificaciones: CISSP (*Certified Information System Security Professional*), CISA (*Certified Information Systems Auditor*) o CISM (*Certified Information Security Manager*), o sus equivalentes o las que las sustituyan. El Banco de México y la CNBV podrán divulgar en su página de internet las certificaciones que sean equivalentes o las que sustituyan a las mencionadas en este inciso.

b) Demostrar experiencia en consultoría en seguridad de la información en el sector financiero de por lo menos dos años.

c) Haber participado en actividades o proyectos relacionados con seguridad de la información en los últimos 24 meses.

II. En materia de continuidad operativa:

Contar con al menos dos de las siguientes certificaciones: ISO 31000, ISO 22301, Basilea II y COSO II, o sus equivalentes o las que las sustituyan. El Banco de México y la CNBV podrán divulgar en su página de internet las certificaciones que sean equivalentes o las que sustituyan a las mencionadas en este inciso.

Demostrar experiencia en auditoría de gestión de continuidad de negocio en el sector financiero de por lo menos 2 años.

La persona moral a través de la cual el Tercero Independiente podrá prestar servicios de evaluación del cumplimiento a las normas contenidas en estas Disposiciones, deberá cumplir con las siguientes características:

I. No deberá estar inhabilitada para celebrar contrato alguno con la Administración Pública Federal, de servicios profesionales relacionados con tecnologías de la información, riesgo operacional, continuidad operativa y prevención de lavado de dinero.

II. En materia de seguridad de la información, deberá cumplir con lo siguiente:

a) Experiencia en consultoría en seguridad de la información en el sector financiero de por lo menos cinco años cuando se trate de Instituciones de Fondos de Pago Electrónico consideradas como relevantes, de conformidad con el artículo 49 de las presentes disposiciones.

Tratándose de Instituciones de Fondos de Pago Electrónico que no se consideren dentro del supuesto antes mencionado, el tercero indepen-diete deberá tener al menos dos años de experiencia en materia de seguridad de la información en el sector financiero o al menos tres años en dicha materia, pero no específicamente en el sector financiero.

b) Perfil orientado a auditoría en seguridad de la información.

III. En materia de continuidad operativa, deberá cumplir con lo siguiente:

a) Experiencia en consultoría en gestión del riesgo en el sector financiero de por lo menos cinco años cuando se trate de Instituciones de Fondos de Pago Electrónico consideradas como relevantes de conformidad con el artículo 49 de las presentes disposiciones.

Tratándose de Instituciones de Fondos de Pago Electrónico que no se consideren dentro del supuesto antes mencionado, el tercero indepen-diete deberá tener al menos dos años de experiencia en materia de seguridad de la información en el sector financiero o al menos tres años en dicha materia, pero no específicamente en el sector financiero.

b) Perfil orientado a auditoría en continuidad de negocio.

IV. Los Terceros Independientes que presten sus servicios a través de la mencionada persona moral no deberán ser subcontratados.

ANEXO 7
Requerimientos técnicos para realizar operaciones a través de comisionistas

La infraestructura tecnológica que utilicen los comisionistas o el Administrador de comisionistas para garantizar la correcta ejecución de las Operaciones y la seguridad de la información de los Clientes, deberá cumplir con los requerimientos a que se refiere el presente anexo.

I. Definiciones. Para efectos del presente anexo, se entenderá por: Identificador Individual, a la cadena de caracteres asignada a cada operador en lo individual.

II. Descripción de las características técnicas de los sistemas, equipos y aplicaciones que el comisionista o el Administrador de comisionistas utilizarán para realizar las Operaciones, desde su inicio hasta la afectación de las respectivas cuentas de la Institución de Fondos de Pago Electrónico, considerando a todos los participantes involucrados.

La referida descripción deberá señalar, al menos, lo siguiente:

a) Descripción de los enlaces de comunicación utilizados por la Institución de Fondos de Pago Electrónico para conectarse con el comisionista que incluya, al menos, el nombre del comisionista, el ancho de banda y el tipo de Operación realizada.

b) Diagrama de telecomunicaciones en donde se muestre la conexión existente entre cada uno de los participantes en la operación del comisionista (prestadores de servicios, centros de datos, Institución de Fondos de Pago Electrónico, entre otros), incluyendo los esquemas de redundancia.
c) En su caso, esquema de interrelación de aplicaciones o sistemas del comisionista o del Administrador de comisionistas, incluyendo los sistemas propios de la Institución de Fondos de Pago Electrónico.
d) Documentación en donde se expongan los mecanismos para asegurar la transmisión de la información en forma cifrada de punto a punto, incluyendo la versión de los protocolos de Cifrado y componentes de seguridad de la Infraestructura Tecnológica implementados en cada uno de los nodos involucrados en el envío y recepción de datos.
e) Detalle del tipo de información de la Institución de Fondos de Pago Electrónico, de sus Clientes o de los usuarios de medios de disposición, precisando, en su caso, el tipo de Información Sensible que será almacenada por el comisionista o el Administrador de comisionistas en sus equipos o instalaciones, o a la que podrán tener acceso. Trátandose de Información Sensible, el comisionistas o Administrador de Comisionistas deberá implementar mecanismos de cifrado.
f) Procedimiento de validación y pruebas a la instalación de la infraestructura tecnológica del comisionista.
g) Criterios relativos a la composición de las contraseñas o claves de acceso de los operadores y de los factores de autenticación a Clientes o usuarios del medio de disposición, incluyendo números de identificación personal (NIP).

III. Requerimientos de la infraestructura tecnológica del comisionista o Administrador de comisionistas.

1. Mecanismos necesarios para realizar las transacciones en línea.

La infraestructura tecnológica del comisionista deberá contar con los mecanismos necesarios para realizar las transacciones en línea tratándose de Operaciones de recepción o retiro de efectivo, es decir, al instante mismo en que se lleve a cabo la Operación, actualizando los saldos del Cliente en línea en apego a lo establecido por las reglas de operación de las propias Instituciones de Fondos de Pago Electrónico.

2. Validación de la infraestructura tecnológica del comisionista.

Únicamente la infraestructura tecnológica de los comisionistas autorizados por la Institución de Fondos de Pago Electrónico tendrá acceso a la Infraestructura Tecnológica dispuesta por aquélla (uso de líneas dedicadas, identificación de direcciones físicas o lógicas, VPN, firmas digitales, entre otros).

Asimismo, la Institución de Fondos de Pago Electrónico deberá obtener evidencia de que la infraestructra tecnológica utilizada por los comisionistas mantienen mecanismos de con-

trol que eviten la lectura y extracción de la información de los Clientes por terceros no autorizados.

3. Políticas y procedimientos para la administración de accesos y configuración de la infraestructura tecnológica del comisionista.

   Es responsabilidad de la Institución de Fondos de Pago Electrónico contar con políticas y procedimientos del comisionista o Administrador de comisionista para:

   a) La configuración de la infraestructura tecnológica que se conecte a los sistemas informáticos de la Institución de Fondos de Pago Electrónico.
   b) La administración de llaves criptográficas utilizadas entre los comisionistas y los sistemas de la Institución de Fondos de Pago Electrónico.

4. Generación de registros electrónicos de Operaciones.

   Todas las Operaciones realizadas a través de los comisionistas deberán generar registros electrónicos que no puedan ser modificados o borrados y en los que deberá incluirse al menos la fecha, hora y minuto en que fueron realizadas, el tipo y monto de la instrucción; en su caso, el número de cuenta del Cliente, medio a través del cual se ejecutó la instrucción, así como la información suficiente que permita la identificación del personal que realizó la instrucción. La custodia de dichos registros deberá estar a cargo de la Institución de Fondos de Pago Electrónico.

IV. Requerimientos de identificación de operadores y autenticación de Clientes.

1. Mecanismos necesarios para la plena identificación de los comisionistas.
2. Las Instituciones de Fondos de Pago Electrónico, en la realización de Operaciones a través del comisionista, deberán contar con mecanismos que les permitan identificar a los operadores, a fin de contar con la información necesaria para la resolución de aclaraciones o disputas. Dichos mecanismos deberán señalarse en el plan general de funcionamiento a que se refiere la fracción I del artículo 47 de las presentes disposiciones.

   Generación y entrega de contraseñas o claves de acceso de los operadores.
3. Las Instituciones de Fondos de Pago Electrónico deberán establecer mecanismos para el proceso de generación y entrega de los factores de autenticación que aseguren que sólo el Comisionista o, en su caso, sus operadores, podrán conocer.
4. Composición de contraseñas o claves de acceso de los operadores.

   Deberán establecerse criterios para las características de la longitud de las contraseñas o claves de acceso de los operadores.
5. Protección de contraseñas o claves de acceso de los operadores y Números de Identificación Personal (NIP) de los Clientes.

   Las Instituciones de Fondos de Pago Electrónico deberán prever lo necesario para evitar la lectura de los caracteres que componen las contraseñas o claves de acceso de los operadores, así como los Números de Identificación Personal (NIP) digitados por los Clientes, respectivamente, en

la infraestructura tecnológica del comisionista, tanto en su captura como en su despliegue a través de pantallas.

Las contraseñas o claves de acceso de los operadores y los Números de Identificación Personal (NIP) de los Clientes deberán validarse y almacenarse a través de mecanismos de encriptación. En ningún momento, los comisionistas podrán tener acceso a los datos relacionados con dichos Números de Identificación Personal (NIP) de los Clientes.

6. Autenticación con dos factores para Clientes.

Para la realización a través de los comisionistas de consultas y Operaciones que representen un cargo a la cuenta de los Clientes, estos últimos deberán autenticarse a través de la infraestructura tecnológica del comisionista con la que se realicen las mencionadas Operaciones utilizando dos factores de autenticación diferentes.

Para efectos de lo anterior, las Instituciones de Fondos de Pago Electrónico podrán optar por la combinación de al menos dos de los siguientes factores de autenticación y ajustarse a lo dispuesto en el artículo 5° de las presentes disposiciones.

7. Para la recepción y operación de transacciones solicitadas por los Clientes a través de la infraestructura tecnológica de los comisionistas, los operadores deberán iniciar una sesión y autenticarse a través de dicha infraestructura.

Los procesos de autenticación deberán ser validados por la Institución de Fondos de Pago Electrónico, a través de los mecanismos y controles que ésta estime conveniente. Será responsabilidad de la Institución de Fondos de Pago Electrónico asegurarse de que los comisionistas cuenten con dichos mecanismos de autenticación de operadores, para la realización de las operaciones.

V. Operación de la infraestructura tecnológica del comisionita.

1. Generación de comprobantes de Operación.

La infraestructura tecnológica del comisionista deberá generar automáticamente los comprobantes de Operación que emitan las Instituciones de Fondos de Pago Electrónico para cada Operación, sin mediar intervención alguna por parte del personal del comisionista. Dichos comprobantes de Operación serán diferentes a aquellos que utilicen los comisionistas para registrar las operaciones propias de su giro comercial.

Cuando se alcancen los límites de operación a que se refiere el artículo 48, según corresponda, no podrán llevarse a cabo las Operaciones solicitadas, por lo que la infraestructura tecnológica del comisionista deberá generar comprobantes que indiquen al Cliente dicha situación. Para tales efectos, deberá proporcionarse un comprobante que incluya la leyenda siguiente:

"Transacción no realizada por haber excedido su límite permitido. Pónganse en contacto con su Institución de Fondos de Pago Electrónico".

Las Instituciones de Fondos de Pago Electrónico deberán adjuntar el diseño del comprobante de cada una de las Operaciones por contratar.

Por ningún motivo deberá mostrarse en el comprobante de operación el domicilio del Cliente.

2. Monitoreo de Operaciones.

La Institución de Fondos de Pago Electrónico deberá establecer mecanismos que le permitan monitorear las actividades realizadas por los operadores, a través de la infraestructura tecnológica de los comisionistas con el fin de detectar transacciones que se alejen de los parámetros habituales de Operación.

3. Almacenamiento de información del Cliente en la infraestructura tecnológica del comisionista.

Los comisionistas no podrán almacenar, conservar o copiar, en su infraestructura tecnológica, información del Cliente de la Institución de Fondos de Pago Electrónico. En los casos en que por razones operativas y técnicas se requiera almacenar parcial o totalmente dicha información en su infraestructura tecnológica, ésta deberá tener mecanismos de encriptación.

Corresponderá a las Instituciones de Fondos de Pago Electrónico verificar el cumplimiento del presente numeral.

ANEXO 8
Formato de Información de Sistemas y Aplicativos (F-SA)

Instrucciones: Los numerales 1 a 11 deben ser eliminados de cada título de las columnas de la tabla una vez documentado el formato, así como las instrucciones que aparecen en el pie de la tabla, y los ejemplos contenidos en la misma.

Nombre de la aplicación o sistema[1]	*Proceso(s) de negocio relacionado(s) con el sistema*[2]	*Nombre del equipo en donde se procesa*[3]		*Lenguaje*[4]	*Plataforma (marca y modelo del equipo de cómputo principal del aplicativo o sistema)*[5]	*Sistema operativo*[6]	
		Físico	*Virtual*			*Físico*	*Virtual*
Ejemplo 1: Nombre de sistema	<Captación, Colocación, Ventanilla, etcétera >	<SRVCORE1>	<SOCPROD2>	<JAVA 1.1>	<IBM i 7.2>	<UNIX>	<Windows Server 2018>
			<SOCPROD3>				<Windows Server 2012>
Ejemplo 2: Nombre de sistema	<Captación, colocación, ventanilla, etcétera >		<SOCPROD2>	<RPG II>		<Fedora>	
			<SOCPROD3>			<Windows Server 2012>	
<…>	<…>	<…>	<…>	<…>	<…>	<…>	<…>

	Base de datos[7]	*Servicios en nube*[8]	*Proveedor del aplicativo / Desarrollo propio*[9]	*Lugar de procesamiento (Sitio Principal / Alterno)*[10]		*Lugar de operación (Sitio Principal / Alterno)*[11]	
				Propio / Terceros[(a)]	*Ubicación*[(b)]	*Nacional / Extranjero*	*Ubicación*
	<Oracle>	<NA>	<Proveedor4, S.A de C.V. >	<Terceros>	<Centro de cómputo principal Triara, S.A. de C.V. Ciudad de México Col. Del Valle, CP 03100> < Centro de cómputo alterno Ciudad de México Alfonso Nápoles Gándara 50, Col. Peña Blanca Santa Fe, CP 01210 >	<Nacional>	<Corporativo>
						<Extranjero>	<Oficina principal Bournemounth, Reino Unido> <Oficina alterno Bournemounth, Reino Unido>
	<DB2>	<SaaS>	<Proveedor1, S.A de C.V. >	<Terceros>	<Zona Norte de Estados Unidos de Norte América del Norte>	<Nacional>	< Centro de cómputo alterno Ciudad de México Alfonso Nápoles Gándara 50, Planta Baja Col. Peña Blanca Santa Fe, CP 01210 >
							<Corporativo >
	<…>	<…>	<…>	<…>	<…>	<…>	<…>

1. *Nombre de la aplicación o sistema: capturar el nombre con el que se identifique la aplicación o el sistema en el interior de la Entidad o de forma comercial.*
2. *Proceso(s) de negocio relacionado(s) con el sistema: describir el(los) proceso(s) de negocio que soporta el sistema.*
3. *Nombre del equipo en donde se procesa: capturar el nombre con el que se identifique el servidor físico y virtual en el interior de la Entidad.*
4. *Lenguaje: indicar el(los) lenguaje(s) de programación del sistema, incluyendo su versión.*
5. *Plataforma (marca y modelo del equipo de cómputo principal del aplicativo o sistema): capturar la marca y el modelo del servidor físico (equipo principal) donde se procesa el sistema.*
6. *Sistema operativo: capturar el nombre y versión del sistema operativo del equipo físico y virtual en donde se procesa el sistema y/o reside la máquina virtual.*
7. *Base de datos: base de datos en donde se almacena la información procesada por el aplicativo.*
8. *Servicios en nube: incluir, en caso de aplicar, el tipo de servicio contratado en el esquema de nube: N/A (No aplica), SaaS (Software as a Service), IaaS (Infrastructure as a Service).*
9. *Proveedor del aplicativo/Desarrollo propio: en caso de ser un desarrollo interno indicar: "Desarrollo propio"; en caso de ser un desarrollo externo, incluir la razón social del proveedor del sistema.*
10. *Lugar de procesamiento (Sitio Principal/Alterno):*

    a) Indicar "Propio" si el centro de cómputo es de la Entidad; en caso contrario se debe indicar la razón social del proveedor del Centro de Cómputo principal.
    b) Especificar el nombre del centro de cómputo como se conoce en el interior de la Entidad o de forma comercial; asimismo, debe especificarse la dirección completa en donde se encuentra el centro de cómputo principal y alterno (calle, número, colonia, delegación o municipio, estado, código postal) cuando sea nacional. En caso de direcciones en el extranjero, deberá precisar la información equivalente a la antes señalada.

11. *Lugar de operación (Sitio Principal/Alterno): indicar si se encuentran en territorio nacional o extranjero (columna Nacional/Extranjero) y especificar la dirección completa en donde se encuentra el personal que tiene acceso y opera el sistema en cuestión (columna Ubicación).*

Anexo 3

Disposiciones de carácter general para regular las Instituciones de Tecnología Financiera, aplicables a las Sociedades de Información Crediticia y Cámaras de Compensación en materia de interfaces de programación de aplicaciones informáticas estandarizadas

CAPÍTULO I
DISPOSICIONES PRELIMINARES

Artículo 1. Definiciones. Además de los términos utilizados en la Ley bajo las definiciones incluidas en dicho ordenamiento, ya sea en singular o plural, en las presentes Disposiciones se entenderá por:

API:	A las interfaces de programación de aplicaciones informáticas estandarizadas a que se refiere el artículo 76 de la Ley.
Certificado Digital Banco de México:	A aquel mensaje de datos en formato digital generado en términos de las "Reglas para Operar como Agencia Registradora y/o Agencia Certificadora en la Infraestructura Extendida de Seguridad" contenidas en la Circular-Telefax 6/2005 expedida por el Banco de México o las que, en su caso, las sustituyan.
Contratos de Interconexión:	A los contratos para la conectividad y acceso de los aplicativos desarrollados o administrados por Entidades Reconocidas a las API establecidas por las cámaras de compensación y SIC, con el fin de compartir datos e información.
Datos Agregados:	A aquellos a que se refiere el artículo 76, fracción II, de la Ley.
Datos Financieros Abiertos:	A aquellos a que se refiere el artículo 76, fracción I, de la Ley.
Datos Transaccionales:	A aquellos a que se refiere el artículo 76, fracción III, de la Ley.
Día Hábil Bancario:	A los días en que las instituciones de crédito no estén obligadas a cerrar sus puertas ni a suspender operaciones, en términos de las disposiciones de carácter general que, para tal efecto, emita la CNBV.
Entidades Reconocidas:	A las Entidades Financieras, los transmisores de dinero, las ITF, las sociedades autorizadas para operar con Modelos Novedosos y los Terceros Especializados, además de las cámaras de compensación y SIC, que, conforme al artículo 76 de la Ley, pueden establecer, por medio de las API que desarrollen, la conectividad a aquellas otras API que establezcan las cámaras de compensación y SIC conforme a ese mismo artículo y las presentes Disposiciones, con el fin de acceder a los datos e información previstos en dicho precepto legal.

Infraestructura Tecnológica:	A la infraestructura de cómputo, telecomunicaciones, software, aplicaciones informáticas y demás herramientas que sean utilizadas por las cámaras de compensación y SIC para establecer y operar las API.
Ley:	A la Ley para Regular las Instituciones de Tecnología Financiera.
Plan de Trabajo:	Al conjunto de documentos e información que las cámaras de compensación y SIC deberán presentar al Banco de México en términos de lo establecido en el Anexo 2 de las presentes Disposiciones.
SIC:	A las personas morales autorizadas para actuar como sociedades de información crediticia en términos de lo previsto en la Ley para Regular las Sociedades de Información Crediticia.
Terceros Especializados:	A los terceros especializados en tecnologías de la información referidos en el artículo 76 de la Ley.

Artículo 2. Establecimiento de las API. Las cámaras de compensación a que se refiere la Ley para la Transparencia y Ordenamiento de los Servicios Financieros y las SIC deberán sujetar a las presentes Disposiciones el intercambio de datos e información señalados en el artículo 76 de la Ley, que podrán compartir mediante las API que están obligadas a establecer y mantener de conformidad con dicho artículo. Por su parte, las Entidades Reconocidas que deseen tener acceso, por medio de las API que desarrollen para ello, a los datos e información que las cámaras de compensación y SIC deben compartirles conforme al citado artículo 76 deberán sujetarse a lo establecido al efecto en las presentes Disposiciones.

Artículo 3. Estándares para la interoperabilidad de las API. En las API que establezcan las cámaras de compensación y SIC, estas deberán cumplir con los estándares de interoperabilidad establecidos en el **Anexo 1** de las presentes Disposiciones. Asimismo, las cámaras de compensación y SIC deberán poner a disposición de las Entidades Reconocidas la información técnica para la interoperabilidad de las API.

CAPÍTULO II
AUTORIZACIONES

Artículo 4. Autorización para el establecimiento de las API para Datos Agregados y, en su caso, Datos Financieros Abiertos. Las cámaras de compensación y SIC deberán obtener la previa autorización del Banco de México para establecer las API a que se refiere el artículo 76 de la Ley.

Para tales efectos, cada cámara de compensación y SIC deberá presentar una solicitud de autorización ante la Dirección de Autorizaciones y Sanciones de Banca Central del Banco de México en términos del **artículo 20** de estas Disposiciones. La referida solicitud deberá contener evidencia que acredite el cumplimiento de lo establecido en el **Anexo 1** de las presentes Disposiciones, así como un Plan de Trabajo que incluya, al menos, los elementos indicados en el **Anexo 2** de estas Disposiciones, y un modelo de clausulado de los Contratos de Interconexión que la cámara de compensación o SIC respectiva pretende celebrar con las Entidades Reconocidas que correspondan.

En la solicitud anteriormente señalada, la cámara de compensación o SIC respectiva

deberá especificar los datos e información previstos en las fracciones I y II del artículo 76 de la Ley que podrá compartir a través de las API correspondientes, conforme a lo siguiente:

I. Tratándose de los Datos Financieros Abiertos, mientras las cámaras de compensación no estén facultadas para ofrecer productos y servicios directamente al público en general y estas o las SIC no cuenten con sucursales u otros puntos de acceso para ofrecer dichos productos, no estarán obligadas a poner a disposición, por medio de sus API, los Datos Financieros Abiertos respectivos. Sin perjuicio de lo anterior, únicamente en la medida en que la cámara de compensación de que se trate obtenga autorización para ofrecer productos y servicios al público en general, adicionalmente a aquellos que estén facultadas a ofrecer a las entidades determinadas en las disposiciones legales aplicables o bien, cuente con sucursales u otros puntos de acceso para ofrecer dichos productos y servicios o se trate de una SIC que obtenga autorización para prestar servicios adicionales a los que puede prestar conforme a lo previsto en el artículo 5 de la Ley para Regular las Sociedades de Información Crediticia o cuente con sucursales, la cámara de compensación o SIC especificará dicha información con el fin de que sea compartida por medio de la API que corresponda.

II. Tratándose de Datos Agregados, cada cámara de compensación y SIC deberá especificar la información estadística relacionada con aquellas operaciones realizadas por o a través de la propia entidad, susceptible de ser objeto de intercambio por medio de la API que establezca conforme a las presentes Disposiciones.

El Banco de México especificará en la autorización respectiva las categorías de datos y la información que la cámara de compensación o SIC de que se trate podrá compartir a través de la API que establezca.

Artículo 5. Autorización para compartir Datos Transaccionales. Por lo que respecta a los Datos Transaccionales previstos en la fracción III del artículo 76 de la Ley, una vez que la cámara de compensación o SIC de que se trate haya obtenido autorización del Banco de México para intercambiar los Datos Agregados y, en su caso, los Datos Financieros Abiertos conforme al artículo anterior, esta deberá presentar una solicitud de autorización adicional para intercambiar los Datos Transaccionales que resulten procedentes de conformidad con los requisitos que el Banco de México establezca mediante resoluciones de carácter general que emita al efecto, en las cuales podrá establecer requisitos adicionales para dicho intercambio.

Artículo 6. Modificaciones al Plan de Trabajo. Las cámaras de compensación y SIC deberán solicitar la autorización del Banco de México para realizar modificaciones al Plan de Trabajo que este haya autorizado. Para tales efectos, las cámaras de compensación y SIC deberán presentar una solicitud a la Dirección de Autorizaciones y Sanciones de Banca Central del Banco de México en términos del **artículo 20** de estas Disposiciones, especificando las modificaciones que deseen realizar al Plan de Trabajo, señalando argumentos y presentando evidencia suficientes para acreditar que las modificaciones propuestas constituirían mejoras para el intercambio de datos o la

seguridad de la información. El Banco de México resolverá sobre la solicitud en términos del **artículo 8** de las presentes Disposiciones.

Asimismo, en protección de los intereses del público, el Banco de México podrá formular, en cualquier momento, modificaciones al Plan de Trabajo para asegurar el buen funcionamiento de las API, el acceso a los datos e información en condiciones equitativas y transparentes, la correcta administración de los datos, la seguridad de la información, o por cualquier otro riesgo o afectación a dichos intereses.

Artículo 7. Autorización a las Entidades Reconocidas para el acceso a las API. Las Entidades Reconocidas que deseen obtener acceso a los datos e información de las cámaras de compensación y SIC, según se prevé en el artículo 76 de la Ley, por medio de las API que establezcan para ello, deberán obtener la previa autorización del Banco de México.

Para tales efectos, a partir de la fecha en que el Banco de México, conforme al **artículo 8** de las presentes Disposiciones, publique en su sitio de internet los tipos de datos e información que las cámaras de compensación y SIC estarán autorizadas a intercambiar mediante las API que establezcan, cada Entidad Reconocida deberá presentar su solicitud de autorización ante la Dirección de Autorizaciones y Sanciones de Banca Central del Banco de México en términos del **artículo 20** de estas Disposiciones. La referida solicitud deberá contener aquellas medidas que implementarán para cumplir los estándares establecidos en la API de las cámaras de compensación y las SIC para asegurar la información y demás procesos relacionados con su conexión con la API.

En la solicitud anteriormente señalada, la Entidad Reconocida respectiva deberá especificar los tipos de datos e información previstos en las fracciones I a III del artículo 76 de la Ley, que el Banco de México haya publicado en su sitio de internet conforme al **artículo 8** siguiente, a los que pretenda acceder a través de las API correspondientes.

Artículo 8. Procedencia de las solicitudes de autorización. El Banco de México evaluará la solicitud de autorización que presente cada cámara de compensación o SIC conforme a los **artículos 4, 5** y **6** anteriores o las Entidades Reconocidas conforme al **artículo 7** anterior y, en cada caso, determinará si aquella reúne los requisitos previstos en las presentes Disposiciones.

En los casos en los que la solicitud de autorización no contenga la información y documentación necesaria, o no cumpla con los requisitos previstos en la Ley o en estas Disposiciones, el Banco de México prevendrá a la solicitante, por escrito y por una sola vez, para que, dentro del plazo de diez Días Hábiles Bancarios contados a partir del Día Hábil Bancario en el que el Banco de México notifique la prevención a la interesada, subsane las omisiones o realice las modificaciones a la solicitud o documentación presentada. El Banco de México podrá otorgar una prórroga al plazo referido hasta por cinco Días Hábiles Bancarios adicionales, previa solicitud que, para tales efectos, presente la interesada dentro del plazo para desahogar la prevención correspondiente. Si transcurrido el plazo establecido en la prevención o, en su caso, en la prórroga correspondiente, la solicitante no hubiere subsanado las omisiones señaladas o realizado las modificaciones requeridas por el Banco de México, este desechará la solicitud.

El Banco de México resolverá sobre la solicitud de autorización dentro de un plazo de ciento ochenta días contados a partir del Día Hábil Bancario inmediato siguiente a

aquel en el que reciba la solicitud. Este plazo se suspenderá una vez notificada la prevención señalada en el párrafo precedente, y se reanudará a partir del Día Hábil Bancario inmediato siguiente a aquel en el que la cámara de compensación o SIC interesada desahogue la prevención.

Transcurrido el plazo mencionado en el párrafo anterior sin que el Banco de México se haya pronunciado respecto a la procedencia de la solicitud de autorización, se entenderá la resolución correspondiente en sentido negativo.

Por lo que respecta a las autorizaciones que el Banco de México otorgue a las cámaras de compensación y SIC conforme a los **artículos 4** y **5** anteriores, aquel publicará en su sitio de internet, ubicado en www.banxico.org.mx, los tipos de datos e información que este haya autorizado a cada cámara de compensación y SIC compartir por medio de su respectiva API conforme a las presentes Disposiciones.

Sin perjuicio de lo anterior, en virtud de la autorización que el Banco de México otorgue a la cámara de compensación o SIC de que se trate conforme a los **artículos 4** y **5** anteriores, aquel tendrá la facultad de requerir a esta, en cualquier momento, el intercambio de datos o información adicionales a los autorizados. Asimismo, el Banco de México podrá establecer, mediante resolución de carácter general, las especificaciones de las operaciones de consulta y su respuesta, así como el diccionario de datos.

Artículo 9. Revocación de las autorizaciones. El Banco de México podrá revocar las autorizaciones a que se refieren las presentes Disposiciones en los casos en que se incumpla lo establecido en la Ley, en estas Disposiciones o en el Plan de Trabajo autorizado por el Banco de México.

En todo caso, las autorizaciones a que se refieren las presentes Disposiciones se considerarán revocadas en los casos en que la autoridad competente revoque la autorización de los sujetos obligados para operar como el tipo de entidad o intermediario financiero de que se trate o, en su caso, pierdan el carácter de Entidad Reconocida.

La revocación a que se refiere el presente artículo se realizará sin perjuicio de la imposición de sanciones a que haya lugar.

CAPÍTULO III
ACCESO A LA INFORMACIÓN

Artículo 10. Contratos de Interconexión. Las cámaras de compensación y SIC deberán permitir el acceso y conectividad a las API que establezcan únicamente a las Entidades Reconocidas que cuenten con la autorización del Banco de México a que se refiere el **artículo 7** de las presentes Disposiciones, así como a aquellos sujetos a que se refiere el párrafo décimo primero del artículo 76 de la Ley para los efectos previstos en dicho párrafo, y que hayan celebrado Contratos de Interconexión con las cámaras de compensación y SIC respectivas. Para estos efectos, los Contratos de Interconexión que celebren las cámaras de compensación y SIC deberán incluir, al menos, los siguientes elementos:

I. La aceptación expresa por parte de la Entidad Reconocida de someterse a lo establecido en el artículo 76 de la Ley y en las presentes Disposiciones.
II. Copia de la autorización para acceder a las API de la Entidad Reconocida, así como la declaración expresa de la Entidad Reconocida que dicha autorización se encuentra surtiendo efectos y, en su caso, la fecha en la que dejará de surtirlos.

III. La obligación de la Entidad Reconocida de notificar a la cámara de compensación o SIC respectiva sobre la revocación de la autorización para el acceso a las API.
IV. Las obligaciones de confidencialidad, seguridad e integridad de la información, en congruencia con lo establecido en la Ley, las presentes Disposiciones y el Plan de Trabajo autorizado por el Banco de México.
V. La aceptación de las partes contratantes para permitirse recíprocamente la remisión al Banco de México de la información y documentación que intercambien entre sí con motivo de la operación del Contrato de Interconexión.
VI. Los mecanismos y esquemas de soporte para solucionar problemas e incidencias de carácter técnico.
VII. Las causas para la suspensión o terminación del acceso a la información por acciones u omisiones cometidas por la Entidad Reconocida, en congruencia con lo establecido en la Ley, las presentes Disposiciones y el Plan de Trabajo autorizado por el Banco de México.
VIII. La prohibición de subcontratar o ceder los deberes, derechos y obligaciones contenidos en el Contrato de Interconexión.
IX. La estipulación de que la vigencia del Contrato de Interconexión estará sujeta a la condición resolutoria de la terminación de la vigencia y de la revocación de las autorizaciones para establecer la API y para acceder a la información compartida a través de las API.
X. La estipulación de que el Contrato de Interconexión podrá rescindirse en caso de que la Entidad Reconocida incumpla con lo establecido en la Ley, las presentes Disposiciones o el Plan de Trabajo autorizado por el Banco de México.
XI. El procedimiento que se llevará a cabo para la rescisión o terminación ordenada del Contrato de Interconexión.
XII. El sometimiento expreso al derecho y tribunales federales mexicanos, renunciando a la competencia que les pudiere corresponder en razón de otras causas.

Los términos y condiciones que las cámaras de compensación y SIC establezcan en los Contratos de Interconexión que formalicen con Entidades Reconocidas deberán guardar congruencia con aquellos previstos en la Ley, las presentes Disposiciones y el Plan de Trabajo que autorice el Banco de México.

CAPÍTULO IV
CONTRAPRESTACIONES

Artículo 11. Requisitos de las contraprestaciones. Las contraprestaciones que cobren las cámaras de compensación y SIC con motivo del intercambio de datos e información en términos de las presentes Disposiciones deberán ser equitativas y transparentes a todos los individuos involucrados, y no deberán constituir barreras de entrada, formales, regulatorias, económicas o prácticas. Las cámaras de compensación y SIC no podrán cobrar contraprestaciones diferenciadas por el acceso a la información.

Artículo 12. Solicitud de registro de las contraprestaciones. Las cámaras de compensación y SIC deberán solicitar al Banco de México el registro de una nueva contraprestación y de cualquier modificación a las contraprestaciones previamente registradas.

La solicitud deberá contener los siguientes elementos:

I. El nombre de la contraprestación.
II. Especificar si la contraprestación es nueva, consiste en un incremento o en una reducción.
III. El acto o hecho generador de la contraprestación.
IV. La periodicidad en la que la contraprestación sería exigible.
V. El importe que correspondería a la contraprestación o, en su caso, el método de cálculo. Tratándose de modificaciones, deberá indicarse tanto el importe o método de cálculo vigente, como el que se pretende registrar.
VI. La moneda en la que se denominaría la contraprestación.
VII. La fecha a partir de la cual se pretenda aplicar la nueva contraprestación o la modificación de una contraprestación previamente registrada.

Artículo 13. Procedencia del registro de las contraprestaciones. El Banco de México evaluará en cada caso si la solicitud de registro de las contraprestaciones contiene los elementos previstos en el artículo precedente. Para tales efectos, el Banco de México podrá requerir a la interesada cualquier información o documentación que estime necesaria.

En los casos en los que la solicitud de registro de las contraprestaciones no contenga los elementos previstos en el **artículo12** de estas Disposiciones, el Banco de México prevendrá a la solicitante, por escrito y por una sola vez, dentro del plazo de siete Días Hábiles Bancarios contados a partir del Día Hábil Bancario inmediato siguiente a aquel en el que se presente la solicitud de registro de una nueva contraprestación o del incremento de una previamente registrada, o dentro del plazo de dos Días Hábiles Bancarios contados a partir

del Día Hábil Bancario inmediato siguiente a aquel en el que se presente la solicitud de registro de la reducción de una contraprestación previamente registrada, para que la solicitante subsane las omisiones o realice las modificaciones a la documentación presentada que requiera el Banco de México dentro del plazo de diez Días Hábiles Bancarios contados a partir del Día Hábil Bancario inmediato siguiente a aquel en el que el Banco de México notifique la prevención. Si transcurrido el plazo establecido en la prevención, la solicitante no hubiere subsanado las omisiones señaladas o realizado las modificaciones requeridas por el Banco de México, este desechará la solicitud.

Transcurrido el plazo aplicable para realizar la prevención conforme a lo señalado en el párrafo anterior sin que el Banco de México haya prevenido a la solicitante, se tendrá por registrada la contraprestación con efectos a partir del Día Hábil Bancario inmediato siguiente a aquel en que la interesada haya presentado su solicitud de registro.

En caso que el Banco de México haya prevenido a la solicitante y esta haya subsanado satisfactoriamente las omisiones señaladas o realizado las modificaciones requeridas por el Banco de México, se entenderá registrada la contraprestación con efectos a partir del Día Hábil Bancario inmediato siguiente a aquel en que la cámara de compensación o SIC interesada desahogue satisfactoriamente la prevención.

El Banco de México, en su caso, podrá comunicar a la cámara de compensación o SIC solicitante que la solicitud de registro de la contraprestación fue desechada, o que la contraprestación o modificación ha sido registrada, indicando la fecha efectiva del registro.

Artículo 14. Observaciones a las contraprestaciones. El Banco de México podrá formular observaciones a la aplicación de contraprestaciones cuando sean nuevas o impliquen un incremento, dentro de los quince Días Hábiles Bancarios siguientes a aquel en que las cámaras de compensación o SIC las hagan de su conocimiento. Para tal efecto, se procederá conforme a lo siguiente:

I. Se entenderá que las cámaras de compensación y SIC hacen las contraprestaciones del conocimiento del Banco de México en la fecha efectiva de su registro.

   Para el caso de las solicitudes de registro de contraprestaciones que se presenten como parte del Plan de Trabajo conforme a lo dispuesto en el **artículo 4** y el **Anexo 2** de las presentes Disposiciones, la fecha efectiva del registro será el Día Hábil Bancario inmediato siguiente a aquel en el que el Banco de México notifique a la solicitante la autorización para el establecimiento de la API.

II. En el evento de que el Banco de México pretenda formular observaciones y, en su caso, vetar las contraprestaciones, lo notificará a la cámara de compensación o SIC de que se trate dentro de los siete Días Hábiles Bancarios siguientes a la fecha efectiva de registro de la contraprestación.

III. La cámara de compensación o SIC tendrá un plazo de tres Días Hábiles Bancarios contados a partir del Día Hábil Bancario inmediato siguiente a aquel en el que reciba la notificación a que se refiere la fracción II anterior para manifestar lo que a su derecho convenga y, en su caso, ofrecer pruebas, mediante escrito dirigido a la Dirección de Autorizaciones y Sanciones de Banca Central del Banco de México, firmado por personas con facultades suficientes para tales efectos.

IV. En caso que dentro del plazo previsto en la fracción II anterior la cámara de compensación o SIC no aporte la información o los elementos que, a juicio del Banco de México, justifiquen evitar que se formulen las observaciones de las contraprestaciones, o no comunique la decisión de desistirse de la solicitud de registro, el Banco de México procederá a formular las observaciones a más tardar en la fecha de vencimiento del plazo señalado en el párrafo primero del presente artículo.

Artículo 15. Veto de las contraprestaciones. Si las cámaras de compensación o SIC deciden aplicar las contraprestaciones a las que el Banco de México haya realizado y publicado observaciones, el Banco de México podrá vetar esas contraprestaciones y dichas entidades no podrán cobrarlas. Sin perjuicio de lo anterior, las cámaras de compensación y SIC deberán de abstenerse de interrumpir el acceso a la información por esta causa.

Artículo 16. Publicación de las contraprestaciones, observaciones y vetos. El Banco de México publicará las contraprestaciones registradas, así como las observaciones que formule sobre ellas y los vetos que aplique, a través de su sitio de internet ubicado en www.banxico.org.mx.

CAPÍTULO V
SUPERVISIÓN Y PROGRAMAS DE REGULARIZACIÓN

Artículo 17. Supervisión. El Banco de México podrá requerir a las cámaras de compensación, SIC, Entidades Reconocidas y sujetos a que se refiere el párrafo décimo primero

del artículo 76 de la Ley, en todo momento, la documentación, datos, registros, informes y, en general, la información que el Banco de México estime necesaria para comprobar el cumplimiento que los sujetos referidos den a lo dispuesto en la Ley, en las presentes Disposiciones o en el Plan de Trabajo autorizado por el Banco de México.

La supervisión que realice el Banco de México se llevará a cabo con apego a lo establecido en las Reglas de Supervisión, Programas de Autocorrección y del Procedimiento Sancionador del Banco de México.

Artículo 18. Suspensión del intercambio de la información. En protección de los intereses del público, el Banco de México podrá, previo derecho de audiencia que se otorgue a la cámara de compensación, SIC o Entidad Reconocida correspondiente, ordenar la suspensión parcial o total, temporal o definitiva, del intercambio de información a través de las API, en los casos en que se incumpla con lo establecido en la Ley o en las presentes Disposiciones. Lo anterior, salvo que el Banco de México apruebe un programa de regularización que la cámara de compensación o SIC de que se trate envíe a este, con objeto de subsanar los incumplimientos.

Artículo 19. Programa de regularización. El programa de regularización que las cámaras de compensación y SIC presenten al Banco de México en términos del artículo anterior deberá incluir, al menos, lo siguiente:

I. La identificación de la notificación del Banco de México respecto de las irregularidades o incumplimientos, así como la indicación de las disposiciones contravenidas.
II. Las acciones que la cámara de compensación o SIC de que se trate tomará para subsanar las irregularidades o incumplimientos, así como las personas y áreas responsables de realizar cada una de ellas, al igual que la forma y plazos en que pretende informar de su avance a los órganos de gobierno de la cámara de compensación o SIC, así como al Banco de México.
III. El plazo en que la cámara de compensación o SIC llevará a cabo las acciones tendientes a corregir las irregularidades o incumplimientos, así como, en su caso, un calendario detallado de actividades a realizar para ese efecto.
IV. La mención del daño o perjuicio que la irregularidad o incumplimiento haya producido a la propia cámara de compensación o SIC o a terceros, en caso de que esto sea del conocimiento de la cámara de compensación o SIC, así como el resarcimiento que, en su caso, se haya hecho de tales daños o perjuicios. En todo caso, deberá adjuntarse la información y documentación necesaria para dar soporte a lo previsto en esta fracción.
V. De ser el caso, la información sobre la suspensión de la acción u omisión que haya motivado la contravención a la norma.
VI. La indicación de la información específica que, en su caso, deba ser tratada como confidencial, en términos de las Leyes General y Federal de Transparencia y Acceso a la Información Pública, en el entendido de que la omisión al especificar el carácter de que se trate, implicará el consentimiento para su divulgación cuando haya una petición de un tercero, atento al principio de máxima transparencia y las bases contenidas en el artículo 6 de la Constitución Política de los Estados Unidos Mexicanos.

VII. La firma del director general o equivalente, así como del presidente del comité de auditoría o su equivalente de la cámara de compensación o SIC correspondiente.

El Banco de México prevendrá a la cámara de compensación o SIC de que se trate cuando su solicitud de autorización del proyecto del programa de regularización no contenga alguno de los requisitos aplicables, el Banco de México presuma alguna irregularidad o exista alguna duda respecto de la solicitud correspondiente.

La cámara de compensación o SIC de que se trate contará con un plazo de diez Días Hábiles Bancarios para desahogar dicha prevención, contados a partir del Día Hábil Bancario inmediato siguiente a aquel en el que el Banco de México la notifique. En casos excepcionales en que las circunstancias así lo justifiquen, la cámara de compensación o SIC supervisada podrá solicitar al Banco de México una prórroga a dicho plazo, la cual podrá otorgarse cuando este lo considere procedente. De no subsanarse las deficiencias dentro del plazo mencionado o de su prórroga, según corresponda, la solicitud se tendrá por desechada y no podrápresentarse nuevamente.

En lo no previsto en las presentes Disposiciones en relación con el programa de regularización, se estará a lo aplicable a los programas de autocorrección a que se refieren las Reglas de Supervisión, Programas de Autocorrección y del Procedimiento Sancionador del Banco de México.

CAPÍTULO VI
DISPOSICIONES GENERALES

Artículo 20. Envío de solicitudes al Banco de México. Las solicitudes de autorización y de registro de contraprestaciones a que hacen referencia los **artículos 4**, **5**, **6**, **7** y **12** de estas Disposiciones deberán ser enviadas vía correo electrónico por la cámara de compensación o SIC de que se trate a la Dirección de Autorizaciones y Sanciones de Banca Central del Banco de México, a la dirección de correo electrónico autorizaciones_api@banxico.org.mx.

Las personas que suscriban las solicitudes deberán:

I. Contar con un Certificado Digital Banco de México vigente expedido a su nombre.

II. Suscribir las solicitudes digitalmente utilizando la herramienta que el Banco de México determine para estos fines y que dé a conocer, así como el Certificado Digital Banco de México al que se refiere la fracción I de este artículo.

En los casos en que las cámaras de compensación o SIC no tengan acceso a los elementos necesarios para enviar las solicitudes firmadas digitalmente, podrán entregarlas en formato físico a la Dirección de Autorizaciones y Sanciones de Banca Central del Banco de México, ubicada en Avenida 5 de Mayo número 2, colonia Centro, código postal 06000, Demarcación Territorial Cuauhtémoc, Ciudad de México, en original por duplicado, suscritas por personas que cuenten con facultades suficientes para ejercer actos de administración o de dominio en representación de la solicitante. Para tales efectos, las cámaras de compensación y SIC deberán acompañar copia certificada y simple de las escrituras en las que consten las referidas facultades a su escrito de solicitud, así como un do-

cumento firmado por el referido representante en el que especifiquen las justificaciones por las cuales se ven en la necesidad de enviar solicitudes por este medio alterno.

Artículo 21. Sanciones. Las cámaras de compensación y SIC que incumplan con lo dispuesto en estas Disposiciones serán sancionadas por el Banco de México de conformidad con la Ley para Regular las Instituciones de Tecnología Financiera, la Ley del Banco de México y las demás disposiciones aplicables. Lo anterior, sin perjuicio de las facultades que las leyes otorguen a otras autoridades.

TRANSITORIOS

PRIMERO. Excepto por lo establecido en el artículo 5 de las presentes Disposiciones, la presente Circular entrará en vigor a los trescientos sesenta días siguientes al de su publicación en el Diario Oficial de la Federación.

SEGUNDO. Las cámaras de compensación y SIC contarán con un plazo de trescientos sesenta días a partir de la entrada en vigor de las presentes Disposiciones para obtener la autorización del Banco de México para el establecimiento de las API.

Las entidades que obtengan autorización para operar como SIC y cámaras de compensación con posterioridad a la entrada en vigor de las presentes Disposiciones contarán con un plazo de trescientos sesenta días a partir de la fecha en la que aquella surta efectos, para obtener la autorización del Banco de México para el establecimiento de las API.

TERCERO. Las solicitudes de autorización para el acceso a los datos e información de las API, así como para la prueba de nuevos productos y servicios, podrán otorgarse por el Banco de México una vez que las cámaras de compensación y sociedades de información crediticia hayan establecido e iniciado la operación de las API de que se trate.

CUARTO. Las cámaras de compensación y SIC, previamente a solicitar autorización del Banco de México para llevar a cabo el intercambio de Datos Transaccionales a través de las API que estas deban establecer conforme al artículo 5 de las presentes Disposiciones, deberán presentar, en un plazo de trescientos sesenta días a partir de la publicación de las presentes Disposiciones, ante la Dirección de Autorizaciones y Sanciones de Banca Central del Banco de México, sus propuestas del tipo de datos e información que deberá quedar comprendida en esta categoría, así como de los mecanismos por medio de los cuales tales entidades podrían autenticar, identificar y recabar, en su caso, el consentimiento expreso de los clientes respectivos para tales efectos. El Banco de México tomará en cuenta la referida información que presenten las cámaras de compensación y sociedades de información crediticia y establecerá, mediante la resolución de carácter general que emita al respecto, los Datos Transaccionales que las cámaras de compensación o sociedades de información crediticia deberán compartir por medio de sus respectivas API, así como los requisitos que deberán cumplir los mecanismos por medio de los cuales, en su caso, se deba recabar el consentimiento expreso del cliente a que se refiere la fracción III del artículo 76 de la Ley.

Con base en lo anterior, el artículo 5 de las presentes Disposiciones entrará en vigor en la fecha que el Banco de México establezca en la resolución de carácter general a que se refiere el párrafo precedente.

ANEXO 1
REQUISITOS MÍNIMOS DE INTEROPERABILIDAD Y MECANISMO DE AUTENTICACIÓN PARA LAS API QUE DEBEN ESTABLECER LAS CÁMARAS DE COMPENSACIÓN Y LAS SOCIEDADES DE INFORMACIÓN CREDITICIA

Las API que establezcan las cámaras de compensación y SIC, así como las Entidades Reconocidas, conforme a las presentes Disposiciones deberán cumplir con los requisitos técnicos descritos a continuación.

I. COMUNICACIÓN

Las API deberán ser capaces de recibir peticiones de servicio mediante los siguientes protocolos de comunicación definidos por la organización "Internet Engineering Task Force", en lo sucesivo IETF, auspiciada por la empresa constituida en los Estados Unidos de América denominada IETF Administration LLC.:

1. IP (Internet Protocol), versión 4 y, opcionalmente, versión 6, como protocolo de direccionamiento, bajo las especificaciones RFC 791 y RFC 8200, respectivamente.
2. TCP (Transmission Control Protocol), como protocolo de control de transmisión de datos, implementado bajo la especificación RFC 675.
3. TLS (Transport Layer Security), versión 1.2 y, opcionalmente, versión 1.3, como protocolo criptográfico y de validación de identidad del punto de acceso, implementado bajo las especificaciones RFC 5246 y RFC 8446, respectivamente.
4. HTTP (HyperText Transport Protocol), versión 1.1, como protocolo de comunicación de datos bajo las especificaciones RFC 7230, RFC 7231, RFC 7232, RFC 7233, RFC 7234 y RFC 7235.

Las cámaras de compensación y SIC podrán poner a disposición las API mediante otros protocolos, de forma adicional a los descritos anteriormente, siempre que estos mantengan el principio de cifrado de datos en tránsito y que permitan la validación, por parte del sistema informático o aplicación que solicita servicio, de la identidad del punto de acceso a las API.

Las API deberán estar disponibles para su ejecución en una dirección del protocolo internet (IP) pública.

II. SEGURIDAD

a. Privacidad e integridad de la información

Los datos que se compartan por medio de las API deberán estar protegidos por mecanismos de privacidad e integridad durante la transferencia por medio de red.

b. Autenticidad de la información

Con objeto que los sistemas informáticos y aplicaciones puedan validar la identidad de los puntos de acceso de las API que establezcan las cámaras de compensación y SIC, dichos puntos de acceso deberán presentar, durante el proceso que establece comunicación segura mediante el protocolo TLS, un certificado digital vigente emitido para estos efectos por una autoridad certificadora que cumpla con los siguientes criterios:

1. Distribución gratuita de su certificado raíz, así como de sus certificados in-

termedios correspondientes a sus autoridades certificadoras subordinadas.

2. Validación gratuita y pública de la no revocación de los certificados emitidos por ella y por sus autoridades certificadoras subordinadas a través de listas de revocación de certificados (CRL por sus siglas en inglés), bajo la especificación RFC 5280, o por medio del protocolo OCSP (Online Certificate Status Protocol), bajo la especificación RFC 6960, ambas definidas por la IETF.

El certificado digital deberá estar emitido conforme al formato X.509 v3, bajo las especificaciones RFC 5280, RFC 6818, RFC 8398 y RFC 8399 definidas por la IETF. Las cámaras de compensación y SIC deberán enviar al Banco de México el certificado digital que utilizarán para efectos de demostrar su identidad conforme a lo descrito en esta sección, con por lo menos siete días de anticipación a la fecha en la que se utilice el referido certificado.

c. Autenticación y control de acceso

Como mecanismo de autenticación y control de acceso para Datos Agregados en las API que establezcan, las cámaras de compensación y SIC deberán implementar listas de control de acceso por dirección del protocolo Internet (IP). Estas listas permitirán autenticar y conceder acceso a las Entidades Reconocidas autorizadas conforme a lo previsto en estas Disposiciones.

III. OPERACIÓN

Las API deberán prestar servicio mediante servicios web diseñados y desarrollados con base en el estilo arquitectural de software denominado REST (Representational State Transfer).

Los datos transmitidos deberán estar representados en el formato JSON (JavaScript Object Notation), definido por la IETF bajo la especificación RFC 8259.

Las cámaras de compensación y las SIC deberán notificar al Banco de México la dirección electrónica a través de la cual estarán disponibles las API, así como cualquier cambio, con por lo menos siete días de anticipación a la fecha en la que comenzará a prestar servicio a través de esta.

La ejecución de las interfaces deberá ser síncrona.

ANEXO 2
PLAN DE TRABAJO

El Plan de Trabajo que las cámaras de compensación y SIC presenten con la solicitud de autorización para el establecimiento de las API deberá contener, al menos, los siguientes elementos:

1. Sobre la transmisión de datos:

    1.1. Las categorías de datos respecto de las cuales soliciten autorización para transmitir a través de la API, detallando la información específica que compartirían en cada una de dichas categorías, observando los principios de confidencialidad, usabilidad y oportunidad.

    1.2. Las medidas para evitar que la transmisión de Datos Agregados permita la identificación de los datos personales o transacciones de las personas.

    1.3. Los mecanismos de autenticación para verificar que los terceros que pretendan acceder a la

API son Entidades Reconocidas con las que tengan formalizados Contratos de Interconexión.

1.4. Las medidas para verificar los mecanismos de autenticación para el acceso a Datos Agregados.

2. Aspectos legales:

2.1. Proyecto de modelo de Contrato de Interconexión, con los términos y condiciones que guarden consistencia con aquellos previstos en la Ley, las presentes Disposiciones y el Plan de Trabajo.

2.2. Solicitud de registro de contraprestaciones que pretendan cobrar.

3. Aspectos de gobierno corporativo:

3.1. Proyecto de manual sobre la transmisión de la información en términos de las presentes Disposiciones.

3.2. La estructura corporativa o de la administración general, incluyendo la normatividad interna y aquellos manuales o reglamentos que la cámara de compensación o SIC de que se trate considere aplicables y, en su caso, las modificaciones que realizarían a los mismos.

4. Riesgo operativo:

4.1. Las medidas y políticas que se tomarán para garantizar la seguridad de la transmisión de la información y asegurar la continuidad operativa de la API.

4.2. Las medidas y políticas en materia de control de riesgos operativos y de ciberseguridad.

4.3. La documentación y demás elementos que acrediten que la Infraestructura Tecnológica que dediquen las cámaras de compensación y SIC para la API está separada de la infraestructura que utilicen para realizar otras actividades.

5. Negocio:

5.1. La documentación y demás elementos que acrediten que la transmisión de datos e información a través de la API no afectará la adecuada provisión de los servicios relacionados con el objeto social de la solicitante.

6. Eficacia y eficiencia:

6.1. Acuerdos de nivel de servicio para la transmisión de la información.

El Banco de México podrá requerir a la interesada cualquier información o documentación que estime necesaria para evaluar la solicitud de autorización y el Plan de Trabajo.

Fuentes consultadas

Accenture, "PSD2: How can banks seize the opportunities?", disponible en <https://www.accenture.com/us-en/insight-psd2-opportunities-banks#block-overview>.

Alex Preukschat (coord.), Blockchain*, la revolución industrial de internet. Gestión 2000*, Grupo Planeta, 2017.

Asobancaria Colombia, "Documento Semana Económica 1144", 2019, disponible en <http://felaban.s3-website-us-west-2.amazonaws.com/publicaciones/archivo20181211205300.pdf>.

Banco Mundial, *Global Financial Development Report 2014*, Washington, D.C., 2013, disponible en <http://siteresources.worldbank.org/EXTGLOBALFINREPORT/Resources/8816096-1361888425203/9062080-1364927957721/GFDR-2014_Complete_Report.pdf>.

Banco Mundial, "Base de datos de desarrollo financiero DFDD", 2013, disponible en <http://databank.bancomundial.org/data/reports.aspx?source=desarrollo-financiero-mundial>, consultado en abril de 2013.

Barclays Bank, "Simplifica el proceso de solicitud de hipotecas para miles de agentes y clientes del Reino Unido gracias a una plataforma de vanguardia para la comunidad", disponible en <https://www.salesforce.com/mx/customer-success-stories/barclays/>.

BBC, "Cómo funcionan los 28 bancos que dominan la economía global", 2016, disponible en <https://www.bbc.com/mundo/noticias/2016/03/160325_economia_mecanismos_hidra_financiera_mundial_mj>.

BBVA, "Reseach Transformación digital y competencia en el sector financiero", 2019, disponible en <https://www.bbvaresearch.com/wp-content/uploads/2019/01/Transformacion-digital-y-competencia-en-el-sector-financiero-vf3_edi.pdf>.

BBVA Research, "Crowdfunding en 360º: alternativa de financiación en la era digital, 2014, disponible en <https://www.bbvaresearch.com/wp-content/uploads/2015/01/Observatorio_crowdfunding.pdf>.

BBVA Research, "Informe Situación Regulación Financiera 1T19", 2019), disponible en <https://www.bbvaresearch.com/wp-content/uploads/2019/01/Situacion_Regulacion_1T19.pdf>.

Boer, Martin, y Jaime Vázquez, "Cyber Security & Financial Stability: How Cyber-Attacks Could Materially Impact the Global Financial System", Institute of International Finance, 2017, disponible en <www.iif.com/system/files/iif_cyber_financial_stability_paper_final_11_13_2017_clean.pdf>.

Bouveret, Antoine, "Cyber Risk for the Financial Sector: A framework for Quantitative Assesment", IMF Working Paper WP/18/143, 2018.

Cañero, J., "La reforma de la regulación del sistema financiero internacional", disponible en >https://www.iefweb.org/wp-content/uploads/2019/01/reforma_regulacion_sistema_financiero_internacional.pdf>.

Capgemini y Efma, *Banca Abierta, el Reporte Mundial de FinTech 2019*, WFTR, 2019, disponible en <https://www.capgemini.com/mx-es/wp-content/uploads/sites/24/2019/06/

Reporte-Mundial-de-FinTech-2019-la-industria-est%C3%A1-cambiando-de-Open-Banking-a-Open-X.pdf>.

CEPAL, "La inversión extranjera directa en América Latina y el Caribe", 2011, disponible en <http://www.cepal.org/publicaciones/xml/0/46570/LIE2011esp.pdf>.

CNBV, Boletín núm. 10, enero-junio de 2017, disponible en <http://www.cnbv.gob.mx/CNBV/Sanciones/Boletin_de_Sanciones_ene-jun_2017.pdf>.

CNBV, "CNBV recibió 85 solicitudes de autorización para operar como Institución de Tecnología Financiera", CNBV, 2019, disponible en <https://www.gob.mx/cnbv/articulos/cnbv-recibio-85-solicitudes-de-autorizacion-para-operar-como-institucion-de-tecnologia-financiera>.

CNBV, "Panorama anual de Inclusión Financiera 2019", 2019.

COFECE, "Trabajo de investigación y recomendaciones sobre las condiciones de competencia del sector financiero", 2014, disponible en <https://www.cofece.mx/cofece/images/banners/sfinanciero/Resumen_Ejecutivo_Trabajo_de_Investigacion_del_Sistema_Financiero.pdf>.

Deloitte, "Tendencias y retos del sector financiero en el entorno actual", 2018, disponible en <https://www.ucm.es/data/cont/docs/459-2018-11-21-Retos%20del%20sector%20financiero%20(19noviembre%202018).pdf>; <https://riull.ull.es/xmlui/bitstream/handle/915/7510/La%20Evolucion%20del%20Sistema%20Bancario.pdf?sequence=1&isAllowed=y>.

Deloitte, "Tendencias tecnológicas 2019. Más allá de la frontera digital", 2019, disponible en <https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/technology/Tendencias_tecnologicas_2019% 20(Reporte%20Completo).pdf>.

"Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina", 2019, disponible en <https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf>.

El Economista, "Bancos piden que big tech tengan las mismas reglas en servicios financieros", 2019, disponible en <https://www.eleconomista.com.mx/sectorfinanciero/Bancos-piden-que-big-tech-tengan-las-mismas-reglas-en-servicios-financieros-20190414-0072.html>.

El Economista, "#Tecnología, clave para la inclusión y competencia en el sistema financiero, 2019, disponible en <https://www.eleconomista.com.mx/sectorfinanciero/Tecnologia-clave-para-la-inclusion-y-competencia-en-el-sistema-financiero-20190529-0003.html>.

EL País, "Internet 'Blockchain': la tecnología que va a cambiar tu vida", disponible en <https://retina.elpais.com/retina/2017/03/30/tendencias/1490871615_134683.html>.

"El Sistema Financiero Digital: los nuevos agentes", 2019, disponible en <http://www3.uah.es/iaes/publicaciones/DT_04_19.pdf>.

El sistema financiero mexicano. Diagnóstico y recomendaciones, Centro de Estudios Espinosa Yglesias, 2017.

Encuesta Nacional de Inclusión Financiera 8, 2017, disponible en <http://www.cnbv.gob.mx/Inclusi%C3%B3n/Documents/Reportes%20de%20IF/Reporte%20de%20Inclusion%20Financiera%207.pdf>.

Endeavor, Embajada Británica, Santander, Finnovista y Google, "Termómetro Fintech: Los retos de la regulación", 2019, disponible en <http://contenido.endeavor.org.mx/descarga-reporte-fintech-2019>.

"Estándar Bancario Abierto: Un estándar para migrar la banca a la economía digital del siglo XXI", disponible en <https://datos.gob.mx/blog/estandar-bancario-abierto-un-estandar-para-migrar-la-banca-a-la-economia-digital-del-siglo-xxi>.

EY, "Open Banking Opportunity Index: donde la banca abierta está llamada a prosperar", 2019, disponible en <https://www.ey.com/es_mx/banking-capital-markets/ey-open-banking-opportunity-index-where-open-banking-is-set-to-thrive>.

Felaban, "IV Informe de Inclusión Financiera", 2018, disponible en <http://felaban.s3-website-us-west-2.amazonaws.com/publicaciones/archivo20181211205300.pdf>.

Fernández de Lis, Santiago, y Pablo Urbiola Ortún, "Transformación digital y competencia en el sector financiero", 2018, disponible en <https://www.bbvaresearch.com/wp-content/uploads/2019/01/Transformacion-digital-y-competencia-en-el-sector-financiero-vf3_edi.pdf>.

Financial Stability Board, "Fintech y estructura del mercado en servicios financieros: Desarrollo del mercado y posibles implicaciones para la estabilidad financiera", 2019.

Finnovating, "Impacto de los competidores en el roe bancario en 2024", 2019, disponible en <https://www.finnovating.com/news/impacto-de-los-competidores-en-el-roe-bancario-en-2024/>.

Flor Esther Salazar, F., L. Guzmán, "¿Quién le come más tarta a los bancos? ¿Google, Apple o Amazon?", disponible en <https://www.estrategiasdeinversion.com/analisis/bolsa-y-mercados/informes/quien-le-come-mas-tarta-a-los-bancos-google-apple-n-424349>.

Global FinTech, "Adoption Index", 2019, disponible en <https://fintechauscensus.ey.com/2019/Documents/ey-global-fintech-adoption-index-2019.pdf>.

"Globalización financiera y crisis económica ¿producto de los cambios en las estructuras bancarias a partir de 1980?", disponible en <http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1692-85632015000200007>.

H. M. Queen Máximajim Yong Kim, "La importancia de la tecnología financiera, el uso de las cuentas y la innovación para lograr la inclusión financiera", disponible en <https://blogs.worldbank.org/es/voices/la-importancia-de-la-tecnolog-financiera-el-uso-de-las-cuentas-y-la-innovaci-n-para-lograr-la>.

Hernández T. N., y G. C. García, *La evolución del sistema bancario*, 2017.

Hussain, K., "Artificial intelligence and its applications goal", *International Research Journal of Engineering and Technology (IRJET)*, vol. 5, t. 1, enero de 2018, pp. 838-841, disponible en <https://irjet.net/archives/v5/i1/irjet-v5i1180.pdf>.

Igual Peña, Francisco, "Qué puede hacer el internet de las cosas por la banca", junio de 2019, disponible en <https://www.bbva.com/es/que-puede-hacer-el-internet-de-las-cosas-por-la-banca/>.

Informe del GAFI, "Monedas virtuales, definiciones clave y riesgos potenciales de LA/FT", 2014, disponible en <http://www.gafilat.org/UserFiles/Biblioteca/Doc20Interes/tipologias%20gafi/MonedasVirtuales(ESP).pdf>.

"Informe sobre Big Data en el sector financiero", disponible en <https://www.ey.com/es/es/home/ey-informe-sobre-big-data-y-analytics-en-el-sector-financiero-espanol#.Xi4pkyPhBlA>.

"La banca abierta es el futuro del sistema financiero en México", 2019, disponible en <https://www.bbva.com/es/mx/la-banca-abierta-es-el-futuro-del-sistema-financiero-en-mexico/>.

Marous, J., "The 'year of ai and machine learning' for financial marketers", 2018, disponible en <https://thefinancialbrand.com/69686/ai-machinelearning-banking-marketing-martech-data-trends/.>

Mayer-Schönberger, Viktor, y Kenneth Cukier, *La revolución de los datos masivos*, Editorial Turner, 2013.

McLean, B., y J. Nocera, *All the Devils Are Here: Unmasking the Men Who Bankrupted the World*, Penguin, 2010.

Nersisyan, Y., y R. Wray, "The Global Financial Crisis and the Shift to Shadow Banking", Working Paper 587, Levy Institute Economics, 2010.

OEA/CNBV, "Estado de la ciberseguridad en el sistema financiero mexicano", 2019.

Office of Financial Research, "2016 Financial Stability Report, 2016, disponible en <https://www.financialresearch.gov/financial-stabilityreports/files/OFR_2016_Financial-Stability-Report.pdf>.

Olloqui, Andrade, y Herrera, "Inclusión financiera en América Latina y el Caribe. Coyuntura actual y desafíos para los próximos años", documento para discusión núm. IDP-DP385, Banco Interamericano de Desarrollo, 2015.

Open Banking, "Preparing forlift of", disponible en <https://www.openbanking.org.uk/wp-content/uploads/open-banking-report-150719.pdf>.

Open Banking, "What It Means For You", 2019, disponible en <https://sencanada.ca/en/info-page/parl-42-1/banc-open-banking/>.

Ortiz Palacios, Luis A., "Desregulación financiera y transformación de los mecanismos de financiamiento y fondeo a la inversión en México", disponible en <http://www.economia.unam.mx/publicaciones/econinforma/pdfs/337/06luisnagelortizpalacios.pdf>.

Ortiz, Guillermo, "La crisis de 1994-95 y la actual crisis", 2009, disponible en <https://expansion.mx/economia/2009/01/30/la-crisis-del-199495-y-la-actual-crisis>.

Presburger Cherem, Enrique, "¿Podrán sobrevivir las Sofomes a la 4T?", 2019, disponible en <https://idconline.mx/corporativo/2019/07/03/podran-sobrevivir-las-sofomes-a-la-4t>.

PSD2 y Open banking, "Lo mejor aún está por llegar", 2018, disponible en <https://www.bbva.com/es/psd2-open-banking-mejor-aun-esta-llegar/>.

PwC, "Los medios de pago, un paisaje en movimiento", Informe del Centro del Sector Financiero de PwC e IE Business School, España, 2015.

PwC, "Banking Banana Skins 2015. The CSFI Survey of bank risk", PwC/Centre for Study of Financial Innovation, 2015.

"¿Qué es y cómo nos afecta la nueva Directiva PSD2?", disponible en <http://www.legaltoday.com/blogs/transversal/blog-ilp-abogados/que-es-y-como-nos-afecta-la-nueva-directiva-psd2>.

Quesada, Palacios A., "Normatividad Bancaria. Inclusión Financiera y Desarrollo", México, Editorial Porrúa, 2017.

Quintas R. Juan, *El sistema financiero ante el cambio tecnológico*, 1990.

"Regulación 'Fintech': tendencias de una nueva era", enero 2019, disponible en <https://www.bbva.com/es/regulacion-fintech-tendencias-de-una-nueva-era/>.

"Regulación sobre la operación con activos virtuales por parte de las Instituciones de Tecnología Financiera e Instituciones de Crédito, disponible en <https://www.banxico.org.mx/sistemas-de-pago/6--acciones-regulatorias-po.html>.

Resoluciones DOF, 2017, disponible en <https://www.cofece.mx/cfcresoluciones/docs/Opiniones/V20/6/3953499.pdf>, consultado el 22 de diciembre de 2019.

S&P Global Ratings, "El futuro de la banca: Tecnología e innovación podrían expandir el acceso a los servicios bancarios en México", 2019, disponible en <https://www.spratings.com/documents/20184/1493074/2019-03-26-El-futuro-de-la-banca-Tecnologia-e-innovacion-podrian-expandir-el-acceso-a-los-servicios-bancarios-en-Mexico/6-81ac5b6-2e82-79a7-168f-54a6b7cd04ae>.

Salazar, F. E. y L. C. Guzmán, "Globalización financiera y crisis bancaria ¿producto de los cambios en las estructuras bancarias a partir de 1980?", *Dimensión Empresarial*, vol. 13 (1), 2015, disponible en <http://dx.doi.org/10.15665/rde.v13i2.531>.

SEGOB, Subsecretaría de Enlace y Acuerdos Legislativis, oficio núm. SELAP/300/2734/17.

SEGOB, Subsecretaría de Enlace y Acuerdos Legislativis, oficio núm. SELAP/300/2734/17.

Statista, "Previsión de la evolución de los dispositivos conectados a internet en el mundo de 2012 a 2020", 2015, disponible en <https://es.statista.com/estadisticas/517654/prevision-de-la-evolucion-de-los-dispositivos-conectados-para-el-internet-de-las-cosas-en-el-mundo/>.

Tapscott, Don, y Alex Tapscotta, *La revolución blockchain*, Ediciones Deusto, 2017.

Titelman, D., *La banca de desarrollo y el financiamiento productivo*, CEPAL, 2003, disponible en <http://www.cepal.org/publicaciones/xml/7/14027/lcl1980e.pdf>.

Tovar, Camilo E., "Las entidades de crédito y la naturaleza cambiante de los riesgos en América Latina y el Caribe", disponible en <https://www.bis.org/publ/bppdf/bispap33esp_c.pdf>.

U.S. Treasury Department Office of Financial Research, "Cybersecurity and Financial Stability: Risks and Resilience", 2017, disponible en <https://www.financialresearch.gov/viewpoint-papers/files/OFRvp_17-01_>.

Vilariño, Ángel, "Regulación financiera y riesgos sistémicos bajo la hegemonía del capital financiero (versión provisional), 2018, disponible en <https://www.ucm.es/data/cont/media/www/pag111196/Regulaci%C3%B3n%20financiera,%20riesgos%20sist%C3%A9micos%20y%20hegemon%C3%ADa%20del%20capital%20financiero.pdf>.

Visa, "El panorama de la innovación en América Latina: Lecciones de las empresas innovadoras de la región", 2019, disponible en <https://www.visa.com.pe/dam/VCOM/regional/lac/SPA/Default/The%20Visa%20Difference/Innovation/el-panorama-de-la-innovaci%C3%B3n-en-am%C3%A9rica-latina.pdf>.

Vives, Xavier, "La industria financiera y la crisis: el papel de la innovación", en *Innovación. Perspectivas para el siglo XXI*, Madrid, BBVA, 2011, disponible en <https://www.bbvaopenmind.com/articulos/la-industria-financiera-y-la-crisis-el-papel-de-la-innovacion/>.

World InsurTech, "Report 2019", disponible en <https://www.capgemini.com/es-es/news/world-insurtech-report-2019/>,

C.P.C. JOSE ANTONIO QUESADA PALACIOS

Vicepresidente de Política Regulatoria
Comisión Nacional Bancaria y de Valores (CNBV)

José Antonio Quesada Palacios es Vicepresidente de Política Regulatoria en la Comisión Nacional Bancaria y de Valores de México (CNBV), desde 2019. En el ámbito internacional y nacional, José Antonio representa a la Comisión en las siguientes funciones:

- Representante de la CNBV en el BCBS (Basel Committee on Banking Supervision) | **BCBS (Comité de Supervisión Bancaria de Basilea).**
- Representante de la CNBV en el FSB SRC (FSB Standing Committee on Supervisory and Regulatory Cooperation) | **FSB SRC (Comité Permanente de Cooperación en Supervisión y Regulación del Consejo para la Estabilidad Financiera).**
- Representante de la CNBV en el FSB SCSI (FSB Standing Committee on Standards Implementation) | **FSB SCSI (Comité Permanente de Implementación de Estándares del Consejo para la Estabilidad Financiera).**
- Miembro del Consejo Directivo de IOSCO (International Organization of Securities Commissions) | **IOSCO Board (Consejo Directivo de la Organización Internacional de Comisiones de Valores)**
- Presidente del IARC (Inter American Regional Committee) de IOSCO | **IARC Comité Regional Interamericano**
- Presidente del Grupo de Trabajo GEMC Fintech de IOSCO | **GEMC (Comité de Mercados Emergentes y en Crecimiento)**
- Miembro del FAC (Finance and Audit Committee) de IOSCO | **FAC (Comité de Auditoría y Finanzas)**
- Miembro del Consejo de AFI (Alliance for Financial Inclusion). | **AFI (Alianza para la Inclusión Financiera)**
- Director de la Región Norte de ASBA (Association of Supervisors of Banks of the Americas) | **ASBA (Asociación de Supervisores Bancarios de las Américas)**
- Miembro de la Junta Directiva de ASBA | **ASBA (Asociación de Supervisores Bancarios de las Américas)**

- Miembro del Consejo de la NAASA (North American Securities Administrators Association) | **NAASA (Asociación de Administradores de Valores de América del Norte)**
- Secretario Ejecutivo del **Consejo Nacional de Inclusión Financiera (CONAIF)**
- Miembro Permanente de la Junta de Gobierno del Comité de Estabilidad Financiera (**CESF**)
- Miembro Permanente de la **Junta de Gobierno** de la Comisión Nacional Bancaria y de Valores (**CNBV**)
- Miembro de la **Junta de Gobierno** de la Comisión Nacional de Seguros y Fianzas (**CNSF**)
- Miembro de la **Junta de Gobierno** del Instituto para la Protección al Ahorro Bancario (**IPAB**).

Anteriormente colaboró como Director de la EGADE Business School del Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM) en su campus Santa Fe. También fue Presidente del Instituto Mexicano de Ejecutivos de Finanzas (IMEF) en el año 2012, y fue miembro del Consejo Directivo de PricewaterhouseCoopers (PWC), firma de la cual fue socio. Su trayectoria en PwC inició desde el año 1986 en el área de especialización dentro de Servicios Financieros donde fue su líder. Posteriormente fue el Socio Líder de Clientes y Mercados (coordina las prácticas de las 14 Industrias y de la estrategia de enfoque al mercado de la Firma). Culmino su participación en PwC en diciembre de 2017. De igual manera, Antonio Quesada fue especialista en trabajos de Corporate Governance, con énfasis en las medidas establecidas en los EEUU en relación con el Código de Mejores Prácticas Corporativas (CMPC).

Ha participado en proyectos de colocación de empresas extranjeras en el Mercado de Capitales en los EEUU.

Es Licenciado en Contaduría por la Universidad Iberoamericana, tiene una Maestría en Administración por el Instituto Tecnológico Autónomo de México (ITAM) y una Maestría en Contaduría por el ITAM y Florida International University. Asimismo, realizó el programa de Perfeccionamiento D-1 del Instituto Panamericano de Alta Dirección de Empresas (IPADE). Cuenta con la Certificación como Contador Público por el Colegio de Contadores Públicos de México. Actualmente, se encuentra en el programa de Doctorado en Ciencias Financieras en el EGADE BS del Tecnológico de Monterrey.

El futuro llegó: bases y condiciones de la transformación del sistema financiero se terminó en la Ciudad de México durante el mes de mayo de 2020. La edición impresa sobre papel de fabricación ecológica con *bulk* a 80 gramos, estuvo al cuidado de la oficina litotipográfica de la casa editora.

Grañén Porrúa Grupo Editorial

El futuro llegó:
9 786078 341979

El pasado ha dado lecciones que deben tomarse en cuenta en el proceso evolutivo en el que está inmerso el sistema financiero. La aparición de las fintechs ha cambiado la interrelación de los participantes y ha propiciado que usuarios y autoridades estén pendientes de los cambios, de su aportación y de su impacto en el sistema financiero, lo que ha generado nuevas reglas y más cautela. Justamente esta realidad es la que expone el autor en este libro, mismo que forma parte de sus obras anteriores, en las que ha planteado, desde diferentes enfoques, la necesidad de que dicha transformación en el sistema financiero sea entendida para sacarle el máximo provecho en una dinámica que se modifica constantemente.

En *El futuro llegó: bases y condiciones de la transformación del sistema financiero*, el autor expone los cambios, la dinámica y los resultados habidos en el sistema financiero internacional y del país. Retoma lecciones aprendidas en México que lo han colocado a la vanguardia y ser un referente en materia legislativa, lo que representa una oportunidad y un compromiso para seguir comprendiendo y aprovechando las transformaciones.

En sus exposiciones y análisis, se remonta a las últimas décadas del siglo pasado porque, desde su perspectiva, es ésa la época en la que se colocaron los cimientos para construir y reconstruir el sistema financiero en el que la innovación se presentaba como una profecía, "sin la seguridad de que se cumpliría, o al menos en qué tiempo y a qué ritmo". *El futuro llegó*, dice ahora el autor, pero también advierte que deben tomarse en cuenta las lecciones aprendidas en el pasado.

Este libro no es una lección de historia, aunque sí representa una compilación de hitos para entender que la evolución del sistema financiero es continua y que seguirá siendo impulsada por las innovaciones tecnológicas, los cambios en la demanda y en la oferta de los consumidores, todo ello derivado de un entorno más competitivo.

Alejandro Valenzuela
Director General, Banco Azteca

EGADE Business School
Tecnológico de Monterrey

MAAT ASESORES

La transformación digital está acelerando los cambios y presenta una disyuntiva: cambiar o quedarse en el camino. El autor toma en cuenta esta realidad para plantear que *el futuro llegó*, aludiendo a la importancia de la innovación tecnológica en temas fundamentales del sistema financiero: ingeniería y arquitectura, riesgos, nuevos participantes y regulación. Para entender el futuro inmediato, que a la vez es un presente, la obra hace un recorrido por el pasado para que el lector tenga los elementos que le permitan saber por qué algunos cambian y otros se quedan en el camino que la tecnología está marcando, que las legislaciones están delineando y que los usuarios determinan. *El futuro llegó: bases y condiciones de la transformación del sistema financiero* es una obra indispensable para entender las acciones de todos los participantes del sistema financiero.

CARLOS ROJO
Presidente Ejecutivo de la
Asociación de Bancos de México

¿Sobre qué bases se está transformando el sistema financiero? Ésta es una de las preguntas que el autor se planteó para mostrar la evolución de una industria que en la última década ha cambiado no sólo por fuera sino también por dentro, lo que representa nuevas condiciones para interactuar en un entorno en el que los cambios ya no se postergan porque su velocidad define quién se queda y cómo.

La transformación —plantea el autor— se presenta dentro de las organizaciones que tradicionalmente han formado parte del sistema financiero y también en los nuevos actores que, si bien surgieron o se adaptaron dentro del cambio, requieren adherirse a una dinámica en la que el consumidor está en primera fila. Esta obra nos lleva por un recorrido para saber sobre qué bases se está transformando el sistema financiero y también cuáles son las condiciones, un binomio que está determinando grandes cambios.

ENRIQUE ZORRILLA
Director General del
Grupo Financiero Scotiabank México