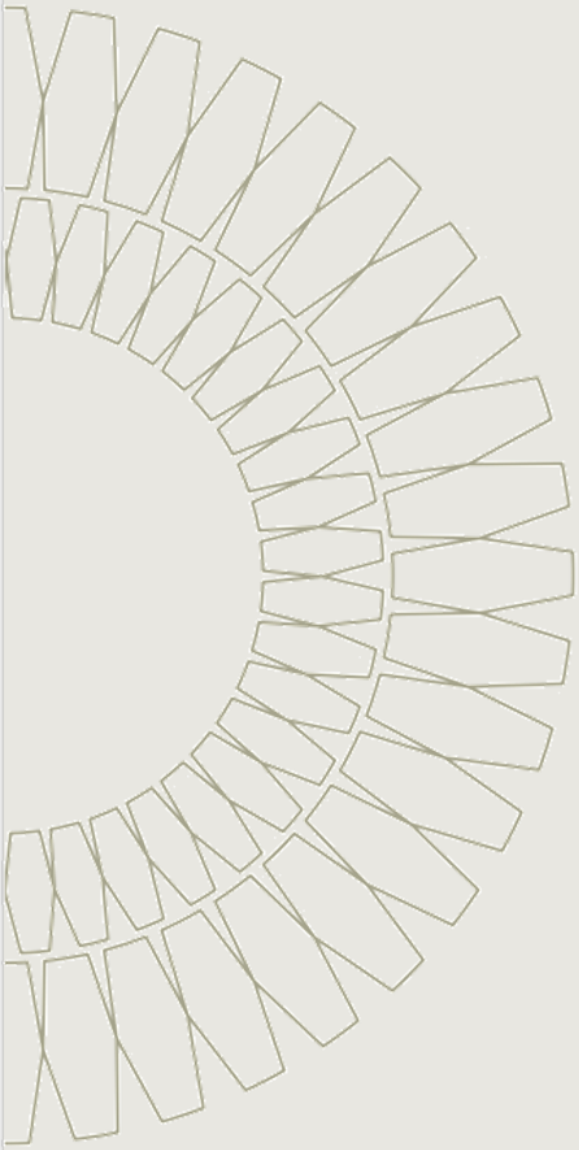


PRÁCTICAS GLOBALES DE REGULACIÓN Y SUPERVISIÓN DE FINTECH

Regulación para la Innovación Responsable y Competitiva del Sector Financiero

DICIEMBRE 2019

ASBA
ASOCIACIÓN DE SUPERVISORES BANCARIOS DE LAS AMÉRICAS

BID | LAB

JUNTA DIRECTIVA

Presidente
Juan Pedro Cantera (hasta octubre de 2018)
Banco Central del Uruguay

Paulo Sérgio Neves
Banco Central do Brasil

Vicepresidente
José A. Arévalo (hasta septiembre de 2018)
Superintendencia de Bancos de Guatemala

Jorge Castaño
Superintendencia Financiera de Colombia

Director Región Andina
Jorge Castaño (hasta octubre de 2018)
Superintendencia Financiera de Colombia

Socorro Heysen Zegarra
Superintendencia de Banca, Seguros y AFP, Perú

Director Región Caribe
Ingeborg Geduld-Nijman
Central Bank van Suriname

Director Región Centroamérica
Ethel Deras
Comisión Nacional de Bancos y Seguros, Honduras

Director Región Norte América
Teresa Rutledge (hasta octubre de 2018)
Office of the Comptroller of the Currency

José Antonio Quesada
Comisión Nacional Bancaria y de Valores, México

Director Región Cono Sur
Paulo Sérgio Neves (hasta octubre de 2018)
Banco Central do Brasil

Juan Pedro Cantera
Banco Central del Uruguay

Secretario General
Rudy V. Araujo (hasta diciembre de 2018)

Pascual O'Dogherty

CONTENIDO

AGRADECIMIENTOS

ASBA agradece a Rudy V. Araujo por su trabajo excepcional y su compromiso con el proyecto *Regulación para la Innovación Responsable y Competitiva del Sector Financiero*.

I. INTRODUCCIÓN

El objetivo de este documento es recopilar y analizar las prácticas globales relativas a la regulación y supervisión de los modelos de negocio, productos y servicios de Tecnologías Financieras o Fintech. Con este fin, el autor revisó las prácticas actuales de regulación y supervisión de las autoridades financieras, basándose en una encuesta distribuida entre los miembros de la Asociación de Supervisores Bancarios de las Américas (ASBA) sobre las regulaciones y enfoques relacionados con Fintech y otros documentos relevantes.

Se examinaron un total de 56 jurisdicciones distribuidas en los cinco continentes, incluyendo 11 miembros de la ASBA.

La lista de jurisdicciones se presenta en el Anexo 1. Cabe señalar que este informe se enfocó en identificar prácticas y tendencias comunes en lugar de catalogar regulaciones específicas.

La estructura del documento es la siguiente: la sección II estudia temas generales relacionados con la regulación y supervisión de Fintech, tales como regulaciones específicas de Fintech, el papel de las autoridades en la promoción de los desarrollos de Fintech y sus prohibiciones; la sección III explora las prácticas relacionadas con productos específicos de Fintech, mientras que la sección IV estudia las prácticas concernientes con las tecnologías que permiten la producción de diversos productos de Fintech. La última sección presenta los comentarios finales.

II. PRÁCTICAS GENERALES DE REGULACIÓN Y SUPERVISIÓN DE FINTECH

1. REGULACIÓN DE LAS ACTIVIDADES DE FINTECH EN FUNCIÓN DEL MARCO GENERAL EXISTENTE

En 2018, la ASBA distribuyó entre sus miembros una encuesta sobre la respuesta de los reguladores ante la irrupción de la tecnología Fintech en sus mercados financieros. Las respuestas fueron analizadas para comprender los enfoques y acciones futuras en materia de regulación y supervisión financiera.

En ese momento, pocas autoridades habían promulgado normativas específicas para los productos Fintech o las empresas especializadas en ello. Aunque la encuesta no fue exhaustiva, menos de 20 de las 38 jurisdicciones que respondieron a la encuesta, tenían regulaciones que podían ser identificadas como específicas para Fintech.

En parte, esta escasez de respuestas normativas se explica por el tamaño relativamente pequeño y la falta de impacto material de productos Fintech, según lo perciben los reguladores y los organismos internacionales como el Consejo de Estabilidad Financiera (FSB, por sus siglas en inglés), el Comité de Supervisión Bancaria de Basilea (BCBS, por sus siglas en inglés) y el Fondo Monetario Internacional (FMI).

La encuesta también destacó que la mayoría de los reguladores habían adoptado un enfoque cauteloso pero diligente para comprender plenamente los diferentes tipos de productos Fintech antes de intentar regularlos: seguir de cerca la evolución de los productos y las empresas de Fintech; fortalecer, en los planes de capacitación del personal, la comprensión de las cuestiones tecnológicas relacionadas con Fintech; así como la contratación de personal especializado.[1]

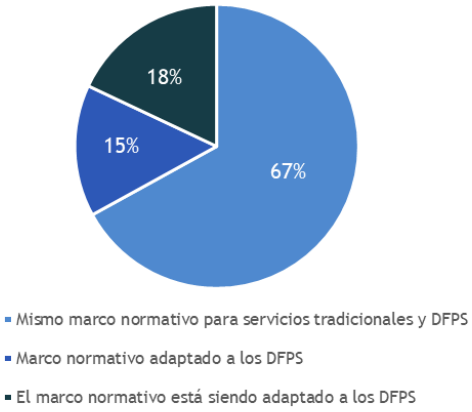
Otra explicación es que la mayoría de las autoridades consideran que los nuevos productos y proveedores de servicios de Fintech pueden o deben adaptarse al marco normativo existente. Una encuesta realizada por la Organización Internacional para la Protección del Consumidor Financiero (FinCoNet, por sus siglas en inglés) aplicada a 24 supervisores financieros de 23 jurisdicciones, incluidos cuatro miembros de la ASBA, respalda esta interpretación.

El informe de FinCoNet mostraba que dentro de los marcos normativos de los productos y servicios financieros digitales (DFPS, por sus siglas en inglés), "sólo el 15% de los encuestados afirmaba haber adaptado ya su marco normativo a los DFPS. Sin embargo, la adaptación específica parece estar relacionada únicamente con determinados productos. En consecuencia, para el resto de los DFPS, estas autoridades parecen encontrarse en una situación similar a la de la mayoría de los encuestados (67%), para los que el marco normativo aplicable es generalmente el mismo para los productos y servicios financieros digitales y tradicionales".[2]

1/ ASBA. Identifying Gaps and Opportunities in Financial Innovation Regulation. Abril de 2018.
2/ FinCoNet. Practices and Tools required to support Risk-based Supervision in the Digital Age. Noviembre de 2018.

El siguiente cuadro muestra la distribución de las respuestas:

GRÁFICA 1: MARCO NORMATIVO APLICADO A LOS DFPS



Fuente: FinCoNet. Practices and Tools required to support Risk-based Supervision in the Digital Age. Noviembre de 2018.

Se han encontrado resultados similares en un estudio entre bufetes de abogados que compara los marcos jurídicos internacionales de Fintech.[3] Ninguna de las 44 jurisdicciones encuestadas tenía, en el momento de la compilación, una ley o reglamento general para Fintech.

Esta práctica general no excluye el desarrollo de regulaciones para productos o empresas específicas de Fintech, principalmente para productos similares a la intermediación financiera (préstamos *peer-to-peer* y financiamiento colectivo (*crowdfunding*)) y pagos electrónicos. Un caso especial es México donde en marzo de 2018, la cámara de diputados aprobó una amplia Ley Fintech[4] que establece dos nuevos tipos de instituciones financieras: una para el financiamiento colectivo (*crowdfunding*) y otra para los pagos electrónicos. También establece la creación de la figura de los "modelos de negocio innovadores" y la facultación de las autoridades financieras para que regulen criptoactivos y para que concedan licencias temporales de forma parecida a los esquemas regulatorios del tipo *sandbox* regulatorio.

Cabe señalar que para los reguladores que siguen un enfoque basado en principios, la inclusión de Fintech en el marco regulador y de supervisión existente es coherente con el principio denominado de "igualdad de servicios/actividades, igualdad de riesgos e igualdad de normas", también denominado principio de "neutralidad tecnológica". Un buen ejemplo de este punto de vista es la Autoridad Supervisora de Mercados Financieros de Suiza (FINMA, por sus siglas en inglés), que adopta este concepto como principio de partida.[5]

El mismo principio fue establecido por la Comisión Europea al instaurar una política sobre la regulación de Fintech que fue expresada de la siguiente manera: "la misma actividad está sujeta a la misma regulación, independientemente de la forma en que se preste el servicio".[6] Sin embargo, la Comisión omitió este principio para una propuesta de regulación sobre financiación en régimen de financiamiento colectivo (*crowdfunding*) a escala europea.

3/ SUMROY, R. and KINGSLEY, B. (Editors). International Comparative Legal Guide to Fintech v2. Global Legal Group, Londres, Mayo de 2018.

4/ México. Ley para Regular las Instituciones de Tecnología Financiera. 9 de marzo de 2018.

5/ OECD. Reviews of Regulatory Reform: Switzerland. 2006.

6/ European Commission. Consultation Document: Fintech: A More Competitive and Innovative European Financial Sector. 2017.

La Comisión indicó que no se mantuvo la opción de "un enfoque basado en los productos, pues incluir la financiación en régimen de financiamiento colectivo (*crowdfunding*) en el actual código único de la UE [Unión Europea] (...), crearía una incertidumbre normativa injustificada a causa de la existencia de mecanismos de autorregulación para su aplicación".[7]

No debe sorprender al lector que este enfoque sea favorecido por las instituciones financieras tradicionales, como lo expresan sus comentarios a un documento de consulta del BCBS titulado *Sound Practices: Implications of Fintech developments for banks and bank supervisors*.[8]

Una de las ventajas de tratar la tecnología Fintech utilizando el marco regulatorio y de supervisión existente es evitar la creación de vacíos regulatorios, lo que podría perjudicar a los usuarios de servicios financieros y a las instituciones financieras tradicionales y reguladas.

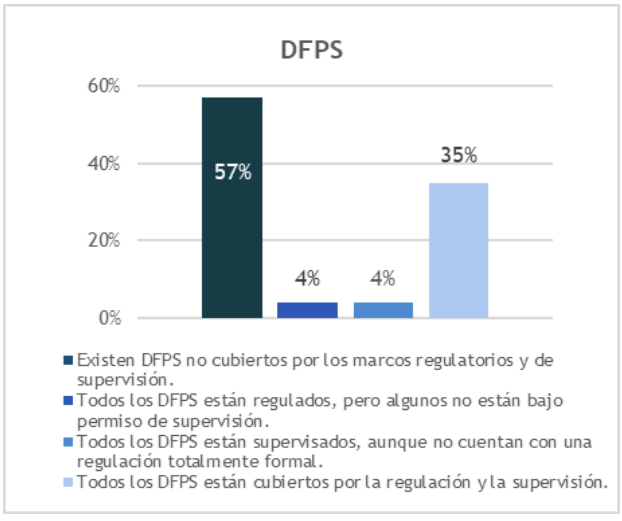
Otro factor de precaución para los reguladores es la incertidumbre en cuanto a la ampliación del perímetro reglamentario para incluir a los nuevos proveedores y productos o servicios no definidos explícitamente en el marco jurídico pertinente. Esta incertidumbre también fue considerada por FinCoNet en su encuesta. Una mayoría sustancial de los encuestados indicó que había DFPS y proveedores de DFPS fuera del perímetro de regulación y supervisión, como se muestra en la Gráfica 2.

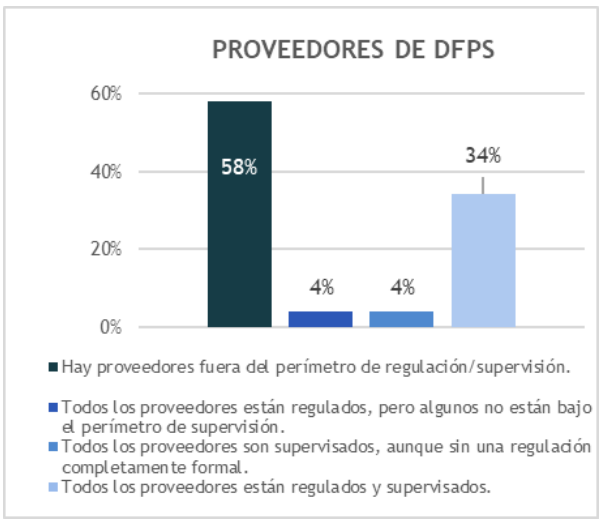
Por supuesto, como ya se ha señalado, los reguladores han tratado de ajustar el perímetro regulatorio para incluir a nuevos actores y emitir reglamentos que cubran productos, servicios y modelos de negocio específicos, permitiendo que las tecnologías cierren las brechas regulatorias. En los siguientes apartados se examinarán estas medidas reglamentarias.

Cualquiera que sea el motivo, para la mayoría de los reguladores, la práctica ha consistido en utilizar el marco regulatorio general existente cuando se enfrentan a la introducción de nuevos productos o a la aparición de nuevos proveedores, en lugar de crear un nuevo marco regulatorio general.

7/ European Commission. Proposal for a Regulation of the European Parliament and of the Council on European Crowdfunding Service Providers (ECSP) for Business. Marzo de 2018.
8/ Véanse los comentarios en International Banking Federation y en World Council of Credit Unions.

GRÁFICA 2: DFPS / PROVEEDORES DE DFPS Y PERÍMETRO DE REGULACIÓN/SUPERVISIÓN





Fuente: FinCoNet. Practices and Tools required to support Risk based Supervision in the Digital Age. Noviembre de 2018.

2. PROHIBICIÓN DE LOS PRODUCTOS FINTECH

Una consecuencia directa de la práctica antes mencionada es que los supervisores probablemente atiendan los riesgos de los productos Fintech utilizando el reglamento financiero general vigente. Muchos productos Fintech no se ajustan exactamente a los servicios o productos financieros regulados tradicionales, ni todos los proveedores de Fintech son empresas reguladas. Por lo tanto, esta incertidumbre regulatoria puede llevar a los supervisores a asumir que un producto y/o su proveedor está infringiendo la ley.

El riesgo de una acción de supervisión adversa para las empresas de Fintech es claro, especialmente para aquellas que ya cuentan con un modelo de negocio rentable. "La incertidumbre regulatoria desalienta la inversión. Los inversores se muestran reacios a invertir en una empresa que trabaja en un entorno no regulado, ya que los organismos reguladores pueden intervenir en cualquier momento y considerar que sus operaciones son ilegales".[9] Por lo tanto, es más probable que estas empresas aboguen por ser reguladas. Una encuesta reciente entre las nuevas empresas Fintech en América Latina reveló que "el treinta y cinco por ciento de los encuestados considera que la regulación es necesaria, a pesar de que actualmente no existe. Esto en comparación con solo el 9 por ciento que considera que actualmente el sector no necesita una regulación específica".[10]

De hecho, se han adoptado medidas de supervisión y aplicación de la ley a ciertos productos y empresas Fintech. En su forma más moderada, las autoridades pueden disuadir a los consumidores de utilizar las empresas Fintech haciendo hincapié en que sólo deben confiar en las empresas autorizadas. En los Estados Unidos, considerando su fragmentado sistema de regulación y supervisión, esta política puede conducir a acciones de cumplimiento por parte de una autoridad a nivel estatal contra las firmas Fintech con licencia en otros estados, como es el caso del Departamento de Servicios Financieros del Estado de Nueva York, que decidió imponer restricciones a los prestamistas online que no tienen licencia de operaciones en dicho estado.[11]

A pesar de los riesgos percibidos, los supervisores rara vez han prohibido productos o conjuntos de empresas Fintech. Estas acciones se han centrado en tres tipos de productos/empresas Fintech:

- Criptoactivos (la clase de activos y las empresas relacionadas con su creación e intermediación)
- Distribución directa de productos financieros sofisticados a usuarios minoristas (opciones binarias y contratos por diferencias)
- *Screen*, *web* y *data scrapping* (una técnica para recolectar los datos transaccionales de los usuarios financieros)

Con mucho, las acciones que restringen o prohíben las transacciones de criptoactivos han sido las más comunes. Aunque las prácticas de supervisión relativas a los criptoactivos se analizarán en detalle más adelante en este informe, es importante señalar aquí la falta de consenso entre las autoridades sobre si se debe prohibir a los consumidores, o a las instituciones financieras, que mantengan o realicen transacciones con criptoactivos. Incluso entre los miembros de la ASBA, existen claras disparidades en las políticas sobre dicha cuestión. En un extremo, Ecuador[12] y Bolivia[13] han prohibido cualquier transacción con criptoactivos, decisión que, en la práctica, sólo puede aplicarse a las instituciones financieras reguladas. Por otro lado, el Banco Central de México ha publicado una regulación de criptoactivos[14] que restringe las transacciones de éstos únicamente entre las instituciones financieras reguladas.

9/ Finextra. The Role of Regulatory Sandboxes in Fintech Innovation. Septiembre de 2018.

10/ Inter-American Development Bank – Finovista. FINTECH - Latin America 2018 - Growth and Consolidation. 2018.

11/ New York State Department of Financial Services. Online Lending Report. Julio de 2018.

12/ Junta de Politica y Regulacion Monetaria y Financiera. Las operaciones en criptomonedas no están autorizadas en el Ecuador. Febrero de 2018.

13/ Banco Central de Bolivia. Comunicado 04/2017. Abril de 2017.

14/ Banco de México. Circular 4/2019. Marzo de 2019.

Un tema relacionado, aunque en el mercado de valores, han sido las prohibiciones y restricciones a las llamadas Ofertas Iniciales de Moneda (ICOs, por sus siglas en inglés), el proceso de lanzamiento y venta de nuevos criptoactivos al público en general. Algunos supervisores, especialmente en China y Corea del Sur, reaccionaron definiendo estas transacciones como ofertas de valores públicos ilegales y decretando prohibiciones generales. Las jurisdicciones que han prohibido los criptoactivos, en consecuencia, también prohíben las ICOs. Replicando el tratamiento de los criptoactivos, algunas jurisdicciones permiten las ICOs, aunque generalmente están sujetas a las regulaciones de valores vigentes. Ejemplos de esta práctica se encuentran en Canadá, Rusia, Singapur, Suiza y algunos países de la Unión Europea (UE). EE.UU. no dispone de un enfoque unificado. La Comisión de Bolsa y Valores (SEC, por sus siglas en inglés) trata a una ICO como una oferta de valores, pero como por lo general no hay empresa establecida que apoye el nuevo criptoactivo, se ha negado a aprobar las solicitudes. Recientemente, la SEC publicó una declaración de política regulatoria[15] junto con su primera "carta de no intervención", en la que se autorizaba a una compañía aérea a emitir un *token* digital.[16]

En cuanto a la cuestión de las opciones binarias y los contratos por diferencias, la Autoridad Europea de Valores y Mercados (ESMA, por sus siglas en inglés) prohibió[17] la oferta de estos productos financieros similares a los juegos de azar entre los consumidores minoristas, ya que los inversores poco sofisticados no entienden bien los riesgos que conllevan. Otros países como Israel[18] y Canadá[19] también optaron por la prohibición total de tales instrumentos, mientras que Nueva Zelanda[20] y Australia permiten el comercio. Aunque el regulador australiano ha expresado su preocupación por las prácticas de los corredores.[21]

Menos extensa es la prohibición del *screen scrapping*. Esta técnica requiere que los usuarios financieros proporcionen a terceros, generalmente empresas Fintech, sus credenciales de acceso a las instituciones financieras reguladas donde poseen cuentas. Las empresas Fintech utilizan estas credenciales para acceder a las cuentas bancarias de los usuarios y capturar los datos transaccionales y así alimentar sus bases de datos y prestar servicios a sus clientes. Este proceso crea evidentes riesgos de seguridad para los usuarios, los bancos y las empresas Fintech. La Unión Europea prohibió esta técnica como parte de la legislación que exige que los bancos ofrezcan a terceros un acceso más seguro y confiable a los datos de sus clientes mediante una Interfaz de Programación de Aplicaciones (API).[22] Esta directiva, denominada como "banca abierta" (*open banking*), fue replicada en la ley mexicana Fintech citada anteriormente. Otros países han considerado una medida similar, pero hasta ahora han optado por no prohibir la técnica. La autoridad estadounidense de protección al consumidor financiero publicó una serie de principios, entre los que se incluye la frase "el acceso no requiere que los consumidores compartan sus credenciales de cuenta con terceros",[23] lo cual se ha interpretado como una señal de una futura prohibición.

Por el contrario, Australia ha adoptado una postura más matizada.

15/ SEC. Statement on Framework for 'Investment Contract' Analysis of Digital Assets. Abril de 2019.

16/ SEC. Response of the Division of Corporation Finance. Abril de 2019.

17/ ESMA. ESMA agrees to prohibit binary options and restrict CFDs. Marzo de 2018.

18/ Israel Securities Authority. The Knesset plenum approved second and third reading of the Binary Options Law. Octubre de 2017.

19/ Canadian Securities Administrators. Multilateral Instrument 91-102 Prohibition of Binary Options. Septiembre de 2017.

20/ New Zealand Financial Markets Authority. Binary options. Septiembre de 2018.

21/ Australian Securities & Investments Commission. ASIC calls on retail OTC derivatives sector to improve practices. Junio de 2018.

22/ European Union. Payment services (PSD 2) – Directive. 2015.

23/ Consumer Financial Protection Bureau. Consumer Protection Principles. Octubre de 2017.

Si bien en Australia se reconoce que las técnicas de *screen scraping* "dependen del consumidor (el titular de la cuenta bancaria) que introduce por primera vez su nombre de usuario y contraseña de banca por Internet (...) podría considerarse que el consumidor infringe los términos y condiciones bancarios estándar para la no revelación de contraseñas a terceros y los requisitos de seguridad de la contraseña que figuran en el Código de Pago Electrónico (...), a condición de que se puedan resolver todos los problemas relacionados con la seguridad de los datos, los consumidores no deben estar en desventaja debido a la utilización de los servicios de agregación de cuentas".[24] Este enfoque cauteloso se justifica por la resistencia de las instituciones financieras tradicionales a compartir los datos de los clientes incluso bajo mandato legal.

Además de estas acciones generales, ha habido múltiples acciones de vigilancia contra empresas individuales que utilizan productos Fintech para cometer fraude o dañar a los consumidores. Estas acciones deben considerarse en el marco de la protección del consumidor, que en algunos casos está dirigido por autoridades no financieras, y no reflejan las prácticas relativas a Fintech per se.

Aunque en algunos casos los supervisores han prohibido determinados productos, en general se han abstenido de disponer prohibiciones amplias contra productos o firmas Fintech.

3. LAS AUTORIDADES FINANCIERAS COMO PROMOTORAS DE FINTECH

En la actitud abierta de los reguladores hacia Fintech que se ha detallado anteriormente, se refleja un consenso entre las autoridades en el sentido de que las tecnologías Fintech podrían ser útiles para promover un sistema financiero más justo, más inclusivo y competitivo. En parte, este punto de vista ha sido promovido por organismos internacionales. Un ejemplo es la "Agenda Fintech de Bali", publicada por el FMI y el Banco Mundial, que establece que las autoridades nacionales deben "adaptar el marco regulatorio y las prácticas de supervisión para el desarrollo ordenado y la estabilidad del sistema financiero y facilitar la entrada segura de nuevos productos, actividades e intermediarios; mantener la confianza y la seguridad; y responder a los riesgos".[25]

Las autoridades financieras han estado implementando una variedad de acciones para ayudar a aquellos interesados en introducir innovaciones tecnológicas en sus mercados, incluyendo desarrollos por parte de instituciones financieras tradicionales, empresas no financieras y empresas de nuevo surgimiento.

La mayoría de estas acciones se pueden clasificar en cuatro grupos:

- Creación de una unidad dedicada a Fintech o, al menos, de un canal directo para consultas relacionadas con Fintech;
- Centros de innovación, concebidos como un lugar de encuentro entre autoridades, entidades financieras y emprendedores;
- Esquemas regulatorios del tipo *sandbox* regulatorio, un entorno de experimentación en vivo que se utiliza para garantizar el cumplimiento de la normativa y los controles de seguridad de las operaciones financieras;
- Licencias especiales de Fintech, que pueden ser generales o específicas para un producto y que, por lo general, tienen una duración limitada.

Otras actividades observadas en el informe incluyen documentos de políticas regulatorias de Fintech, incubadoras de Fintech en las que la autoridad financiera ayuda directamente a una empresa aspirante a madurar sus productos, enviar funcionaros especializados en Fintech a la cámara legislativa y otorgar asistencia directa a las autoridades de otros países en cuestiones de Fintech .[26]

24/ Australian Securities & Investments Commission. Review into Open Banking in Australia. Septiembre de 2017.

25/ IMF and World Bank. The Bali Fintech Agenda. Octubre de 2018.

26/ NLTimes. New Dutch Fintech envoy named: Former Finance Secretary Vermeend. February 2016. The Government of the United Kingdom also named a special Fintech envoy: HM Treasury. Fixing the foundations: Creating a more prosperous nation. Julio de 2015.

De las 56 jurisdicciones analizadas en este documento, más de la mitad (32) tenían por lo menos un programa implementado o propuesto, incluyendo 7 miembros de la ASBA. Este hallazgo no es sorprendente, ya que estas jurisdicciones fueron seleccionadas por tener una escena activa de Fintech. Cabe señalar que en dos países (Australia y España), los esquemas no fueron observados en la entidad encargada de supervisar a los bancos, sino en el regulador del mercado de valores. Además, en EE.UU., solo dos de los reguladores financieros federales tenían un esquema especial de promoción de Fintech.

La siguiente tabla muestra la distribución por región y tipo de esquema.

TABLA 1: ESQUEMAS DE PROMOCIÓN DE FINTECH OBSERVADOS POR LAS AUTORIDADES FINANCIERAS

Continente	Esquema observado	Unidad/canal dedicado	Centro de innovación	*Regulatory sandbox*[27]	Licencia especial de Fintech
Europa	14	13	12	9	2
Asia	8	8	6	8	4
Oceanía	2	1	1	1	0
África	1	1	0	0	0
América	6	4	3	4	3
Total	**32**	**27**	**22**	**22**	**9**
Como % de las 56 jurisdicciones analizadas	57%	48%	39%	39%	16%

Fuente: Información recopilada por el autor. Análisis por jurisdicción en Anexo 2.

Es evidente que las autoridades europeas, o más precisamente las que pertenecen a la Unión Europea, son los promotores más proactivos de Fintech, seguidos por las jurisdicciones asiáticas. En parte, este resultado refleja la presión competitiva para atraer la actividad Fintech, algo que en algunos países se ha convertido en una política nacional.

Este es el caso de la Unión Europea, donde su poder ejecutivo, como parte de una política integral de la UE, ha pedido a sus miembros "que tomen iniciativas para facilitar la innovación (...), [incluyendo] el establecimiento y funcionamiento de centros de innovación y esquemas de regulación tipo *sandbox* regulatorio".[28] Considerando que 12 de las 14 jurisdicciones europeas son miembros de la Unión Europea, que es, en efecto, una jurisdicción única en este aspecto, la proporción de jurisdicciones con esquemas promocionales activos se reduce al 47%, principalmente en Asia, reflejando la asimetría de políticas entre la UE y Asia Oriental, por un lado, y el resto del mundo, por otro.

De los cuatro esquemas observados, la creación de un canal dedicado a Fintech es el más simple y barato. En algunos casos, el canal es solo una dirección de correo electrónico específica. Las unidades dedicadas pueden ser tan pequeñas como tres empleados de medio tiempo. Los centros de innovación, incluso cuando son iniciados por la autoridad financiera, suelen financiarse mediante contribuciones de otras organizaciones del sector público y de la industria. En el otro lado del espectro se encuentran las licencias especiales de Fintech y los *sandboxes* regulatorios que, en muchas jurisdicciones, en particular las que están bajo un régimen jurídico de derecho civil, requieren una acción legislativa. Ambas opciones se analizan más adelante en este capítulo.

27/ Esta columna incluye tres países en donde se han propuesto esquemas regulatorios tipo *regulatory sandbox* pero éstos aún no han sido implementados.

28/ European Commission. Fintech action plan. Marzo de 2018.

Por lo tanto, la decisión de una autoridad financiera de promover activamente las actividades Fintech depende de la existencia de una política nacional, de la presión competitiva para atraer esas actividades y de su capacidad técnica y financiera.

La práctica más común y asequible, tanto en términos legales como financieros, implementada por las autoridades dispuestas a promover las actividades de Fintech en su jurisdicción, es la creación de un canal de comunicación específico que está conformado por un grupo pequeño, pero dedicado y bien informado de funcionarios, y que está abierto a todos aquellos que estén interesados en explorar la manera de introducir las innovaciones tecnológicas en el mercado financiero.

4. *SANDBOX* REGULATORIO

Quizás la desviación más emblemática de las prácticas tradicionales de supervisión financiera ha sido los esquemas de experimentación de regulación tipo *sandbox* regulatorio implementados por varias autoridades en todo el mundo. El FSB define estos esquemas como "marcos para probar nuevas tecnologías en un entorno controlado".[29] Estos *sandbox* se han vuelto cada vez más populares y están siendo promovidos activamente por algunos países, en particular Singapur y el Reino Unido, y por la industria. Hasta cierto punto, existe la percepción de que, para atraer la actividad de Fintech, un país necesita proporcionar un esquema de este tipo.

Sin embargo, de acuerdo con FinCoNet, "actualmente no existen definiciones o principios rectores claros y consistentes acordados a nivel internacional para lo que constituye un centro de innovación o un *sandbox* regulatorio".[30] Además, teniendo en cuenta que el primer regulatory *sandbox* no se estableció sino hasta 2016, la experiencia adquirida con estos esquemas es limitada y está intrínsecamente vinculada al marco legal de las jurisdicciones que los han establecido.

Dentro de la Unión Europea y en cumplimiento de un mandato específico de la Comisión Europea para desarrollar prácticas generales sobre los "facilitadores de la innovación", las tres Autoridades Europeas de Supervisión (ESAs por sus siglas en inglés)[31] elaboraron un informe conjunto sobre los *sandboxes* regulatorios, en el que concluyen que "se ha adquirido una experiencia limitada en el funcionamiento de los facilitadores de la innovación a los que se refiere este informe, ya que la mayoría de ellos se establecieron hace poco tiempo. Sin embargo, pueden formularse algunas observaciones a raíz de los resultados del análisis comparativo y de la participación de las ESAs, las autoridades competentes y el sector, que pueden orientar el establecimiento de un conjunto de principios operativos".[32]

Cabe señalar que uno de los objetivos clave del informe es garantizar la convergencia entre las autoridades nacionales de la UE en estos esquemas. La Comisión Europea, al encargar a las ESAs el estudio de los *sandboxes*, reconoció que "las autoridades nacionales expresaron opiniones encontradas: algunos supervisores consideran que estas iniciativas no forman parte de su mandato; por el contrario, los supervisores que están abiertos a estos esquemas regulatorios consideran que otros deberían tomar iniciativas similares".[33]

En otras jurisdicciones, el uso de sandboxes regulatorios por parte de los supervisores también está siendo disputado, sobre todo en EE.UU. El fragmentado sistema de regulación financiera en ese país ha sido identificado por el gobierno federal y la industria como una barrera para la innovación. Este hallazgo ha llevado al Departamento del Tesoro a recomendar "que los reguladores financieros federales y estatales establezcan una solución unificada que coordine y acelere la asistencia regulatoria en virtud de las leyes y reglamentos aplicables para permitir la experimentación significativa de productos, servicios y procesos innovadores". Tales esfuerzos formarían, en esencia, un sandbox regulatorio.[34]

29/ Financial Stability Board. Financial Stability Implications from Fintech. Junio de 2017.

30/ FinCoNet (2018).

31/ La Autoridad Bancaria Europea (EBA), la Autoridad Europea de Valores y Mercados (ESMA) y la Autoridad Europea de Seguros y Pensiones de Jubilación (EIOPA), conocidas colectivamente como ESAs.

32/ ESASs. Joint report on regulatory sandboxes and innovation hubs. Enero de 2019.

33/ European Commission (2018).

34/ US Treasury. Nonbank Financials, Fintech, and Innovation. Julio de 2018.

El supervisor financiero directamente bajo la dirección del Departamento del Tesoro, la Oficina del Contralor de la Moneda (OCC, por sus siglas en inglés), respondió rápidamente proponiendo un nuevo tipo de licencia bancaria: un "banco nacional con fines especiales". Según la OCC, "se trata de un banco nacional que realiza una gama limitada de actividades bancarias o fiduciarias, se dirige a una base limitada de clientes, incorpora elementos no tradicionales o tiene un plan de negocios con objetivos muy concretos".[35]

El Departamento de Servicios Financieros del Estado de Nueva York reaccionó a esta idea expresando que el supervisor a nivel estatal "se opone implacablemente a que el Departamento del Tesoro respalde los esquemas regulatorios tipo *sandbox* para las compañías de tecnología financiera. La idea de que la innovación sólo prosperará si se permite a las empresas eludir las leyes que protegen a los consumidores, y que también protegen los mercados, así como también mitigan el riesgo para el sector de los servicios financieros, es absurda. Los niños pequeños juegan en areneros. Los adultos juegan según las reglas. Las empresas que realmente quieren crear un cambio y prosperar a largo plazo aprecian la importancia de desarrollar sus ideas y proteger a sus clientes dentro de un marco regulatorio estatal sólido".[36]

La Oficina de Protección Financiera del Consumidor (CFPB, por sus siglas en inglés) también anunció su intención de establecer un *regulatory sandbox*,[37] siguiendo las recomendaciones del Departamento del Tesoro. Entre los varios comentarios recibidos en la consulta, una carta firmada por 22 fiscales estatales se distingue por concluir que "la innovación no debe venir a expensas de los consumidores o de la estabilidad del sistema financiero de EE.UU. Si algo nos ha enseñado la crisis financiera es que los reguladores deben tener cuidado con las innovaciones en el sector financiero hasta que puedan evaluar exhaustivamente sus riesgos. Además, los acontecimientos del pasado reciente no inspiran confianza en que las empresas de los sectores financiero y tecnológico sean capaces de supervisarse a sí mismas. Desafortunadamente, las políticas propuestas encarnan precisamente el tipo de fe ciega en la industria y la desconfianza regulatoria para la cual fue creado la CFPB, y le instamos a que las revoque".[38]

En vista de la breve historia de los *sandboxes* regulatorios, sus requerimientos legales, técnicos y de personal, así como los puntos de vista opuestos que estos esquemas crean, no es posible presentar las características observadas como prácticas generales. No obstante, reconociendo el interés que este esquema ha generado entre los supervisores, y teniendo en cuenta que tres miembros de la ASBA -Barbados,[39] Colombia[40] y México[41]- han implementado esquemas tipo *sandbox* y que otros están considerando esta opción, las lecciones y consejos prácticos brindados por aquellos que operan los *sandboxes* regulatorios serán revisados en futuros trabajos.

5. CONCESIÓN DE LICENCIAS ESPECIALES DE FINTECH

Como se mencionó, algunas jurisdicciones han introducido una nueva clase de licencias relacionadas con Fintech. Estas licencias pueden clasificarse en dos grandes grupos. Por un lado, algunas jurisdicciones, como México,[42] Dubái[43] y EE.UU.,[44] han implementado *sandboxes* regulatorios exigiendo a las empresas sin licencia que soliciten una licencia específicamente adaptada para este propósito. Este enfoque contrasta con el adoptado por la mayoría de las autoridades que operan esquemas tipo *sandbox*, que, o bien eximen a las empresas que aspiran a obtener una licencia antes de realizar las pruebas (i.e. el caso de Australia y Singapur), o bien exigen a las empresas que soliciten una licencia ordinaria (Reino Unido).

35/ OCC. Considering Charter Applications From Financial Technology Companies. Julio de 2018.
36/ VULLO, M. T. Statement by DFS Superintendent. Julio de 2018
37/ CFPB. Policy on No-Action Letters and the BCFP Product Sandbox. Diciembre de 2018.
38/ New York State Attorney General's Office. Comment Submitted. Febrero de 2019.
39/ Central Bank of Barbados. Regulatory Sandbox. Iniciado en octubre de 2018.
40/ Superintendencia Financiera. La arenera. Iniciado en abril de 2018.
41/ México. Ley para Regular las Instituciones de Tecnología Financiera. 9 de marzo de 2018.
42/ Ídem.
43/ Dubai Financial Services Authority. The DFSA Rulebook General Module – Amendment. Mayo de 2017.
44/ OCC (2018).

Estas concesiones vinculadas *al sandbox* regulatorio son de carácter temporal, suelen ser específicas para cada producto y tienen condiciones de salida explícitas.

Por otro lado, algunas autoridades ofrecen a las empresas de Fintech una licencia especial permanente con requisitos regulatorios menos estrictos que los de las licencias financieras estándar. El objetivo de esta licencia es que los nuevos actores puedan competir de manera efectiva con las instituciones financieras ya establecidas, al tiempo que se satisfacen los elementos clave del marco estándar de concesión de licencias. En algunas jurisdicciones, este tipo de licencia coexiste con las vinculadas a los *sandboxes* regulatorios; la primera está dirigida a proveedores con productos Fintech más maduros que a aquellos que desean probar sus productos en un *sandbox*.

Algunas jurisdicciones, en caso de que su marco jurídico lo permita, simplemente renuncian a algunos requisitos de licencias estándar para reducir la carga regulatoria de las nuevas instituciones financieras. Por ejemplo, la Comisión de Servicios Financieros de Corea del Sur indicó que "concederá a los nuevos bancos que operan exclusivamente en línea, un período de gracia de dos o tres años para la implementación de las regulaciones de Basilea III, (...) el aplazamiento consiste en dar tiempo a los recientes bancos virtuales para que se adapten a un nuevo régimen regulatorio, lo que aliviará la carga regulatoria de los mismos en la fase inicial de su operación de negocios".[46]

Otras autoridades establecen restricciones operativas y exenciones reglamentarias para quienes obtienen una licencia Fintech, como lo ilustra la licencia suiza de Fintech, que limita el tamaño de los depósitos individuales[47] y prohíbe el pago de intereses.

Sin embargo, el enfoque ampliamente adoptado para la concesión de licencias a las empresas de Fintech consiste en expedir autorizaciones para productos específicos, por lo general dentro de dos grandes grupos: servicios de pago y préstamos innovadores. Aunque inicialmente no se concibieron específicamente para las empresas Fintech, las licencias relacionadas con pagos están disponibles casi universalmente y son adecuadas para muchos de los productos Fintech.

Además, para muchas empresas de nueva creación y grandes empresas tecnológicas de carácter no financiero, la obtención de una licencia de proveedor de servicios de pago podría considerarse como un primer paso para entrar en el mercado financiero regulado. Monzo Bank y Starling Bank en el Reino Unido, así como PayU en la India son ejemplos de empresas de nueva creación con una licencia inicial limitada a servicios de pago que más tarde comenzaron a ofrecer préstamos y captar depósitos, convirtiéndose en bancos en línea con todos los servicios. Hasta ahora, todas las incursiones de Big Tech en servicios financieros han comenzado con licencias de servicios de pago, como Alibaba y Tencent en China, mientras que Amazon, Facebook, Google y Microsoft han obtenido licencias de "transmisoras de dinero" en EE.UU. Además, estas empresas, excepto Tencent, han obtenido una licencia de proveedor de servicios de pago en la Unión Europea. "A partir de entonces, algunos se expanden a la provisión de productos de crédito, seguros y ahorro e inversión, ya sea directamente o en cooperación con instituciones financieras asociadas ".[48]

Por otra parte, para los supervisores, la regulación y la supervisión de los servicios de pago tienen un largo y fiable historial, y los riesgos se conocen mejor. Por lo tanto, ofrecer una licencia restringida a los servicios de pago podría considerarse una vía segura para garantizar que las empresas que carecen de experiencia financiera adquieran progresivamente las competencias necesarias antes de que se les permita captar depósitos y prestar dinero.

De las 56 jurisdicciones analizadas para este documento, 44 tienen una licencia exclusiva de pagos; en muchos casos, esta licencia está adaptada para atender a las empresas de Fintech. Menos comunes son las licencias de préstamos *peer-to-peer* o de financiamiento colectivo (*crowdfunding*), que se utilizan en aproximadamente un tercio de las jurisdicciones.

45/ En particular, México.

46/ Financial Services Commission. FSC to delay implementation of Basel III for new online-only banks. Marzo de 2019.

47/ Swiss Financial Market Supervisory Authority. Fintech licence. Marzo de 2018.

48/ FROST, J. et al. BigTech and the changing structure of financial intermediation. BIS Working Papers No 779. Abril de 2019.

Sólo tres jurisdicciones han puesto en marcha una licencia de banca virtual o relacionada con criptoactivos. Cabe señalar que la categoría de pagos incluye la emisión de dinero electrónico (*e-money*), las transferencias electrónicas locales e internacionales, así como los monederos electrónicos.

La Unión Europea ha emitido directivas sobre el dinero electrónico (*e-money)*[49] y los servicios de pago[50] y está considerando una directiva a escala de la UE sobre financiación en régimen de financiamiento colectivo (crowdfunding) y de préstamos *peer-to-peer*,[51] en la cual se establecerían licencias especiales para estas áreas. Así pues, todos los países miembros de la UE, así como los que pertenecen al Espacio Económico Europeo (EEA, por sus siglas en inglés),[52] han incorporado o incorporarán estas directivas a su legislación nacional.

El análisis consideró si el régimen de licencias era lo suficientemente distintivo como para suponer que se adaptaba a los productos y empresas de Fintech y no tenía en cuenta los casos en los que la regulación y/o el enfoque de la autoridad eran indistinguibles de los sistemas tradicionales de licencias.

La siguiente tabla muestra la prevalencia y distribución geográfica de las licencias especiales de Fintech.

49/ European Union. E-money - Directive 2009/110/EC. Septiembre de 2009.

50/ European Union. Payment services (PSD 2) - Directive (EU) 2015/2366. Noviembre de 2015.

51/ European Commission. Legislative proposal for an EU framework on crowd and peer to peer finance. Marzo de 2018.

52/ El EEA incluye a todos los países de la UE e Islandia, Liechtenstein y Noruega. Permite que estos países formen parte del mercado único de la UE al tiempo que adoptan todas las normativas de la UE. Para más información, véase European Economic Area (EEA) / Relations with the EU.

TABLA 2: ESQUEMAS DE CONCESIÓN DE LICENCIAS DE FINTECH OBSERVADOS

Continente	Pago	*Peer-to-peer*	Financiamiento colectivo (*crowdfunding*)	Criptoactivos	Bancas virtuales	Jurisdicciones analizadas
Europa	20	5	8	1	0	23
Asia	11	5	3	1	3	13
Oceanía	0	1	1	0	0	2
África	5	0	0	0	0	7
América	8	3	5	1	0	11
Total	**44**	**14**	**17**	**3**	**3**	**56**
Como % de las jurisdicciones analizadas	79%	25%	30%	5%	5%	100%

Fuente: Información recopilada por el autor. Análisis por jurisdicción en Anexo 3.

A la luz de estos resultados, está claro que la concesión de una licencia de servicios de pago compatible con Fintech es una práctica común. No puede decirse lo mismo de las licencias de préstamos *peer-to-peer* o de las licencias orientadas al financiamiento colectivo (crowdfunding). Aún más raras son las licencias para intermediarios o emisores vinculados a criptoactivos o para bancos que solo operan en línea.

6. PRÁCTICAS RELATIVAS A LAS PRESTACIONES TRANSFRONTERIZAS DE FINTECH

Casi todas las jurisdicciones analizadas legalmente prohíben la prestación transfronteriza de servicios financieros si el proveedor no está autorizado por un supervisor local. Hay algunas excepciones a esta práctica general que vale la pena mencionar. La Unión Europea, incluida el EEA, permite el pleno acceso de instituciones financieras autorizadas en otra jurisdicción miembro, lo que se conoce como "derecho de pasaporte" y es coherente con el concepto de un mercado financiero único integral de la UE.

Además, la Directiva sobre Mercados de Instrumentos Financieros (MiFID II) permite la prestación de servicios financieros específicos por parte de empresas no pertenecientes al EEA sin necesidad de una sucursal o licencia. La gama de servicios es limitada y está principalmente vinculada a los mercados mayoristas de capitales, como el comercio de derivados del mercado extrabursátil (*Over-the-counter* (OTC)), las operaciones de cobertura y otras transacciones similares. Aunque la directiva no excluye ni menciona los productos Fintech, no se conocen empresas Fintech que utilicen esta facultad.

Otra excepción notable a la práctica general es Suiza. "La normativa suiza en materia de banca y de prevención contra el lavado de dinero no se aplica a los operadores de tecnologías de la información domiciliados en el extranjero que ofrecen sus servicios en Suiza sobre una base puramente transfronteriza, es decir, sin emplear a personas de forma permanente sobre el territorio de Suiza y sin establecer una sucursal u oficina de representación o cualquier otra forma de presencia física relevante en Suiza".

Asimismo, el *sandbox* de Bank Negara Malaysia "está abierto a todas las empresas Fintech, incluidas las que no tienen presencia en ese país".

No obstante, en reportes anteriores se ha destacado el hecho de que las tecnologías que sustentan muchos de los productos de Fintech permiten la prestación de servicios y productos financieros a los usuarios de un país por parte de una empresa sin presencia física o legal en ese país. Muchas autoridades, reconociendo que bloquear el acceso a los servicios o productos financieros suministrados electrónicamente desde el extranjero puede ser difícil en ausencia de controles de capital, han tratado de establecer un mecanismo de cooperación con el supervisor de los países de origen de los proveedores de productos Fintech.

El uso de memorandos de entendimiento (MoUs, por sus siglas en inglés) específicos de Fintech entre supervisores constituye un método común en todo el mundo. Un paso más ha sido incluir no sólo a los supervisores, sino también a otras autoridades y participantes del mercado en los acuerdos de cooperación bilateral o Fintech bridges. Según un analista, se han firmado 63 acuerdos tipo Fintech bridge, que abarcan la mayoría de las regiones, como se muestra en el siguiente mapa.

53/ European Union. Directive 2014/65/EU. May 2014, in force since early 2018.

54/ HSU, P. and FLÜHMANN, D. Regulating innovation. International Financial Law Review. April 2017.

55/ Bank Negara Malaysia - Financial Technology Enabler Group. FAQ.

56/ See: UK-Australia Fintech Bridge.

GRÁFICA 3: FINTECH *BRIDGES*

Fuente: KAE. Fintech Bridges across the Globe.

La naturaleza intangible de los productos Fintech, el alcance global de las redes de telecomunicaciones y la ausencia de control de capital en la mayoría de los países, subrayan la alta probabilidad de que los usuarios reciban productos Fintech desde fuera de su jurisdicción. Por lo tanto, está claro que las autoridades financieras buscan MoUs específicos de Fintech para acelerar la cooperación de los supervisores del país de origen de dichos proveedores. Al mismo tiempo, reconociendo que la actividad de Fintech trasciende la esfera de los mercados financieros, estas autoridades están tratando de involucrar a otras autoridades en estos acuerdos para asegurar una respuesta unificada e informada ante la prestación transfronteriza de servicios financieros.

7. PRÁCTICAS EN MATERIA DE PLD Y FT

De todos los temas tratados en este capítulo, el enfoque de regulación y supervisión en materia de Prevención de Lavado de Dinero y Financiamiento al Terrorismo (PLD y FT) en el contexto de los productos y empresas de Fintech es el más homogéneo entre las jurisdicciones examinadas. En gran medida, esta uniformidad refleja los esfuerzos que están realizando los organismos internacionales, en particular el Grupo de Acción Financiera Internacional (GAFI),[57] para analizar los desafíos que plantean las Fintech a las prácticas tradicionales de PLD y FT y, a continuación, ajustar sus recomendaciones para abordar las deficiencias que se perciben.

En el análisis de este tema, encontramos que, en varias jurisdicciones, incluso las actividades Fintech fuera del perímetro regulatorio de los supervisores financieros han estado sujetas a obligaciones en materia de PLD y FT por parte de otras autoridades que se beneficiaron de la amplia gama de actividades cubiertas por las legislaciones nacionales en materia de PLD y FT.

Esta práctica se alinea con el enfoque del GAFI hacia Fintech, que identifica tres áreas de preocupación:

- Criptoactivos
- Tecnología de Registro Distribuido (*Distributed Ledger Technology*)
- Identificación Digital

Las empresas e individuos involucrados en criptoactivos, que a veces son reacios a ser regulados, se han visto forzados, cada vez más, a cumplir con regulaciones en materia de PLD y FT similares a las que se aplican en el sector financiero, sin perjuicio de su estatus regulatorio como actores financieros.

La práctica general con respecto a las regulaciones de las firmas de criptoactivos en materia de PLD y FT, es ordenar, como mínimo, procedimientos estrictos de identificación del cliente y verificación de la fuente de los fondos en las plataformas de negociación de critoactivos, en las que se intercambian moneda fiduciaria y criptoactivos, así como exigir a las firmas que operan las plataformas que cumplan con los requisitos para la presentación de informes estandarizados. Muchas jurisdicciones también requieren que las empresas de criptoactivos tengan un encargado de cumplimiento de la legislación.

Con respecto a otras actividades de Fintech, se han identificado prácticas similares. Sin embargo, la tendencia a la reducción de riesgos observada en varias jurisdicciones ha afectado en algunos casos al desarrollo de Fintech.

En su primer informe sobre los resultados del primer *sandbox* regulatorio en el Reino Unido, la Autoridad de Conducta Financiera declaró lo siguiente: "Hemos sido testigos, de primera mano, de la negación de los servicios bancarios en varias empresas de las dos primeras cohortes del *sandbox*. Las dificultades han sido particularmente acentuadas para las empresas que desean aprovechar la DLT, las que desean convertirse en entidades de pago o convertirse en entidades de dinero electrónico (*e-money*). Nos preocupa lo que parecen ser rechazos generales para ciertos tipos de empresas solicitantes. También hay aparentes inconsistencias dentro de los bancos individuales con respecto a cómo aplican sus criterios de evaluación al aprobar el acceso a los servicios bancarios".[58]

57/ GAFI. Fintech & RegTech Initiative.
58/ FCA. Regulatory sandbox lessons learned report. Octubre de 2017.

En varias economías en desarrollo, se identificó que las jurisdicciones examinadas utilizaban una combinación de enfoques basados en el riesgo y proporcionalidad en la regulación de PLD y FT para productos y empresas clave de Fintech vinculados a la inclusión financiera. En estos casos, el supervisor considera que las tecnologías relacionadas con Fintech son una solución a algunas de las afirmaciones expresadas por las instituciones financieras existentes acerca de las debilidades percibidas en los controles de PLD y FT en las nuevas empresas de Fintech, especialmente en las prácticas de incorporación de los clientes y los procesos Conoce a tu Cliente (KYC, por sus siglas en inglés) a distancia. A veces es difícil separar las preocupaciones genuinas, tales como la tendencia general del *de-risking* observada en muchos países en desarrollo, de justificaciones para imponer barreras a otros competidores potenciales.[59]

Una práctica común implementada por los supervisores para evitar restricciones excesivas relacionadas con requerimientos PLD y FT sobre las empresas de Fintech es la introducción de cuentas simplificadas, junto con un proceso KYC simplificado que permite a los agentes llevar a cabo la diligencia debida inicial con respecto a los nuevos clientes y, en algunos casos, la introducción de tecnología de identificación biométrica.[60]

8. CIBERSEGURIDAD

El riesgo de que una institución financiera sea objeto de ataques criminales a través de los canales de comunicación y los centros de procesamiento de datos ha crecido significativamente en los últimos años. Aunque no se trata de una cuestión específica de Fintech, es indudable que Fintech está aumentando la dependencia de los sistemas automatizados y electrónicos en la prestación de servicios financieros. Tanto las nuevas empresas de Fintech como las instituciones financieras tradicionales están expuestas a ataques cibernéticos, ya que es en este punto en cual estos dos grupos de empresas interactúan. Además, "las empresas de Fintech son objetivos cada vez más atractivos y suelen tener menos recursos dedicados a la ciberseguridad, ya que dan prioridad al crecimiento y a la adaptación del producto al mercado".[61]

Esta nueva tendencia ha llevado a las autoridades financieras a adaptar tanto el marco normativo, como sus instrumentos de supervisión, para garantizar que todos los participantes en los mercados financieros mantengan un nivel mínimo de seguridad. La gestión del riesgo de ciberseguridad se considera parte de un proceso más amplio de gestión del riesgo operativo. Como tal, las actividades de evaluación y mitigación incluyen no sólo las actividades dentro de las instituciones reguladas, sino también las actividades de las empresas que prestan servicios electrónicos a las primeras.

La iniciativa del Banco Mundial de recopilar prácticas de regulación y supervisión[62] e investigaciones sobre el tema,[63] ha evidenciado la relevancia que ha adquirido esta cuestión. Estas prácticas de regulación y supervisión incluidas en estos documentos no son específicas de Fintech, aunque está claro que los productos Fintech han motivado algunos desarrollos recientes. Cabe mencionar las siguientes acciones:

En 2016, el Banco de la Reserva de la India emitió una "directiva"[64] para las empresas financieras no bancarias que actúan como "agregadores de cuentas", que se define como " el servicio de recuperación o recopilación (...) de información financiera relativa a sus clientes".[65]

59/ Alliance for Financial Inclusion. Stemming the tide of de-risking through innovative technologies and partnerships. 2016.
60/ Alliance for Financial Inclusion. Proportionality in Practice. Case Studies (Volume 1). Agosto de 2018.
61/ Ng, C. Regulating Fintech: Addressing Challenges in Cybersecurity and Data Privacy. Febrero de 2018.
62/ World Bank. Financial Sector's Cybersecurity: A Regulatory Digest. Octubre de 2017.
63/ Almansi, A.A. Financial sector's cybersecurity: regulations and supervision. Enero de 2018.
64/ Reserve Bank of India. Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions. 2017.
65/ Ídem.

El documento especifica el marco de gestión de riesgos que deben tener estas empresas, así como el mandato de que "adopten un marco de tecnologías de información (IT, por sus siglas en inglés) adecuado e interfaces necesarias para garantizar la seguridad de los flujos de datos desde los proveedores de información financiera hacia sus propios sistemas y hacia los usuarios de la información financiera".[66]

Otro ejemplo de una práctica de ciberseguridad vinculada a Fintech es el esquema de banca abierta (*open banking*) del Reino Unido. Al igual que en el caso anterior, este esquema establece el marco para el intercambio de información financiera entre las instituciones financieras y terceros. Las autoridades británicas han optado por una combinación de regulaciones[67] y estándares. La Entidad de Implementación de Banca Abierta (OBIE, por sus siglas en inglés), una empresa creada por la Autoridad de Competencia y Mercados ha definido el "Estándar OBIE"[68] que incluye métodos de seguridad específicos y herramientas de gestión de riesgos. Los participantes del programa, tanto instituciones financieras como terceros, en su mayoría empresas Fintech, deben obtener una "conformidad y certificación" de la OBIE para convertirse en un programa participante.

En paralelo, la Autoridad de Conducta Financiera (FCA, por sus siglas en inglés) tiene en cuenta la aplicación de los estándares al mismo tiempo que supervisa a los participantes. El supervisor verifica, entre otras cosas, los procedimientos de gestión de incidentes, la idoneidad de las medidas de mitigación y los mecanismos de control implementados. La FCA espera que el "enfoque de las empresas supervisada en materia de gestión del riesgo operativo y de seguridad sea proporcional a su tamaño y naturaleza, alcance, complejidad y nivel de riesgo de su modelo operativo, así como de los servicios de pago que ofrece".[69]

Cabe señalar que estas prácticas cuentan con el apoyo del organismo nacional de ciberseguridad,[70] que presta asistencia técnica y apoyo a la gestión de crisis a personas y organizaciones, incluidas las instituciones financieras. Otro ejemplo de un enfoque de ciberseguridad que combina la reglamentación y el apoyo para aumentar la capacidad de las instituciones financieras de gestionar adecuadamente la ciberseguridad es la Iniciativa para el Fortalecimiento de la Ciberseguridad de la Autoridad Monetaria de Hong Kong (HKMA, por sus siglas en inglés). Este esquema incluye "un marco común de evaluación de riesgos para los bancos de Hong Kong, un programa de formación y certificación profesional que pretende aumentar la oferta de profesionales calificados, y una plataforma para compartir inteligencia cibernética".[71] Al mismo tiempo, la HKMA espera explícitamente que las empresas supervisadas mejoren "su cultura de ciberseguridad dotando al personal de las competencias, conocimientos y el comportamiento apropiados".[72] Aunque la HKMA hace hincapié en que este no es un requisito obligatorio, encaja con el enfoque general de supervisión de la gestión de riesgos de la banca electrónica.[73]

La Autoridad Monetaria de Singapur (MAS, por sus siglas en inglés) ha implementado requisitos similares con respecto a las competencias en ciberseguridad por parte de los miembros de la junta directiva y el personal. El documento normativo establece que el supervisor "espera que la Junta se mantenga regularmente informada de los avances tecnológicos más destacados y de los riesgos cibernéticos",[74] lo cual representa un requisito muy adecuado para las instituciones financieras tradicionales que trabajan con empresas Fintech o que implementan productos Fintech.

América Latina y el Caribe no son inmunes a los ciberataques. Un informe de la Organización de los Estados Americanos (OAS, por sus siglas en inglés) indica que al menos 9 de cada 10 entidades bancarias sufrieron incidentes cibernéticos durante 2017; el 37% de los bancos de la región fueron víctimas de ataques exitosos, y el 39% de los incidentes no fueron reportados.

66/ Reserve Bank of India. Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions. 2017.

67/ UK Treasury. The Payment Services Regulations. 2017.

68/ Open Banking. Open Banking Standard.

69/ FCA. Payment Services and Electronic Money – Our Approach. Diciembre de 2018.

70/ National Cybersecurity Centre.

71/ HKMA. Guide to Enhanced Competency Framework on Cybersecurity. Enero de 2019.

72/ Idem.

73/ HKMA. Supervisory Policy Manual Risk Management of E-banking. Septiembre de 2015.

74/ MAS. Circular on Technology risk and cyber-security training for Board. October 2015.

Según el informe, la subestimación es particularmente frecuente entre los bancos medianos y pequeños. El informe también indica que el costo promedio para que una institución financiera se recupere de un incidente de ciberseguridad es de $1.9 millones de dólares, aunque la cifra para los grandes bancos es mucho mayor, es decir, $5.3 millones de dólares. En cambio, los gastos en ciberseguridad son relativamente menores en proporción al EBITDA que los observados en otras regiones. El informe destaca que el 62% de los bancos encuestados indicaron que sus gastos en protección de la ciberseguridad aumentaron con respecto al año anterior debido a los requisitos reglamentarios.

Estos resultados contrastan con la importante proporción de clientes que utilizan regularmente los canales digitales para realizar transacciones financieras, el 88%. Cabe destacar que el 27% de los usuarios encuestados manifestaron que la confidencialidad, integridad o disponibilidad de su información o de sus recursos financieros estaba comprometida por su banco, con el 43% de ellos sufriendo pérdidas económicas como consecuencia de ello.

El informe concluye recomendando que las autoridades "emitan directrices, recomendaciones e instrucciones, según sea el caso, derivadas de la revisión periódica de las buenas prácticas y/o estándares internacionales aplicables en materia de seguridad digital, así como del marco regulatorio internacional aplicable al sector bancario, y, en su caso, emitan los instrumentos jurídicos necesarios para su aplicación".[75]

No es de extrañar que una serie de autoridades financieras de América Latina y el Caribe, impulsadas por ciberataques de alto perfil, hayan implementado acciones de ciberseguridad sobre todo en forma de regulación. Este fue el caso de México, donde el supervisor financiero, la Comisión Nacional Bancaria y de Valores (CNBV), renovó sus regulaciones después de un ciberataque de alto perfil a los bancos. Los cambios se aplican a las instituciones de crédito,[76] incluidas las dos "instituciones de tecnología financiera"[77] creadas por la "Ley Fintech" de 2018, aunque se hace hincapié en las "instituciones financieras colectivas", que abarcan tanto los préstamos *peer-to-peer* como ciertos tipos de financiamiento colectivo (*crowdfunding*).

Entre los cambios más notables se encuentra la obligación de nombrar a un "Director de Seguridad de la Información", una prueba de intrusión obligatoria bianual realizada por una empresa especializada independiente, junto con pruebas internas trimestrales, y la notificación al supervisor de cualquier "incidente de seguridad " en un plazo de 60 minutos a partir del momento en que la institución toma conocimiento de éste. Además, la regulación reformada amplió el marco de gestión del riesgo operacional, introduciendo un nuevo plan maestro anual de seguridad y funciones específicas relacionadas con la ciberseguridad para el máximo ejecutivo de la institución. La CNBV emitió por separado estas normas de ciberseguridad para los prestamistas financieros tradicionales y las más recientes empresas Fintech. Aunque ambas versiones contienen requisitos similares, las regulaciones para las instituciones financieras tradicionales son más específicas.

El supervisor financiero de Chile también amplió sus directrices de gestión de riesgos para incluir la ciberseguridad. El supervisor espera que la dirección y el consejo "detecten, investiguen y generen regularmente acciones para mitigar el impacto de estos eventos y salvaguardar la confidencialidad, disponibilidad e integridad de sus activos de información". Además, las directrices establecen requisitos específicos para notificar al supervisor y a los usuarios afectados, e impone un "deber de los bancos para compartir información sobre ataques relacionados con la ciberseguridad."[79]

Ambas regulaciones latinoamericanas, en comparación con las prácticas de ciberseguridad identificadas en otros lugares, son mucho más prescriptivas, alcanzando un nivel de detalle ausente en las directrices mencionadas en Hong Kong o en el Reino Unido.

75/ OAS. State of Cybersecurity in the Banking Sector in Latin America and the Caribbean. 2018.

76/ CNBV. Disposiciones de carácter general aplicables a las instituciones de crédito. Reformado en noviembre de 2018.

77/ CNBV. Disposiciones de carácter general aplicables a las instituciones de tecnología financiera. Reformado en marzo de 2019.

78/ Superintendencia de Bancos e Instituciones Financieras Chile. Recopilación actualizada de normas. Capítulo 1-13. 2013.

79/ Superintendencia de Bancos e Instituciones Financieras Chile. Recopilación actualizada de normas. Capítulo 20-8. 2018.

III. PRÁCTICAS RELATIVAS A PRODUCTOS FINTECH ESPECÍFICOS

1. DINERO ELECTRÓNICO (*E-MONEY*)

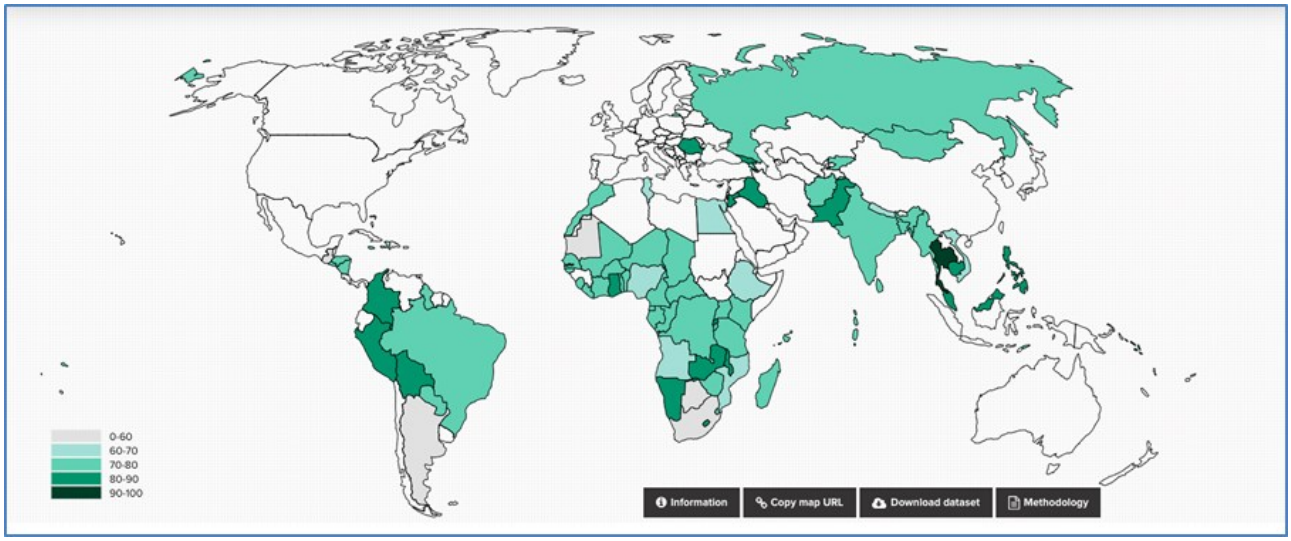
Entre los productos Fintech, los que implican emisión de dinero electrónico (*e-money*), pagos móviles y almacenamiento de valor por parte de entidades no bancarias han sido regulados y supervisados desde hace ya mucho tiempo. Por lo tanto, no es sorprendente que ya exista un cuerpo sustancial de buenas prácticas estrechamente vigiladas por las autoridades a nivel mundial. Para los fines de esta sección, el dinero electrónico (*e-money*) incluye los siguientes productos de Fintech: banca por teléfono móvil, integración operadora de telefonía celular e institución financiera, monederos electrónicos en dispositivos móviles, tarjetas prepagadas virtuales, pagos móviles cooperación directa banco-operador de telefonía celular, facturación directa a móviles y pagos móviles basados en mensajería de texto.

Una fuente de convergencia regulatoria en esta área ha sido el Grupo de Trabajo de Servicios Financieros Digitales, el cual ha comprometido a los supervisores financieros de distintos países con un objetivo de inclusión financiera. Este grupo de trabajo declara que uno de sus objetivos clave es "estimular el debate y el aprendizaje sobre nuevos enfoques y buenas prácticas en materia de regulación de los DFS [*Digital Fianancial Services*]".[80] La presencia de grandes operadores de telefonía móvil (MNOs, por sus siglas en inglés) internacionales también ha contribuido a esta armonización, ya que son los principales proveedores de estos productos en muchas economías en desarrollo.

El organismo internacional de comercio de los MNOs, el Sistema Global para las Comunicaciones Móviles (GSMA, por sus siglas en inglés), ha estado promoviendo un enfoque internacional común para la regulación del dinero electrónico (*e-money*). El GSMA elaboró un "Índice Regulatorio de Dinero Electrónico (*e-money*) [que] mide los factores reguladores que facilitan la adopción del dinero electrónico (*e-money*)".[81] El Gráfico 4 muestra los resultados del índice para las 80 jurisdicciones que fueron foco del estudio.[82]

80/ Digital Financial Services Working Group. Fact sheet. Julio de 2018.
81/ GSMA. Mobile Money Regulatory Index – Methodology. Septiembre de 2018.
82/ No se analizaron los países de color blanco, a pesar de que muchos de ellos cuentan con regulaciones sobre el dinero electrónico (*e-money*), como en el caso de México (Gráfica 4).

GRÁFICA 4: ÍNDICE REGULATORIO DE DINERO MÓVIL



Fuente: GSMA. Regulatory Index. Consultado en Abril de 2019.

Al combinar la información obtenida directamente de las jurisdicciones encuestadas con la base de datos del GSMA sobre la regulación del dinero electrónico (*e-money*), surgieron claramente un conjunto de prácticas.

Entidades no financieras pueden prestar servicios de dinero electrónico (*e-money)* directamente o a través de una subsidiaria.

Solo unos pocos países permiten a los proveedores participar en otras actividades financieras o no financieras. Sin embargo, cabe señalar que, en Kenia, cuna del dinero electrónico (*e-money*) masivo, el proveedor (*Safaricom*) está ofreciendo otros productos financieros en alianzas estratégicas con bancos regulados,[83] mientras que en la Unión Europea algunas empresas Fintech que comenzaron como proveedores de dinero electrónico (*e-money*) han pasado a convertirse en bancos comerciales de pleno derecho, como *Wirecard Bank,* en Alemania, y *Starling Bank*, en el Reino Unido.

Para participar en servicios de dinero electrónico (*e-money*), los proveedores requieren una autorización formal con un conjunto de requisitos diferentes y menos estrictos que los que se aplican a las instituciones financieras tradicionales.

Tras la exitosa experiencia del servicio de dinero móvil de "M-Pesa" de *Safaricom* en Kenia, casi todas las jurisdicciones encuestadas han creado una licencia para proveedores de dinero electrónico (*e-money*). Cabe señalar que la Unión Europea estableció un requisito de capital inicial de 1 millón de euros en su primera directiva sobre el dinero electrónico (*e-money)*.[84] En 2009, la UE redujo el requisito a €350,000 y en 2015, introdujo un esquema escalonado con un requisito de capital inicial mínimo de sólo €50,000 para los "pequeños" proveedores.[85]

Los fondos de los clientes se separan de los fondos del proveedor. En la mayoría de los casos, los fondos se mantienen en una institución financiera regulada como depósitos o en fideicomisos.

83/ CGAP. Top 10 Things to Know About M-Shwari. Abril de 2015.
84/ European Union. Directive 2000/46/EC. Septiembre de 2000.
85/ European Union (2015).

Algunas jurisdicciones requieren que los proveedores diversifiquen los fondos de los clientes, en varias instituciones y/o instrumentos. Un ejemplo es Kenia, que exige que "un proveedor de servicios de pago (...) emplee estrategias apropiadas de mitigación de riesgos para garantizar que los fondos que se mantienen en el Fondo Fiduciario estén suficientemente diversificados.[86]

El marco de protección de consumidores de servicios financieros cubre los servicios de dinero electrónico (*e-money*).

Además de la protección contra la insolvencia del proveedor cubierta por la segregación de fondos, casi todas las jurisdicciones han ampliado el perímetro del marco de protección del consumidor para incluir los servicios de dinero electrónico (*e-money*) con licencia. Esto permite procedimientos y derechos similares con respecto a la mala conducta financiera. Sin embargo, algunos estudios han detectado que "los consumidores no están seguros de a quién dirigirse si tienen quejas relacionadas con el dinero electrónico (*e-money*), especialmente cuando este servicio involucra al MNO".[87]

Los proveedores de dinero electrónico (*e-money*) están sujetos a las regulaciones y supervisión en materia de PLD y FT.

En todas las jurisdicciones analizadas, los proveedores de dinero electrónico (*e-money*) deben cumplir con las regulaciones en materia de PLD y FT. Dependiendo del marco jurídico específico y del acuerdo de supervisión, el cumplimiento puede ser verificado por diferentes autoridades. Este es el caso de EE.UU., donde los proveedores de servicios de dinero electrónico (*e-money*) pueden ser supervisados por autoridades federales o estatales. En algunos estados, las "empresas de servicios monetarios" (MSBs por sus siglas en inglés) no están reguladas. Esta situación se refleja en una evaluación del GAFI, que indica que "el marco regulatorio y de supervisión en EE.UU. es altamente complejo y multifacético, con la participación de una serie de autoridades tanto a nivel federal como estatal".[88] No obstante, el informe reconoce que "el proceso de coordinación de los controles de las MSBs entre la Red de Ejecución de Delitos Financieros (FinCEN, por sus siglas en inglés), el Servicio de Impuestos Internos de EE.UU (IRS SBSE, por sus siglas en inglés) y los Estados está evolucionando positivamente. La FinCEN y el IRS SBSE han tomado iniciativas para abordar a los remitentes de dinero no registrados a través de acciones de divulgación y aplicación de la ley que han sido eficaces.[89]

La regulación permite a los proveedores de dinero electrónico (*e-money*) utilizar agentes para realizar transacciones. El proveedor debe informar y, en la mayoría de los casos, buscar la autorización del supervisor antes de usar un agente. El proveedor de dinero electrónico (*e-money*) debe aceptar asumir cualquier responsabilidad por las pérdidas que los agentes puedan ocasionar a los clientes.

Algunas jurisdicciones, por ejemplo, Bangladesh,[90] restringen la gama de actividades que pueden realizar los agentes, como el ingreso y el egreso de efectivo. En otros casos, como el de Ghana,[91] los agentes pueden inscribir nuevos clientes y realizar procesos básicos de KYC, a menudo dentro de un esquema de agentes escalonados.

2. PRÉSTAMOS *PEER-TO-PEER*, FINANCIAMIENTO COLECTIVO (*CROWDFUNDING*) Y OTROS PRODUCTOS DE INTERMEDIACIÓN FINANCIERA

Los productos Fintech que implican intermediación financiera son, después de los productos relacionados con los pagos, el terreno más fértil para la actividad reguladora y supervisora a nivel mundial, si bien con un menor grado de consenso entre las autoridades.

86/ Kenia National Treasury. The National Payment System Regulations. 2014.

87/ United Nations Conference on Trade and Development. Mobile Money for Business Development in the East Africa Community. 2012.

88/ GAFI. AML/CFT measures - United States - Mutual Evaluation Report. Diciembre de 2016.

89/ Ídem.

90/ Bangladesh Bank. Bangladesh Mobile Financial Services (MFS) Regulations. Julio de 2018.

91/ Bank of Ghana. Agent Guidelines. Julio de 2015.

El conjunto de productos Fintech revisados en esta sección son los siguientes: préstamos con fondos propios a consumidores y empresas; préstamos *peer-to-peer* a consumidores y empresas y una serie de servicios de financiamiento colectivo (crowdfunding), incluyendo los accionarios (*equity*), bienes raíces, donaciones y recompensas.

En primer lugar, es importante señalar que, en la mayoría de las jurisdicciones, la donación y el financiamiento colectivo (*crowdfunding*) de recompensas rara vez están regulados, ya que no se consideran productos financieros siempre y cuando la persona que proporciona los fondos no espere un retorno monetario.

Sin embargo, la FCA del Reino Unido somete ambos tipos de actividades de financiamiento colectivo (*crowdfunding*) a su regulación de pagos, incluyendo los requerimientos de normas en materia de PLD y FT.[92] Del mismo modo, Suiza requiere que una plataforma de financiamiento colectivo (*crowdfunding*), independientemente de su objetivo, obtenga una licencia bancaria si "acepta fondos sobre una base comercial y, en lugar de remitirlos al desarrollador del proyecto en un plazo de 60 días (...), los retiene durante algún tiempo [y] siempre y cuando los fondos aceptados para el redireccionamiento no excedan un millón de francos suizos".[93]

Otra demarcación importante se refiere a las plataformas de préstamo en balance, que por lo general no se regulan o se consideran como otras compañías financieras tradicionales que no captan depósitos.

El tratamiento reglamentario de los demás productos (préstamos *peer-to-peer* y financiamiento colectivo (*crowdfunding*) de acciones (*equity*)/bienes raíces) es menos claro. Un estudio de la Organización para la Cooperación y el Desarrollo Económicos (OECD, por sus siglas en inglés) señala que "diferentes países han elegido diferentes enfoques regulatorios para las plataformas de financiamiento colectivo (*crowdfunding*) basadas en préstamos. Varios países han establecido una legislación específica para regular explícitamente las plataformas de financiamiento colectivo (*crowdfunding*) basadas en préstamos (Francia, Reino Unido e Israel). Otros países han introducido una regulación de la financiación en régimen de financiamiento colectivo (*crowdfunding*) que se aplica tanto a la financiación en régimen de préstamo como a la financiación en régimen de inversión, o bien no parece distinguir entre los dos modelos de negocio (Austria, Bélgica, Finlandia, México y Portugal). La propuesta de la UE entra en esta última categoría".[94]

Estos enfoques diferenciados probablemente se derivan de las prioridades y realidades del mercado de los reguladores. Como señaló un comentarista en 2013, "es interesante ver que mientras los reguladores de EE.UU. han estado creando una regulación en torno al financiamiento colectivo (*crowdfunding*) accionario como parte de la Ley *Jumpstart Our Business Startups* (JOBS Act), los reguladores del Reino Unido han estado diseñando simultáneamente una regulación en torno a los préstamos *peer-to-peer*".[95] En el caso del Reino Unido, el énfasis en los préstamos *peer-to-peer* estaba indudablemente relacionado con la retirada de los bancos tradicionales de los préstamos a las PyME tras la crisis bancaria, mientras que en EE.UU. el papel de los mercados de capitales en la financiación de las empresas era determinante para el interés inicial sobre el financiamiento colectivo (*crowdfunding*) de acciones (*equity*).

A pesar de las diferencias entre el micro financiamiento colectivo (*crowdfunding*) de capital y los préstamos *peer-to-peer*, una práctica común es exigir a los proveedores de plataformas que adviertan a los clientes que los rendimientos no están garantizados y que podrían perder su inversión si el prestatario o la empresa que recibe la inversión fracasa. Además, los proveedores deben declarar claramente que los fondos invertidos no están protegidos por un esquema de garantía de depósitos.

92/ FCA. Crowdfunding and authorisation. Agosto de 2017.
93/ FINMA. Crowdfunding. Agosto de 2017.
94/ HAVRYLCHYK, O. Regulatory Framework for the Loan-Based Crowdfunding Platforms. Noviembre de 2018.
95/ RENTON, P. New UK Regulation Provides a Best Practices Template for P2P Lenders. Octubre de 2013.

Este requisito se aplica incluso en los casos en que el proveedor establece un "fondo de provisión" para cubrir las pérdidas esperadas.

En la mayoría de las regulaciones tanto para los préstamos *peer-to-peer* como para el financiamiento colectivo (*crowdfunding*) de acciones, "la regulación a menudo especifica que el dinero de los clientes debe mantenerse en una cuenta especial de fideicomiso (i.e. Israel y México), o en la mayoría de los países las plataformas ni siquiera tienen el derecho de manejar el dinero de los clientes y deben depender de una institución de pago u obtener una licencia de una institución de pago para hacerlo.[96]

En lo que se refiere específicamente a los préstamos *peer-to-peer*, la regulación y supervisión sigue siendo un trabajo en curso, y algunas autoridades están reelaborando sus reglamentos. En particular, la FCA del Reino Unido está desarrollando actualmente su segunda generación de reglamentaciones para subsanar las deficiencias de su primer régimen establecido en 2014. Un área de especial interés es garantizar que el fracaso de las plataformas de préstamos *peer-to-peer* no perjudique a los clientes. Una revisión del marco regulatorio indicó que "hasta ahora, las pérdidas y los impagos en el sector de préstamos *peer-to-peer* han sido bajos. Sin embargo, es importante reconocer que el sector es todavía relativamente nuevo y que no ha pasado por un ciclo económico completo. Cuando las condiciones económicas se hacen más difíciles, las pérdidas en préstamos e inversiones pueden aumentar. El sector aún no ha experimentado un ajuste de este tipo y, por lo tanto, la resiliencia de los modelos de negocio de préstamos *peer-to-peer* observados sigue siendo relativamente incierta."[97]

Esta preocupación llevó a la FCA a proponer que se reforzara el mandato actual para garantizar que los préstamos existentes puedan seguir gestionándose en caso de fallo de la plataforma. Específicamente, la FCA propone un "manual de resolución de préstamos *peer-to-peer*" con un contenido similar al de los llamados "testamentos de voluntad anticipada" requeridos para las instituciones financieras sistémicas importantes:

- ""personal crítico y sus respectivos roles
- premisas fundamentales
- sistemas de tecnología de la información
- sistemas de mantenimiento de registros, incluida la forma en que se organizan los registros
- todas las cuentas bancarias y facilidades de pago relevantes
- todos los actores relevantes fuera de la plataforma y sus respectivas funciones, incluidos los proveedores de servicios de tercerización (*outsourcing*)
- toda la documentación jurídica pertinente, incluidos los contratos de clientes, servicios y proveedores
- un diagrama de estructura de grupo
- las medidas que deberían aplicarse en el marco de los acuerdos de liquidación
- los términos de los contratos en los que pueda ser necesario apoyarse y
- la forma en que los sistemas de la plataforma pueden producir el detalle especificado con respecto a la divulgación continua.[98]

Del mismo modo, en Francia, las plataformas están obligadas a firmar un contrato con una entidad de pago externa para garantizar la continuidad del negocio."[99]

Otra área de preocupación es la transparencia informativa y los conflictos de interés en el proceso de selección de los préstamos que se ofrecen a los clientes. En algunos países, los esquemas *peer-to-peer* han demostrado ser un terreno fértil para esquemas fraudulentos prohibidos durante mucho tiempo en la banca tradicional.

96/ HAVRYLCHYK (2018).

97/ FCA. Loan-based ('peer-to-peer') and investment-based crowdfunding platforms: Feedback on our post-implementation review and proposed changes to the regulatory framework. Julio de 2018.

98/ Ídem.

99/ France. Ordinance No 2014-559 relating to crowdfunding. Mayo de 2014.

El fracaso de una gran empresa de préstamos *peer-to-peer* en China en 2016, Ezubao, afectó a casi un millón de clientes con pérdidas que superaron los $9,200 millones de dólares.[100] Tres años más tarde, otra ola de fracasos afectó a más de 380 plataformas de préstamos *peer-to-peer* en ese país.[101]

En EE.UU., la Comisión Federal de Comercio (FTC, por sus siglas en inglés), el organismo de control no financiero de protección al consumidor- detectó un incidente diferente que afectaba a su mayor plataforma *peer-to-peer* y acusó a la plataforma "de realizar promesas falsas a los consumidores respecto a que recibirían un préstamo sin "comisiones ocultas", cuando, en realidad, la empresa dedujo de los préstamos centenares, o incluso millares de dólares en concepto de comisiones ocultas por adelantado".[102]

Es comprensible que estos acontecimientos hayan conducido a un fortalecimiento de las regulaciones y las políticas de supervisión en China, EE.UU. y otros países.

La FCA señaló que la manipulación de la información provocada por los conflictos de interés puede adoptar formas sutiles y enumeró los siguientes esquemas que ha observado:

- "acuerdos de comisiones poco transparentes entre los prestatarios y la plataforma
- estructuras de grupo que generan estratos adicionales e invisibles de ganancias para la propia plataforma; por ejemplo, una empresa del mismo grupo como plataforma puede pre financiar préstamos y venderlos a la plataforma a través de novación, pero la empresa conserva una acción en cada préstamo y el precio del préstamo se fijará a un tipo de interés más alto que el recibido por los inversores minoristas
- plataformas que permiten a los empleados o a los miembros de la familia realizar transacciones en el mercado secundario, creando el riesgo de que tengan acceso a información que no está disponible para todos los inversores y que puede beneficiarles (...)
- plataformas (a veces a través de las empresas matrices) que mantienen *skin in the game* (es decir, compran una parte de los préstamos que ayudan a originar); aunque esto puede conducir a un mejor estándar de debida diligencia, también puede dar lugar a conflictos de interés si son capaces de utilizar el mercado secundario para vender anticipadamente (posiblemente sobre la base de un mayor acceso a información), en lugar de mantenerse hasta el vencimiento
- plataformas cuyos directores han facilitado préstamos para negocios vinculados, pero no han declarado estas conexiones a los inversores
- la transferencia de préstamos de un cliente a otro a un precio inadecuado
- premisas fundamentales"[103]

Cabe señalar que la FCA y muchas otras autoridades permiten e incluso alientan a los proveedores de préstamos *peer-to-peer* a participar en el mercado de préstamos minoristas; la Unión Europea en su propuesta de reglamento de préstamos *peer-to-peer*, lo prohíbe.

Las autoridades también han tratado de impedir que los proveedores de servicios de préstamos *peer-to-peer* atiendan a un segmento específico del mercado, ya sean inversores o prestatarios.

Con pocas excepciones, las regulaciones para préstamos *peer-to-peer* establecen un monto máximo para los préstamos originados, expresando la preferencia de las autoridades por destinar este producto a la financiación de las PyME. El límite máximo varía mucho de una jurisdicción a otra, pero no supera los $6 millones de dólares.

100/ Reuters. Leader of China's $9 billion Ezubao online scam gets life; 26 jailed. Septiembre de 2017.

101/ Associated Press. China seizes $1.5 billion in online lending crack-down. Febrero de 2019.

102/ FTC. FTC Charges Lending Club with Deceiving Consumers. Abril de 2018.

103/ FCA (Julio 2008).

Por otro lado, la FCA propone introducir restricciones de comercialización que limitarían las promociones financieras directas a los inversores que:

- "están certificados o se auto certifican como inversionistas sofisticados;
- están certificados como inversores de alto valor neto;
- confirman, antes de recibir una promoción específica, que recibirán asesoramiento en materia de inversiones o servicios de gestión de inversiones regulados de una persona autorizada; o bien
- certifican que no invertirán más del 10% de su cartera neta de inversiones en acuerdos de préstamos *peer-to-peer*"[104]

La FCA reconoce que esta restricción forzaría un cambio drástico en el grupo objetivo de muchas plataformas de préstamos *peer-to-peer*, aunque alinearía la regulación del Reino Unido con la regulación actual en los EE.UU., que en gran medida es la misma que la que se aplica a las inversiones.

En lo que respecta a las prácticas de financiamiento colectivo (*crowdfunding*) de acciones (*equity*), la mayoría de las autoridades reconocen que este producto de Fintech es intrínsecamente más arriesgado que los préstamos *peer-to-peer* y otros tipos de financiación colectiva. Al mismo tiempo, la reducción de la financiación de las PyME por parte de los bancos, así como la creciente toma de conciencia del riesgo entre las fuentes tradicionales de financiación para la creación de empresas tras la crisis financiera mundial de 2008-09, han creado un "déficit de capital de crecimiento".[105] Por lo tanto, las autoridades están buscando mecanismos de financiación innovadores para restablecer la financiación de estos sectores. La financiación colectiva (*crowdfunding*) de acciones (*equity*) se considera un posible complemento a otras iniciativas. Por ejemplo, en EE.UU., el *JOBS Act* creó una exención bajo las leyes federales de valores para que el financiamiento colectivo (*crowdfunding*) pueda ser utilizado para ofrecer y vender valores al público en general".[106] En Europa, Australia y Japón se han llevado a cabo iniciativas gubernamentales similares.

La regulación de micro financiamiento colectivo de capital es generalmente equivalente a la que se aplica a la inversión minorista, con requisitos menos estrictos para permitir que las empresas de nueva creación y empresas que no cotizan en la bolsa obtengan capital a través de estas plataformas. El producto está sujeto a las mismas normas que otras empresas de valores con respecto a la divulgación de las condiciones financieras de la empresa emisora, los principales riesgos, el manejo del dinero del cliente, el requisito de que los inversores deben tener experiencia en inversiones, y la adecuación en la gestión de riesgos de la plataforma.

3. CRIPTOACTIVOS

Las prácticas de las autoridades financieras con respecto a los criptoactivos, como ya se ha mencionado, han sido muy divergentes, e incluso han adoptado puntos de vista opuestos en algunos aspectos. Además, las autoridades incluso utilizan palabras diferentes para identificar dichas prácticas. "Algunos de los términos utilizados por los países para referirse a la criptomoneda incluyen moneda digital (Argentina, Tailandia y Australia), bienes virtuales (Canadá, China y Taiwán), cripto-token (Alemania), token de pago (Suiza), moneda cibernética (Italia y Líbano), moneda electrónica (Colombia y Líbano) y activos virtuales (Honduras y México)".[107]

La ausencia de un término común se reflejó incluso en un documento sobre Fintech[108] elaborado por el BCBS, en el que las "criptomonedas virtuales", las "criptomonedas digitales" y las "criptomonedas" se refieren a la misma clase de activos. Un año más tarde, el BCBS optó por utilizar en su lugar el término "criptoactivos", lo que refleja su "opinión de que estos activos no ofrecen de forma fiable las funciones estándar del dinero y no son seguros como medio de cambio o almacenamiento de valor".[109]

104/ FCA (Julio 2008).
105/ OECD. New Approaches to SME and Entrepreneurship Financing: Broadening the Range of Instruments. Febrero de 2015.
106/ US Securities and Exchanges Commission. Spotlight on Crowdfunding. Febrero de 2019.
107/ US Library of the Congress. Regulation of Cryptocurrency Around the World. Junio de 2018.
108/ BCBS. Sound practices: Implications of Fintech developments for banks and bank supervisors. Febrero de 2018.
109/ BCBS. Statement on crypto-assets. Marzo de 2019.

Esta discrepancia refleja la novedad de los productos, la falta de claridad en cuanto a su naturaleza, la reticencia inicial de los individuos y las empresas involucradas en criptoactivos a comunicarse con las autoridades y la reticencia de las instituciones financieras reguladas a comprometerse con cualquier cosa etiquetada con el prefijo "cripto".

Mientras las transacciones con criptoactivos eran insignificantes y se limitaban a un pequeño grupo de personas, las autoridades consideraron que cualquier medida relativa a los criptoactivos no ameritaba que se les prestara atención. Cabe recordar que el primer criptoactivo, Bitcoin, apareció hace diez años, justo cuando la crisis financiera mundial exigía la atención de los supervisores de todo el mundo al sector financiero.

Fue sólo en 2013, cuando un aumento sostenido y acelerado del valor de los criptoactivos comenzó a atraer compradores más allá del grupo inicial de personas comprometidas, que las autoridades comenzaron a mirar hacia este nuevo mundo.

Los primeros pasos fueron tentativos y orientados a detener el uso de criptoactivos como mecanismo para eludir las regulaciones en materia de PLD y FT y las sanciones financieras. La autoridad de aplicación de la PLD y FT en los Estados Unidos, la Red de Control de Delitos Financieros (FinCEN, por sus siglas en inglés), declaró que "un administrador o cambista que (1) acepte y transmita una divisa virtual convertible o (2) compre o venda una divisa virtual convertible por cualquier razón, debe considerarse como un transmisor de dinero de acuerdo con las regulaciones de la FinCEN".[110]

Desde esta acción de supervisión inicial, muchas jurisdicciones han emitido regulaciones o políticas, o han llevado a cabo acciones de observancia con respecto a los criptoactivos, sus intermediarios o usuarios. La compilación de las normas sobre criptoactivos de la Biblioteca del Congreso de los Estados Unidos que abarca 130 jurisdicciones, constituye un recurso útil para identificar prácticas sobre este tema.

Ese informe y la confirmación directa en los sitios web de las autoridades, revelan algunas tendencias comunes. Tras los debates de finales de 2017, los bancos centrales del G20 comenzaron a emitir declaraciones de redacción similar, a las que otros países se sumaron rápidamente en un raro ejemplo de convergencia de políticas sobre criptoactivos. Por lo tanto, estas declaraciones se consideran una práctica general.

Más allá de esta afirmación, las prácticas difieren considerablemente, como muestra el siguiente cuadro.

La mayoría de las jurisdicciones advierten a sus ciudadanos que los criptoactivos no son monedas de curso legal, no están respaldados por ninguna autoridad o institución financiera y son inversiones altamente especulativas.

110/ FinCEN. Guidance FIN-2013-G0001. Marzo de 2013.

TABLA 3: REGULACIÓN Y SUPERVISION DE CRIPTOACTIVOS: CONTRASTE DE PRÁCTICAS

Utilización de criptoactivos por el público en general en transacciones o como inversión	Prohibido: Ecuador, Bolivia, Argelia, Egipto	Explícitamente permitido: Suiza (algunos cantones), Malta, Gibraltar
Uso de criptoactivos por parte de las instituciones financieras	Prohibido: India, Pakistán, Nepal	Explícitamente permitido: México, Japón, Isla de Man
Ofertas iniciales de moneda	Prohibido: China, Pakistán	Regulado como oferta de valores: Suiza, EE.UU., Gibraltar, Canadá
Cambio de criptoactivos	Prohibido: China, Namibia	Regulado o registrado por el supervisor financiero: Japón, Corea del Sur, Australia, Filipinas

Fuente: Biblioteca del Congreso de los Estados Unidos (2018) e información recopilada por el autor.

La tabla muestra los extremos de la gama de prácticas en jurisdicciones representativas. Para cada área, hay un rango de prácticas entre esas posiciones extremas. Al igual que con otros productos de Fintech, este es un tema en constante evolución, que probablemente se volverá más complejo a medida que los bancos centrales lancen sus propias monedas digitales. La Biblioteca del Congreso de los Estados Unidos enumera cinco jurisdicciones, dos de las cuales son miembros de la ASBA,[111] que han lanzado o están probando monedas digitales nacionales.

Un tema relacionado con los criptoactivos es la tecnología que sustenta la mayoría de ellos: la Tecnología de Registro Distribuido (DLT, por sus siglas en inglés). Muchas instituciones financieras, bancos centrales y otras autoridades financieras están estudiando activamente los posibles usos de la DLT para hacer que las transacciones financieras sean más baratas y seguras. Sin embargo, hay poca evidencia de regulaciones o prácticas de supervisión con respecto a la DLT, en parte porque hay muy pocos servicios o productos financieros que utilicen esa tecnología. Sólo dos jurisdicciones tienen regulaciones específicas: Gibraltar y Malta.

La Comisión de Servicios Financieros de Gibraltar (GFSC, por sus siglas en inglés) reguló "el uso de Tecnología de Registro Distribuido a través de los negocios para almacenar o transmitir el valor perteneciente a otros, que debe ser regulado como una actividad controlada en virtud de la Ley de Servicios Financieros (Ley de Inversión y Servicios Fiduciarios)".[112] La norma crea un nuevo tipo de empresa de servicios financieros con licencia, el proveedor de DLT, y detalla nueve principios reguladores a los que los proveedores de DLT deben adherirse, reproduciendo en la mayoría de los casos los principios de alto nivel para la gestión de las instituciones financieras.

Malta, por otra parte, adoptó un enfoque totalmente diferente. El país aprobó dos leyes: una crea la Autoridad de Innovación Digital de Malta (*Malta Digital Innovation Authority*)[113] como la organización encargada de conceder licencias, regular y supervisar a los "proveedores de servicios de tecnología innovadora", que se definen en la segunda ley.[114] Aunque ambas leyes se centran en la tecnología DLT y otras técnicas afines, como los contratos inteligentes, pueden incluirse otras nuevas tecnologías. Cabe señalar que no hay referencias a los servicios financieros en ninguna de las dos leyes, aparte del requisito de coordinar con la Autoridad de Servicios Financieros de Malta y otras autoridades sobre cuestiones que van más allá de las meramente tecnológicas.

4. BANCA VIRTUAL

La HKMA define este tipo de institución financiera como "un banco que presta principalmente servicios de banca minorista a través de Internet u otras formas de canales electrónicos en lugar de utilizar sucursales físicas".[115]

Como institución financiera a la que se permite realizar toda la gama de actividades, como cualquier otro banco tradicional, en principio, debería estar regulada y supervisada como tal. De hecho, la mayoría de los bancos tradicionales ofrecen una proporción significativa de sus servicios minoristas a través de canales electrónicos, y la mayoría de los reglamentos ya prevén este canal de entrega.

Sin embargo, un pequeño número de autoridades han optado por adaptar sus enfoques de regulación y supervisión para abordar cuestiones exclusivas de la banca virtual. En las tres jurisdicciones con prácticas bancarias virtuales específicas -Hong Kong, Corea del Sur y la Unión Europea- la justificación ha sido fomentar la autorización de nuevos competidores en sus mercados. Por lo tanto, las regulaciones y políticas de supervisión se relacionan principalmente con el proceso de autorización inicial.

111/ El Banco Central del Caribe Oriental y el gobierno venezolano.
112/ GFSC. Financial Services (Distributed Ledger Technology Providers) Regulations. Octubre de 2017.
113/ Malta Parliament. Malta Digital Innovation Authority Act. Julio de 2018.
114/ Malta Parliament. Innovative Technology Arrangements and Services Act. Noviembre de 2018.
115/ HKMA. Banking Ordinance Authorization of Virtual Banks. Junio de 2018.

En los casos de Hong Kong y Corea del Sur, los reguladores han intentado flexibilizar el proceso de concesión de licencias para eliminar las barreras que impiden a las empresas no financieras convertirse en accionistas significativos de nuevos bancos virtuales. En el caso de Corea del Sur, una nueva ley[116] permite a las empresas no financieras poseer hasta un 34% de un banco que opera exclusivamente por Internet, en lugar del máximo estándar del 4%. La HKMA también flexibilizó el requisito de la política estándar de que sólo los bancos pueden poseer más del 50% del capital de un banco constituido en Hong Kong, aceptando que las empresas no financieras puedan poseer bancos virtuales, aunque sea a través de una sociedad de cartera intermedia constituida en Hong Kong.[117]

El Banco Central Europeo (ECB, por sus siglas en inglés) acepta una gama más amplia de posibles accionistas en los "bancos Fintech": "nuevas filiales Fintech de bancos autorizados existentes; nuevos participantes en el mercado que adoptan la innovación tecnológica para competir con bancos establecidos (...)[y] proveedores de servicios financieros existentes (por ejemplo, entidades de pago, sociedades de inversión, entidades de dinero electrónico [*e-money*], etc.) que amplían su ámbito de aplicación a fin de incluir las actividades bancarias y que, por lo tanto, pueden ser considerados como nuevos aspirantes a entrar en el mercado que precisan de una licencia bancaria.[118]

Tanto la HKMA como la Comisión de Servicios Financieros de Corea (KFSC, por sus siglas en inglés) identifican a las empresas de telecomunicaciones como los candidatos más probables para solicitar licencias de banca virtual. En el caso de Corea, dos de estas empresas ya tienen pequeñas participaciones en bancos.

En sus políticas, las autoridades sitúan a estas nuevas instituciones financieras como competidores de los bancos establecidos en el mercado minorista.

La KFSC espera que los bancos virtuales desarrollen productos de préstamo dirigidos a personas con crédito promedio utilizando un sistema de calificación crediticia basado en big-data, que proporcionen remesas móviles de forma sencilla a través de teléfonos inteligentes y que acepten solicitudes de préstamo sin necesidad de presentar documentos, entre otras características orientadas al cliente minorista.[119]

Del mismo modo, la HKMA prevé que "las bancas virtuales deben desempeñar un papel activo en la promoción de la inclusión financiera en la prestación de sus servicios bancarios. Aunque no se espera que los bancos virtuales mantengan sucursales físicas, deben esforzarse por atender las necesidades de sus clientes objetivo, ya sean particulares o PyMEs. Los bancos virtuales no deberían imponer a sus clientes ningún requisito de saldo mínimo en sus cuentas ni comisiones por saldos bajos".[120]

Un área común en los enfoques de estas jurisdicciones para el otorgamiento de licencias a los bancos virtuales es la de requerir conocimientos tecnológicos relevantes por parte de la gerencia y los miembros de la junta directiva, mismos que les permitan comprender los riesgos que el modelo de negocio requiere.

Una preocupación compartida por la HKMA y el ECB es que los bancos virtuales podrían emprender una campaña agresiva para obtener una cuota de mercado, lo que podría dar lugar a actividades más riesgosas. Además, estas autoridades consideran que estos nuevos bancos podrían enfrentarse a riesgos y dificultades inesperados para conseguir capital adicional si fuera necesario. Por lo tanto, ambas autoridades están exigiendo planes de salida.

Como los bancos virtuales están sujetos a desafíos competitivos no evaluados y a riesgos desconocidos asociados con la naturaleza de sus modelos de negocio, además de la solicitud de licencia, el solicitante debe preparar un plan de salida en caso de que su modelo de negocio no tenga éxito.

116/ National Law Information Center. Act on Special Cases Concerning the Establishment of Internet-Only Banks. 2019.

117/ HKMA (2018).

118/ ECB. Guide to assessments of Fintech credit institution licence applications. Marzo de 2018.

119/ Global Legal Insights. Banking Regulation 2019 – Korea. Marzo de 2019.

120/ HKMA (2018).

Una vez concedida la autorización, las tres autoridades estipulan que los bancos virtuales estarán sujetos al mismo conjunto de estándares que los bancos convencionales, incluyendo el marco pertinente de protección al cliente.

La falta de presencia física y la dependencia de los bancos virtuales hacia los canales electrónicos de entrega no deben afectar el derecho de sus clientes a recibir un trato justo. Por lo tanto, las quejas deben ser manejadas a través de los mismos canales, y los clientes deben ser conscientes de sus responsabilidades para mantener la seguridad en el uso de los servicios de banca virtual y su potencial responsabilidad si no lo hacen.

IV. PRÁCTICAS RELATIVAS A LAS TECNOLOGÍAS DE SOPORTE DE FINTECH

En las secciones anteriores, este informe examinó las prácticas relativas a los productos representativos de Fintech y el panorama en general. Esta sección examina las acciones de las autoridades financieras en relación con tecnologías específicas asociadas a los productos Fintech.

A partir de la evaluación, es evidente que los supervisores aún intentan definir una estrategia en relación con estas tecnologías. En algunos casos, la práctica ha consistido en tratar de integrar el tratamiento de estas tecnologías en el conjunto de reglamentos y políticas existentes, mientras que en otros se ha aplicado un enfoque más restrictivo.

Esta ambivalencia refleja la necesidad de comprender los efectos que estas tecnologías tienen en la capacidad de las instituciones financieras para mantenerse sanas y gestionar eficazmente sus riesgos.

Por último, los supervisores están examinando cómo aprovechar las tecnologías emergentes para mejorar sus capacidades, las denominadas *RegTech* y *SupTech*, que son un tema interesante que va más allá del alcance del presente documento.

1. SERVICIOS BASADOS EN LA NUBE (*CLOUD-BASED SERVICES)*

Las instituciones financieras, como muchas otras industrias, han aprovechado los beneficios de transferir el almacenamiento de datos, el procesamiento de información e incluso la prestación de servicios a terceros a través de servidores ubicados en forma remota. La reacción inicial de muchos supervisores fue tratar estos acuerdos como cualquier otro contrato de tercerización (*outsourcing*).

Sin embargo, algunas autoridades vieron la necesidad de crear políticas y directrices específicas a medida que la dependencia de las instituciones financieras crecía exponencialmente. El Banco de Israel fue uno de los primeros en emitir una política específica sobre los servicios basados en la nube en 2015.

El Banco de Israel restringió la capacidad de las entidades financieras reguladas para utilizar estos servicios, prohibiendo el "uso de servicios basados en la nube para actividades y/o sistemas críticos"[121] y requiriendo la aprobación previa del supervisor para utilizar otros servicios basados en la nube, aun cuando no incluyeran datos de los clientes.

Dos años más tarde, el Banco de Israel comenzó a flexibilizar el conjunto inicial de restricciones, permitiendo a los bancos utilizar ciertos servicios basados en la nube sin aprobación previa cuando no cumplían alguna de las siguientes cuatro condiciones:

a) "La aplicación basada en la nube incluye información que la corporación bancaria define como sensible.

b) El banco no define la información como sensible; sin embargo, la divulgación de información puede ser utilizada para deducir ciertos detalles que permitirán atacar o dañar al banco y/o a sus clientes.

c) La disrupción o interrupción de la actividad de la aplicación de servicios basados en la nube puede perjudicar la conducta de la corporación bancaria y/o su capacidad para servir y responder a sus clientes.

d) La aplicación en la nube proporciona medidas de defensa cibernética y seguridad de la información como la única capa de protección, sin que existan medidas similares en las instalaciones de la corporación bancaria".[122]

Posteriormente, a finales de 2018, el supervisor indicó que "en vista de ello y de la experiencia acumulada, y de forma similar a las directivas emitidas por las autoridades supervisoras paralelas de todo el mundo, la nueva directiva/enmienda facilita las cosas a las entidades bancarias al anular la necesidad de solicitar previamente al Departamento de Supervisión Bancaria la autorización para la implantación de la tecnología de servicios basados en la nube para determinadas aplicaciones, como el almacenamiento de la información sensible de la entidad bancaria y/o del cliente".[123] Sin embargo, la prohibición sobre los sistemas críticos se mantiene en pie.

Paralelamente, la Autoridad Bancaria Europea (EBA, por sus siglas en inglés) publicó un informe[124] sobre los servicios basados en la nube, armonizando el enfoque divergente adoptado por los supervisores nacionales en esta materia.

El documento contiene 7 recomendaciones:

- Evaluación de la materialidad, especificando que antes de comprometerse con un proveedor de servicios basados en la nube, la institución financiera debe evaluar la criticidad de los datos o procesos tercerizados (*outsourced*);

- Deber de informar adecuadamente a los supervisores, proporcionando a la autoridad la información necesaria para evaluar adecuadamente la idoneidad del proveedor y los acuerdos contractuales;

- Derechos de acceso y auditoría, permitiendo a la institución financiera y a su supervisor el acceso a las instalaciones del proveedor, directamente o a través de terceras partes especializadas;

- Seguridad de los datos y sistemas, estableciendo las obligaciones del proveedor para garantizar la protección de los datos recibidos;

- Localización de datos y procesamiento de datos, incluyendo dentro del proceso de gestión de riesgos la incidencia de los riesgos políticos, de privacidad de datos y de seguridad de la jurisdicción del proveedor;

- Tercerización (outsourcing) en cadena, especificando la justificación del proveedor para subcontratar elementos del servicio a otros proveedores y los riesgos adicionales involucrados; y

- Planes de contingencia y estrategias de salida, debidamente documentados por la institución financiera.

121/ Bank of Israel. Risk management in a cloud computing environment. Junio de 2015.
122/ Bank of Israel. Directive 362—Cloud Computing. Julio de 2017.
123/ Bank of Israel. The Banking Supervision Department is making it easier for the banks to use public cloud technology. Noviembre de 2018.
124/ EBA. Recommendations on outsourcing to cloud service providers. Diciembre de 2017.

Por otra parte, la Autoridad Australiana de Regulación Prudencial (APRA, por sus siglas en inglés)) actualizó recientemente su guía sobre los servicios basados en la nube, indicando que "para los acuerdos con bajo riesgo inherente que no impliquen traslado de ciertas actividades al extranjero, la APRA no esperaría que una entidad regulada por ella misma la consulte antes de suscribir el acuerdo".[125]

En América Latina y el Caribe, los reguladores también han incluido requisitos y límites explícitos sobre el uso de los servicios basados en la nube en el marco de la gestión del riesgo operacional. El supervisor de Chile, por ejemplo, desarrolló un capítulo especial en sus regulaciones de tercerización (*outsourcing*) de servicios basados en la nube, afirmando que, cuando se utilizan proveedores de servicios basados en la nube para servicios críticos, las instituciones reguladas deben llevar a cabo una debida diligencia "reforzada" por parte del proveedor. En esos casos, la institución financiera debe asegurarse de que el proveedor cuente con certificaciones reconocidas internacionalmente en materia de seguridad, continuidad del negocio y buenas prácticas. Además, debe existir una opinión legal sobre la privacidad y el acceso a los datos en la jurisdicción del proveedor de servicios basados en la nube. La normativa exige que la institución financiera cuente con un "centro de procesamiento de datos de contingencia ubicado en Chile y demuestre un tiempo de recuperación compatible con la criticidad del servicio subcontratado".[126] Es interesante señalar que la jurisdicción de origen de cualquier empresa de tercerización (*outsourcing*), incluidos los proveedores de servicios basados en la nube, deben tener una calificación-país de riesgo de grado de inversión.

Asimismo, el supervisor financiero de Colombia emitió recientemente una regulación específica para los servicios basados en la nube. El documento define los procesos obligatorios de gestión de riesgos y las condiciones mínimas para los contratos de servicios basados en la nube. El supervisor también establece requisitos específicos de reporte para estos servicios y la documentación que las instituciones financieras deben tener disponible para su inspección. La autoridad también indica que la institución financiera debe "establecer las medidas necesarias para garantizar que, en caso de tomar el control, las [autoridades financieras], o quien ellas designen, puedan acceder a la información y a la administración de los sistemas de información que operan en la nube".[127]

2. INTELIGENCIA ARTIFICIAL

Bajo este marco, cada vez más, se ha probado y utilizado un conjunto de tecnologías relacionadas para ayudar en los procesos de toma de decisiones en los mercados financieros. Sin embargo, como señala el FSB en un informe, "debido a que la Inteligencia Artificial (AI, por sus siglas en inglés) y las aplicaciones de aprendizaje automatizado son relativamente nuevas, no se conocen normas internacionales específicas en este ámbito".[128]

Las pocas prácticas de supervisión identificadas en relación con el uso de esta tecnología en los mercados financieros se encuentran en el mercado de valores, en concreto sobre la orientación de modelos algorítmicos basados en AI por parte de una organización autorregulada de EE.UU., la Autoridad Reguladora de la Industria Financiera (FINRA, por sus siglas en inglés)[129] y la Directiva de la Unión Europea relativa a los Mercados de Instrumentos Financieros, conocida como MiFID II.[130]

En ambos casos, se hace hincapié en el deber de las entidades reguladas de contar con "un proceso de desarrollo sólido (...) para garantizar que se tengan en cuenta los posibles riesgos en todas las fases del proceso de desarrollo (...) a fin de evitar el abuso de mercado y evitar que la estrategia contribuya a un comportamiento desordenado del mercado o lo cause".[131]

125/ APRA. Outsourcing Involving Cloud Computing Services. Septiembre de 2018.
126/ Superintendencia de Bancos e Instituciones Financieras Chile. Recopilación actualizada de normas. Capítulo 20-7. 2018.
127/ Superintendencia Financiera de Colombia. Instrucciones relacionadas con el uso de servicios de computación en la nube. Marzo de 2019.
128/ FSB. Artificial intelligence and machine learning in financial services. Noviembre de 2017.
129/ Finra. Rule 3110. Supervision. Junio de 2015.
130/ EU. Directive 2014/65/EU. Mayo de 2014.
131/ FSB (2017).

Existen otras preocupaciones con respecto al uso de esta tecnología, como el sesgo incorporado en el análisis de crédito y bancos que confían sus estrategias en algoritmos de toma de decisiones sin tener una comprensión completa del proceso lógico que hay detrás del proceso. Sin embargo, no está claro cómo abordar estas cuestiones.

Por otro lado, los supervisores están mirando positivamente hacia desarrollos que podrían simplificar el cumplimiento por parte de la comunidad regulada y apoyar sus propias actividades como parte de las ya mencionadas *RegTech* y *SupTech*.

3. IDENTIFICACIÓN BIOMÉTRICA DEL USUARIO

La creciente amenaza de fraude financiero mediante el uso de credenciales de identificación robadas ha impulsado el desarrollo de diversas técnicas que garantizan que una persona que accede de forma remota a una institución financiera sea el propietario legítimo de la cuenta. Entre las tecnologías emergentes pertinentes, la identificación biométrica[132] se ha incorporado cada vez más en la denominada autenticación multifactorial.

Existen pocas prácticas de supervisión identificadas en relación con el uso de la biometría en los mercados financieros. La iniciativa más notable, por su tamaño y su impacto en la inclusión financiera, es el requisito del Banco de la Reserva de la India de que "los bancos garanticen que toda la nueva infraestructura de aceptación de tarjetas emitida con efecto a partir del 1 de enero de 2017 esté habilitada para procesar transacciones de pago utilizando autenticación biométrica basada en Aadhaar".[133] Aadhaar es un sistema nacional de identificación que incorpora huellas dactilares para autenticar a la persona. Aunque, a raíz de una sentencia del Tribunal Supremo, no es obligatorio que las personas tengan el carné de identidad de Aadhaar para abrir una cuenta bancaria, la decisión del supervisor ha garantizado que el sistema de pago esté listo para realizar transacciones seguras utilizando la identificación biométrica.

Otro caso de un supervisor que exige la identificación biométrica es la resolución del Departamento de Servicios Financieros del Estado de Nueva York sobre ciberseguridad, que exige que las instituciones financieras reguladas proporcionen autenticación multifactorial, incluyendo "factores inherentes, como, por ejemplo, una característica biométrica".[134]

Cabe señalar que la CNBV de México prescribió la tecnología biométrica obligatoria para identificar a los usuarios financieros dentro de las regulaciones de ciberseguridad mencionadas en la sección II.8. Esta norma estipula que las instituciones financieras, incluidas las nuevas instituciones de tecnología financiera, deben implementar la identificación biométrica para marzo de 2020.

La norma también especifica que, si bien no se ha implementado la identificación biométrica, "en el caso de que sus clientes presenten reclamaciones [por fraude] (....) realizadas por terceros que aleguen ser el cliente en cuestión, se comprometen a asumir los riesgos y, por tanto, los montos de dichas reclamaciones (...) Las respectivas cantidades serán pagadas, a más tardar veinte días después de la presentación de la reclamación".[135] Esta normativa, sin duda, incentiva a las instituciones financieras a implementar la identificación biométrica mucho antes de la fecha límite oficial.

Otra disposición interesante es que "antes de la captura de los datos biométricos de sus usuarios, las instituciones deben capturar los mismos datos biométricos de sus empleados, directivos y funcionarios encargados de esta función, y verificar que los datos biométricos de los clientes no se corresponden con los de dichos empleados, directivos y funcionarios".[136]

132/ Entendida como las características individuales inherentes a una persona específica.

133/ Reserve Bank of India. Aadhaar-based Authentication for Card Present Transactions. Septiembre de 2016.

134/ New York State Department of Financial Services. Cybersecurity Requirements for Financial Services Companies. Marzo de 2017.

135/ CNBV. Disposiciones de carácter general aplicables a las instituciones de crédito. Reformado en noviembre de 2018.

136/ Ídem.

V. COMENTARIOS FINALES

Como se ha mencionado en varias ocasiones a lo largo de este informe, las prácticas de regulación y supervisión están en continua evolución, como resultado de nuevas experiencias y de una mayor comprensión por parte de las autoridades de los riesgos y beneficios de los productos Fintech y sus tecnologías asociadas.

Hay algunos temas que son relevantes para los servicios financieros que no se abordan en este informe, como la privacidad de los datos, ya que su regulación suele estar fuera del ámbito de las autoridades financieras. Además, los desarrollos en Fintech que son de interés con respecto a las propias actividades de las autoridades fueron excluidos de la discusión, ya que están fuera del alcance de este documento.

ANEXO 1

JURISDICCIONES ANALIZADAS

Nombre	Continente	Nombre	Continente
Argentina	América	Alemania	Europa
Barbados	América	Dinamarca	Europa
Bolivia	América	España	Europa
Brasil	América	Finlandia	Europa
Canadá	América	Francia	Europa
Chile	América	Gibraltar	Europa
Colombia	América	Holanda	Europa
Ecuador	América	Hungría	Europa
México	América	Irlanda	Europa
Perú	América	Isla de Man	Europa
EE.UU.	América	Islandia	Europa
China	Asia	Italia	Europa
Corea	Asia	Lituania	Europa
Dubái	Asia	Luxemburgo	Europa
Filipinas	Asia	Malta	Europa
Hong Kong	Asia	Noruega	Europa
India	Asia	Polonia	Europa
Indonesia	Asia	Portugal	Europa
Israel	Asia	Reino Unido	Europa
Japón	Asia	Rusia	Europa
Malasia	Asia	Suecia	Europa
Singapur	Asia	Suiza	Europa
Taiwán	Asia	Ucrania	Europa
Turquía	Asia	Botsuana	África
Australia	Oceanía	Camerún	África
Nueva Zelanda	Oceanía	Ghana	África
		Kenia	África
		Nigeria	África
		Sudáfrica	África
		Tanzania	África

ANEXO 2

ESQUEMAS DE PROMOCIÓN DE FINTECH OBSERVADOS POR LAS AUTORIDADES FINANCIERAS

Jurisdicción	Unidad/ Canal Dedicado	Centro de Innovación	*Regulatory Sandbox*	Licencia Especial de Fintech
Dinamarca	X	X	X	
Finlandia	X	X		
Francia	X	X		
Italia	X			
Malta	X	X	X	
Holanda	X	X	X	
Polonia	X	X	X	
Portugal	X	X		
Lituania	X	X	X	X
Suecia		X		
Reino Unido	X	X	X	
España	X		X	
Suiza	X	X	X	X
Isla de Man	X	X	X	
Australia		X	X	
Nueva Zelanda	X			
Dubái	X	X	X	X
Singapur	X	X	X	
Japón	X	X		
Corea	X		X	X
Malasia	X	X	X	
India			X	
Indonesia	X		X	X
Hong Kong	X	X	X	X
Taiwán	X	X	X	
Sudáfrica	X			
EE.UU.	X		X	
Brasil				X
México		X	X	X
Argentina	X	X		
Barbados	X		X	
Colombia	X	X	X	X
Total	**27**	**22**	**22**	**9**

ANEXO 3

ESQUEMAS DE CONCESIÓN DE LICENCIAS DE FINTECH OBSERVADOS
Análisis por Jurisdicción

Jurisdicción	Pago	*Peer-to-peer*	Financiamiento colectivo (*crowdfunding*)	Criptoactivos	Bancas virtuales
Dinamarca	X				
Finlandia	X		X		
Francia	X	X	X		
Alemania	X		X		
Hungría	X				
Irlanda	X				
Italia	X		X		
Luxemburgo	X				
Lituania	X	X			
Malta	X				
Holanda	X	X			
Polonia	X				
Portugal	X		X		
Suecia	X				
Reino Unido	X				
España	X	X	X		
Islandia	X				
Noruega	X				
Suiza			X		
Gibraltar	X			X	
Isla de Man	X	X	X		
Dubái	X	X	X		
Nueva Zelanda		X	X		
Singapur	X				
Japón	X			X	
Corea	X				X
Malasia	X	X	X		X
India	X	X			
Indonesia	X	X			
Filipinas	X				
China	X	X	X		

ANEXO 3

ESQUEMAS DE CONCESIÓN DE LICENCIAS DE FINTECH OBSERVADOS
Análisis por Jurisdicción

Jurisdicción	Pago	*Peer-to-peer*	Financiamiento colectivo (*crowdfunding*)	Criptoactivos	Bancas virtuales
Hong Kong	X				X
Taiwán	X				
Camerún	X				
Ghana	X				
Kenia	X				
Nigeria	X				
Tanzania	X				
Canadá	X	X	X		
EE.UU.	X		X	X	
Colombia	X		X		
Brasil		X	X		
México	X	X	X		
Chile	X				
Perú	X				
Ecuador	X				
Bolivia	X				
Total	**44**	**14**	**17**	**3**	**3**

MIEMBROS DEL GRUPO DE TRABAJO

Carolus Walters
Centrale Bank van Curaçao en Saint Maarten

Christiano Costa Moreira
Banco Central Do Brasil

Aldo Enrique Matsuoka Tanaka
Superintendente de Banca, Seguros y AFP, Perú

Carolina Flores Tapia
Comisión para el Mercado Financiero, Chile

Nadia Herrera Bellot
Autoridad de Supervisión del Sistema Financiero, Bolivia

Rocío H. Robles Peiro
Comisión Nacional Bancaria y de Valores, México

Thays Bermúdez
Superintendencia de Bancos de Panamá

Marco Antonio Cerrato Cruz
Comisión Nacional de Bancos y Seguros, Honduras

Runako Brathwaite
Central Bank of Barbados

Roberto González Ruíz
Superintendencia General de Entidades Financieras, Costa Rica

Jorge Álvarez Ledezma
Superintendencia General de Entidades Financieras, Costa Rica

Maximir Álvarez
Consultor
International Consulting Consortium, Inc.

ASBA
Marcos Fabián
Antonio Pineda
Ricardo Toranzo

MIEMBROS ASBA

Miembros Asociados

Región Andina

Superintendencia Financiera de Colombia
Superintendencia de las Instituciones del Sector Bancario, Venezuela
Autoridad de Supervisión del Sistema Financiero, Bolivia
Superintendencia de Bancos del Ecuador
Superintendencia de Banca, Seguros y AFP, Perú

Región Caribe

Central Bank of Belize
Oficina del Comisionado de Instituciones Financieras, Puerto Rico
Banco Central de Cuba
Bank of Guyana
Bank of Jamaica
Banque de la République d' Haïti
Cayman Islands, Monetary Authority
Centrale Bank van Aruba
Centrale Bank van Curaçao en Sint Maarten
Eastern Caribbean Central Bank
Financial Services Regulatory Commission, Antigua y Barbuda
Turks & Caicos Islands Financial Services Commission
Central Bank of Barbados
Central Bank of the Bahamas
Central Bank of Trinidad and Tobago
Centrale Bank van Suriname
Financial Services Commission, British Virgin Islands

Región Centroamérica

Superintendencia de Bancos, Guatemala
Comisión Nacional de Bancos y Seguros, Honduras
Superintendencia de Bancos y de Otras Instituciones Financieras de Nicaragua
Superintendencia del Sistema Financiero, El Salvador
Superintendencia General de Entidades Financieras, Costa Rica
Superintendencia de Bancos de Panamá
Superintendencia de Bancos de República Dominicana

Región Norte América

Board of Governors of the Federal Reserve System, USA
Office of the Comptroller of the Currency, USA
Federal Deposit Insurance Corporation, USA
Comisión Nacional Bancaria y de Valores, México

Región Cono Sur

Comisión para el Mercado Financiero, Chile
Banco Central do Brasil
Banco Central de la República Argentina
Banco Central del Paraguay
Banco Central del Uruguay

No Regionales

Banco de España

Miembros Colaboradores

Banco Central de Reserva de El Salvador
Comisión Nacional de Microfinanzas, Nicaragua
Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, México

PRÁCTICAS GLOBALES DE REGULACIÓN Y SUPERVISIÓN DE FINTECH

Agencia Ejecutora: Asociación de Supervisores Bancarios de las Américas (ASBA)

Financiado por: BID Lab

Proyecto: Regulación para la Innovación Responsable y Competitiva del Sector Financiero

Cooperación Técnica: ATN/ME-15724-RG

Diciembre de 2019.

Información adicional: asba@asbasupervision.org

C. Picacho Ajusco #238, Of. 601

Col. Jardines en la Montaña, C.P. 14210

Ciudad de México, México

(5255) 5662-0085

A S B A