

LA PROTECCIÓN AL CONSUMIDOR EN EL NUEVO ENTORNO DE INNOVACIÓN TECNOLÓGICA FINANCIERA

CONSIDERACIONES DE REGULACIÓN Y SUPERVISIÓN

Regulación para la innovación
responsable y competitiva del
sector financiero

Junio 2020



Este estudio, *La protección al consumidor en el nuevo entorno de innovación tecnológica financiera: Consideraciones de regulación y supervisión*, ha sido financiado por el proyecto ATN/ME-15724-RG (Regulación para la Innovación Responsable y Competitiva del Sector Financiero) cofinanciado por la Asociación de Supervisores Bancarios de las Américas (ASBA) y BID Lab, el Laboratorio de Innovación del Grupo BID.

© ASBA y BID Lab, Primera Edición. Junio 2020.

Este estudio (*La protección al consumidor en el nuevo entorno de innovación tecnológica financiera: Consideraciones de regulación y supervisión*) es propiedad de ASBA y BID Lab. Queda permitido reproducir este estudio parcial o totalmente, siempre y cuando se tenga consentimiento previo de ASBA y BID Lab y su autoría quede atribuida.

La información y las opiniones presentadas en este estudio (*La protección al consumidor en el nuevo entorno de innovación tecnológica financiera: Consideraciones de regulación y supervisión*) son de los autores y no representan necesariamente la posición oficial del Banco Interamericano de Desarrollo (BID).

Información adicional: asba@asbasupervision.org

asbasupervision.com

T. (5255) 5662-0085

Diseño editorial de Tinta Roja Editoras, contacto@tintarojaeditoras.com

AGRADECIMIENTOS

La Asociación de Supervisores Bancarios de las Américas agradece a Juan Pedro Cantera y a los demás integrantes de la Junta Directiva en 2017 por impulsar de manera decisiva la realización del proyecto de *Regulación para la Innovación Responsable y Competitiva del Sector Financiero*. Asimismo, y de manera particular, la Asociación agradece a Rudy V. Araujo por su trabajo excepcional y compromiso con este proyecto.

Este proyecto fue posible gracias a la contribución y apoyo del BID Lab.

CONTENIDO

INTRODUCCIÓN	11
PREOCUPACIONES EN TORNO A LA PROTECCIÓN DEL CONSUMIDOR FINANCIERO DIGITAL	13
PRECONDICIONES PARA LA PROTECCIÓN DEL CONSUMIDOR FINANCIERO DIGITAL	17
CONSIDERACIONES Y RECOMENDACIONES GENERALES	21
CONSIDERACIONES Y RECOMENDACIONES CON RESPECTO A LOS DEBERES Y DERECHOS DE LOS CONSUMIDORES FINANCIEROS DIGITALES	27
CONSIDERACIONES ESPECÍFICAS PARA PRODUCTOS FINTECH DE MAYOR RELEVANCIA EN LAS AMÉRICAS	35
ALTERNATIVAS PARA UN MODELO DE SUPERVISIÓN DE CONDUCTA Y PROTECCIÓN AL CONSUMIDOR EN EL NUEVO ENTORNO TECNOLÓGICO	41
CONSIDERACIONES PARA LA IMPLEMENTACIÓN DE ESTRATEGIAS DE SUPERVISIÓN	47
COMENTARIOS FINALES Y DESAFÍOS PENDIENTES PARA LAS AUTORIDADES	55
TÉRMINOS Y ABREVIATURAS	59

INTRODUCCIÓN

Los desarrollos de las Fintech han introducido el uso de tecnologías innovadoras en la provisión de servicios bancarios, remodelando los modelos de negocios, canales, servicios y competencia de mercado de la industria financiera, así como la creación de nuevos riesgos. Bajo este nuevo esquema disruptivo sin precedentes, la Asociación de Supervisores Bancarios de las Américas (ASBA), con apoyo del Banco Interamericano de Desarrollo (BID), conformó un Grupo de Trabajo (GDT)¹ bajo la guía de un consultor experto², con el objetivo de establecer consideraciones mínimas y recomendaciones de regulación para la incorporación de tecnologías innovadoras en el sector financiero de manera responsable, transparente y competitiva. Para cumplir con el objetivo, la Asociación decidió analizar el ecosistema de productos financieros tecnológicos (Fintech) desde los enfoques prudencial y no prudencial.

1 Agradecemos la participación del Grupo de Trabajo conformado por las siguientes instituciones miembros de ASBA: Autoridad de Supervisión del Sistema Financiero (Bolivia), Banco Central Do Brasil (Brasil), Comisión para el Mercado Financiero (Chile), Superintendencia General de Entidades Financieras (Costa Rica), Banco de España (España), Superintendencia de Banca, Seguros y AFP (Perú).

2 Roberto Borrás, es abogado colombiano, asesor en materia regulatoria financiera y socio de Garrigues desde 2015. Fue Superintendente Financiero de Colombia, Director General de Regulación Financiera del Ministerio de Hacienda y Crédito Público (actualmente URF) y Presidente del Autorregulador del Mercado de Valores de Colombia. Fue además Superintendente Adjunto de Riesgos y Superintendente de Conglomerados en la Superintendencia Financiera de Colombia. Entre otros cargos fue asesor del Gobierno Nacional en la preparación del Proyecto de Ley de Inclusión Financiera (1735 de 2014) mediante el cual se crearon las SEDPES. Ha sido consultor del Banco Mundial y del Banco Interamericano de Desarrollo.

Este documento se enfoca en el análisis no prudencial de la regulación y supervisión de Fintech. Para el desarrollo de las recomendaciones normativas y de supervisión, se realizó un estudio sobre las prácticas de comercialización, divulgación de información y transparencia, a partir del cual se identificaron buenas prácticas y oportunidades de mejora, siempre teniendo como punto de referencia la protección al usuario de los productos o servicios identificados. Con la revisión de la información recolectada, de la experiencia identificada en otras jurisdicciones, de la asesoría del GDT y del equipo técnico de ASBA, el documento recoge aquellas propuestas de consideraciones normativas y de supervisión mínimas que resultan aplicables a los productos y servicios de las Fintech en la región.

A partir del análisis realizado, es posible establecer consideraciones y recomendaciones mínimas con base en las iniciativas y tendencias comunes de regulación y supervisión conductual para la protección al consumidor. Éstas serán desarrolladas a lo largo del documento considerando tres aspectos fundamentales.

En primer lugar, se considera que la **regulación debe ser neutral** con respecto al cambio tecnológico y modelos de negocio y no debe alentarlos ni obstaculizarlos. En cambio, la regulación debe permitir una competencia justa entre todos los actores del mercado, esto es, análogo frente a digital; modelos de negocios existentes frente a nuevos modelos con alto componente digital; empresas digitales locales frente a competidores extranjeros en expansión. Lo anterior, sin perjuicio del deber de las Autoridades de Regulación y Supervisión (ARS) de

conocer y analizar los desarrollos tecnológicos para evaluar el potencial de éstos, entre otros frente a iniciativas de inclusión financiera, así como los riesgos que dichos desarrollos pueden plantear.

En segundo lugar, se considera que **la regulación debe estar basada en principios**. Las jurisdicciones a la vanguardia en el desarrollo de la industria de proveedores de productos y servicios financieros digitales tienden a aplicar dicho enfoque de regulación, debido a que es mucho más flexible en términos de su aplicación real sobre emprendimientos financieros en contraposición a la regulación basada en reglas, no importa si se elige un canal analógico o digital.

La regulación basada en principios ha demostrado proporcionar espacio para la innovación, además de reconocer los acelerados cambios en la prestación de servicios financieros, lo que permite una aplicación dinámica y eficaz de la norma en un entorno cambiante. En contraste, un esquema sobreprescriptivo, caracterizado por controlar todo hasta el último detalle, tiende a sofocar la innovación³.

En tercer lugar, es fundamental **prevenir la aparición de brechas o arbitrajes regulatorios** provocados por la aparición de nuevos prestadores que, por estar fuera del perímetro regulatorio desarrollen actividades iguales o estructuralmente similares a las desarrolladas por parte de proveedores de Entidades Financieras Tradicionales (incumbentes)⁴.

En este aspecto es relevante considerar que varias entidades incumbentes de la región han sido activas en el desarrollo de iniciativas Fintech. Estos incumbentes buscan optimizar la prestación de sus servicios, al tratar de llegar a más ciudadanos en distintos lugares, sin importar su zona geográfica, con la creación de nuevos canales, además de proponer mejores condiciones de funcionamiento de los productos, haciéndolos más seguros para el consumidor y procurando esquemas más competitivos. Por lo general, los desarrollos por parte de incumbentes, por estar en el perímetro regulatorio, se han dado con estricta sujeción a normativas de protección al consumidor, ya sea

atendiendo reglas especiales para la industria financiera o normas transversales aplicables a ésta.

Debe tenerse en cuenta que existe una relación estrecha entre las directrices de privacidad en el ámbito financiero, la protección de datos personales y la adecuada protección al consumidor financiero. Es por esto que resulta evidente que muchos de los temas tratados en este documento pueden comprender actividades y funciones no sólo de supervisores y reguladores financieros, sino también de las instituciones de supervisión de datos personales presentes en cada jurisdicción.

También, es conveniente mencionar que las ARS financieras deben colaborar estrechamente con estas instituciones para fortalecer la divulgación de las normativas y que sean tenidas en cuenta en los proyectos financieros de innovaciones tecnológicas. Se destaca que las legislaciones regionales en materia de protección de datos personales comparten filosofía y directrices con el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) europeo, lo que proporciona una amplia base legal en el tema⁵.

Dicho lo anterior, este documento se divide en ocho secciones. En la primera, se describen las características de los consumidores digitales y algunas de sus preocupaciones transversales. En la segunda, se plantean algunas consideraciones previas para desarrollar estrategias y acciones eficaces que las autoridades reguladoras pueden adoptar de cara a la adecuada protección del consumidor financiero digital. En la tercera, se establecen consideraciones y recomendaciones generales con el fin de garantizar la igualdad de condiciones evitando el arbitraje regulatorio entre las Fintech y las entidades financieras tradicionales. En la cuarta, se hacen consideraciones y recomendaciones particulares con respecto a los deberes y derechos de los consumidores financieros digitales. En la quinta, se presentan consideraciones específicas para los productos o servicios identificados de mayor uso y/o potencial de uso en las Américas. En la sexta, se analizan alternativas para un modelo de supervisión de conducta y protección al consumidor en el nuevo entorno tecnológico (modelo de supervisión basado en riesgo y modelo de responsabilidad demostrada). En la séptima, se desarrollan consideraciones para la implementación de estrategias de supervisión. Por último, en la octava se describen los desafíos pendientes para las Autoridades de regulación y supervisión y se hacen los comentarios finales.

³ <https://www.bbva.com/en/countries-leading-fintech-regulation/>

⁴ A lo largo del presente documento se utilizará el término incumbente (adaptado del anglicismo Incumbent), como aquellas entidades financieras tradicionales que se contraponen a los proveedores financieros innovadores.

⁵ <https://gdpr-info.eu/>

PREOCUPACIONES EN TORNO A LA PROTECCIÓN DEL CONSUMIDOR FINANCIERO DIGITAL

Las innovaciones digitales, el aumento de potencia de las redes de telecomunicaciones y dispositivos móviles, el uso extendido de las redes sociales, y la computación en la nube, han creado consumidores más exigentes.

Hoy en día los consumidores cuentan con herramientas para investigar, seleccionar y comprar productos y servicios digitales, pero son menos conscientes de sus derechos como consumidores que aquellos que utilizan medios tradicionales. Algunos estudios⁶ muestran las siguientes descripciones de los consumidores financieros digitales:

- Pertenecen en su mayoría a la generación de los llamados *millennial* (nacidos entre 1981 y 1993) debido a que son la primera generación totalmente digital. Estos consumidores muestran una mayor dependencia de las plataformas digitales y adoptan los productos y servicios con las características digitales más nuevas disponibles en el mercado, cada vez a un ritmo más rápido y con el mayor alcance.
- Consideran que es más fácil “crear” una cuenta con una aplicación móvil de un proveedor Fintech no supervisado que utilizar una herramienta o canal provisto por una Institución Financiera (IF) tradicional. Mientras que las generaciones mayores prefieren más la interacción personal con sus proveedores financieros y tienden a desconfiar de las soluciones digitales, los más jóvenes prefieren no visitar una IF

tradicional, ya que consideran que consume mucho tiempo y, más aún, no confían en estas instituciones después de lo ocurrido en la crisis financiera.

- Desean acceder a la misma variedad de productos y servicios en todos los canales (omnicanalidad), ya sea a través de la página web o mediante una aplicación (app), y utilizando un móvil inteligente, una tableta o un computador sin que esto afecte la calidad del servicio.
- Consideran que las nuevas empresas de servicios Fintech pueden tener tasas y tarifas más atractivas para sus servicios que las IF tradicionales.
- Esperan un servicio 24/7 porque piensan que pueden acceder a más servicios y productos mientras realizan una actividad cotidiana en lugar de solo un servicio específico por el cual deben visitar una sucursal. Igualmente, esperan que sus solicitudes y quejas se resuelvan en plazos muy breves, en las horas siguientes o el mismo día de su reclamación.
- Están convencidos de que las soluciones innovadoras de tecnología financiera brindan una mejor experiencia y funcionalidad en línea para conocer sus servicios en comparación con el sitio web de una IF tradicional, se familiarizan intuitivamente con las características de las apps de Fintech, ya que la experiencia del usuario está centrada en obtener resultados en lugar de proporcionar mucha información que consideran “innecesaria”.
- Están dispuestos a cambiar de entidad si otra les ofrece mejores condiciones. Además, compartirán algún comentario o queja por redes sociales.
- Están en gran riesgo de experimentar estrés y embarcarse en malas gestiones financieras. De hecho, aquellos que usan pagos móviles tienen

⁶ <https://pdf4pro.com/cdn/millennials-and-wealth-management-inside-article-21c251.pdf>; <https://www.bbva.com/es/cliente-mas-exigente-consumidor-digital/>; <https://usa.visa.com/dam/VCOM/global/partner-with-us/documents/visa-new-digital-consumer.pdf>

casi 16 puntos porcentuales más de posibilidades de sobregirarse en sus cuentas corrientes (que aquellos que no usan pagos móviles) y 23 puntos porcentuales más próximos a acceder a servicios financieros alternativos (casas de empeño y préstamos día a día). Así mismo, aquellos que usan pagos móviles muestran menores niveles de educación financiera y peores prácticas de gestión financiera que los no usuarios⁷.

Bajo este entorno, es apropiado que las ARS consideren cómo deben estar protegidos los consumidores financieros y si los riesgos que surgen de la digitalización se abordan adecuadamente en sus procesos y normativas de protección al consumidor actual.

Al respecto, el *Bureau Européen des Unions de Consommateurs* (BEUC) en respuesta a la consulta pública de la Comisión Europea sobre Fintech ha sostenido que desde el punto de vista del consumidor “no importa si un banco, un proveedor de servicios de pago no bancario, una plataforma de financiación colectiva o un robot-asesor proporcionan un servicio financiero; el consumidor espera tener un trato justo (igual) en las etapas pre-contractual, contractual y postcontractual tales como publicidad clara y no engañosa, una explicación de todos los riesgos posibles relacionados con el producto y un marco eficiente para resolver posibles disputas”⁸.

De esta manera, la digitalización de los productos y servicios financieros puede significar que los consumidores financieros digitales también estén expuestos a riesgos “nuevos” (particularmente cuando se comparan con los productos financieros tradicionales), y es especialmente importante comprender los problemas potenciales de la innovación y la digitalización desde la perspectiva del consumidor. A continuación, se presentan algunas pre-

ocupaciones transversales con respecto a la protección del consumidor.

Acceso a los productos y servicios financieros

- Acceso reducido a productos y servicios financieros para consumidores que carecen de habilidades digitales, escasa educación financiera o poco acceso a tecnología para operar en el entorno de servicios financieros digitalizados.
- El acceso instantáneo y/o simplificado a productos y servicios financieros puede resultar en una mala toma de decisiones y en un potencial detrimento financiero para el consumidor.
- El uso único de datos digitales del consumidor para evaluar la solvencia crediticia puede reducir la precisión de las evaluaciones crediticias y aumentar la exclusión financiera (efecto exactamente contrario al deseado).
- Dificultad para que las empresas identifiquen a los consumidores vulnerables e interactúen con ellos debido a la pérdida de la interacción humana directa.
- Exclusión de ciertos productos y servicios personalizados porque el consumidor no ha generado una huella digital o suficientes datos personales en línea, o se niega a compartir sus datos personales.
- La personalización de los productos puede reducir el pensamiento crítico por parte de los consumidores en el proceso de toma de decisiones.

Divulgación de información y asesoría a los consumidores

- Uso de promociones y/o publicidad pagada acerca de productos o servicios en línea que se presentan falsamente como imparciales o independientes.
- Uso de marketing en las redes sociales para dirigirse de forma inapropiada a los consumidores que no comprenden completamente los riesgos relacionados con ciertos productos y servicios, particularmente los de inversión.

7 GFLEC New Insights Report. Millennial mobile payment users: A look into the personal finances and financial behaviours. <https://gflec.org/wp-content/uploads/2018/04/GFLEC-Insight-Report-Millennial-Mobile-Payment-Users-Final.pdf?x83489>

8 https://www.beuc.eu/publications/beuc-x-2017-073_fintech_a_more_competitive_and_innovative_eu_financial_sector.pdf

- La presentación de información mal diseñada en un formato en línea o móvil que pueda incitar a malas elecciones, lo que podría resultar en una "mala venta" para el consumidor.
- Los consumidores no entienden el costo total del servicio, se enfrentan a términos complicados y documentación inadecuada.
- Poco o nulo conocimiento y comprensión de los consumidores sobre la complejidad de las tecnologías y los sistemas subyacentes involucrados en el suministro de productos y servicios financieros, como el uso de algoritmos en la provisión de robot-asesoría.

Idoneidad de productos y servicios ofrecidos

- El suministro inadecuado de asesoría sobre productos o servicios inconvenientes debido a la recopilación de información incompleta o inexacta del cliente (KYC).
- Los clientes pueden ser tratados injustamente debido a una estructura de bonificaciones inadecuada.
- Las empresas persuaden a los clientes para que se beneficien de transacciones y servicios particulares, no porque sean de su mejor interés, sino porque ofrecen tarifas o comisiones más altas.
- Mayor endeudamiento de los consumidores debido a la facilidad de acceso y uso del crédito en línea.

Gestión de quejas y reclamaciones

- Las definiciones legales de queja son diversas y difusas en relación con solicitudes y peticiones.
- Los consumidores no saben que tienen derecho a quejarse; o pueden saber que tienen este derecho, pero no conocen los canales adecuados; o saben

cómo y dónde presentar una queja, pero no reciben una respuesta adecuada.

- Un error en los sistemas o en la información en una herramienta automatizada puede dar como resultado que se generen simultáneamente muchas quejas de los consumidores afectados.
- Se dificulta identificar al responsable de un producto o servicio si participan diferentes proveedores especializados en el desarrollo del producto o servicio o, si las Fintech se han asociado con proveedores de servicios no financieros.
- Se pueden producir limitaciones, sesgos o errores en la tecnología subyacente que podrían causar un perjuicio significativo al consumidor en cuanto al valor reclamado. Adicionalmente, la complejidad de la tecnología que subyace en el proceso de manejo de reclamos puede ser difícil de entender o cuestionar por parte de los consumidores para buscar una reparación adecuada del perjuicio.

Retención de registros de los consumidores

- A medida que aumenta el número de registros pueden producirse problemas de gobernanza, registros inadecuados y falta de procedimientos de auditoría de datos.
- Fraude y robo de datos del consumidor si no existen sistemas de seguridad estrictos para proteger los datos personales y financieros.
- Dificultad para capturar y registrar con precisión los registros de transacciones de los clientes a través de las redes sociales y de las plataformas digitales a la mano.

PRECONDICIONES PARA LA PROTECCIÓN DEL CONSUMIDOR FINANCIERO DIGITAL

Las ARS enfrentan el desafío de adaptar la normativa y el enfoque de supervisión actual al uso creciente de innovaciones tecnológicas en la prestación de servicios financieros, ya sea por parte de incumbentes o de las Fintech. Las autoridades deben encontrar un equilibrio entre garantizar la solidez del sistema financiero, mantener la integridad y transparencia del mercado y velar por la adecuada protección de los consumidores financieros (independientemente de los canales y proveedores utilizados para adquirir productos y servicios financieros), al tiempo que permiten o incluso propician los avances tecnológicos.

La supervisión de las Fintech puede implicar nuevas formas de interactuar con estas empresas o prestadores, por lo cual se estima necesario plantear algunas consideraciones previas para desarrollar estrategias y acciones eficaces de cara a la adecuada protección del consumidor de productos y servicios financieros:

ASEGURAR UN MARCO REGULATORIO Y DE SUPERVISIÓN PARA LA PROTECCIÓN DE LOS CONSUMIDORES FINANCIEROS Y LA OPORTUNA ATENCIÓN DE QUEJAS Y RECLAMOS

En la encuesta realizada a las ARS de la región⁹, se identificó que el arreglo institucional para la protección al

consumidor financiero es variable. Algunas autoridades de supervisión prudencial tienen facultades en la materia, otras comparten dicha responsabilidad con autoridades transversales de protección al consumidor (vigilan la materia en otras industrias), en otros casos hay una autoridad especializada en la protección al consumidor financiero y en otros esquemas si bien la autoridad prudencial no tiene un mandato específico en protección al consumidor, despliegan o coordinan acciones en la materia.

Por lo tanto, dependiendo del arreglo institucional presente en cada jurisdicción se tienen los siguientes modelos:

- Picos gemelos (Twin Peaks): funciones de supervisión y/o regulación en dos autoridades, una de supervisión prudencial y la otra a cargo de supervisión de la conducta de los negocios.
- Modelo integrado: funciones de supervisión y/o regulación en una sola autoridad, con tres pilares al interior, una dirección o su equivalente para temas prudenciales, otra dirección o equivalente para mercado de valores e infraestructura y una dirección o equivalente de conductas de los negocios y protección al consumidor.
- Modelo sectorial o institucional: funciones de supervisión y/o regulación de acuerdo con la actividad legal de las entidades, desde una perspectiva prudencial

características y desafíos que los supervisores puedan enfrentar ante una revisión del cuerpo normativo e intensidad supervisora para la incorporación de tecnologías innovadoras en el sector financiero de manera responsable, transparente, y competitiva. La encuesta fue completada por 14 jurisdicciones miembros de ASBA, las cuales son: Bolivia, Brasil, Chile, Costa Rica, Ecuador, El Salvador, España, Guatemala, Guyana, Honduras, México, St Kitts & Nevis, Turks & Caicos Islands y Uruguay.

⁹ Con el fin de profundizar el entendimiento de las prácticas de comercialización, de divulgación de información y protección del consumidor de los productos Fintech en las distintas jurisdicciones de la región, la Asociación elaboró y distribuyó en 2019 una encuesta con el objetivo último de desarrollar una visión de conjunto sobre las principales

y de conducta de los negocios. Es decir, una autoridad de supervisión para banca, otra para seguros y otra para valores y pensiones y, cada autoridad con una dirección o su equivalente para protección del consumidor. En este modelo la supervisión de algunas industrias puede estar o no integrada (por ejemplo, banca y seguros, valores y pensiones, etc.).

- Modelo de tres picos: funciones de supervisión y/o regulación en tres autoridades, una de supervisión prudencial, otra del mercado de valores y protección del inversor y una autoridad independiente de protección al consumidor con mandato de supervisión, educación de los consumidores financieros, y fortalecimiento de la educación financiera entre los ciudadanos.

Es una condición esencial evaluar al interior de cada arreglo institucional si el área, dirección o su equivalente a cargo de labores de protección al consumidor financiero cuenta con el mandato y recursos humanos y técnicos para supervisar la protección al consumidor financiero como mínimo en los siguientes aspectos:

- Gestión del riesgo de protección al consumidor;
- Análisis de la protección al consumidor en las etapas precontractuales, contractuales y postcontractuales de prestación del servicio;
- Cuidado del suministro adecuado de información y transparencia;
- Anticipación en actividades de supervisión de riesgos que, como el operativo, son de alta incidencia en la adecuada protección al consumidor;
- Atención de quejas y reclamaciones y análisis de éstas como insumo para las estrategias de supervisión al consumidor;
- Capacidad para adelantar procesos sancionatorios frente a entidades vigiladas en materia de protección al consumidor;
- Fomento del desarrollo de mecanismos de resolución de conflictos;
- Participación en el desarrollo de estrategias y acciones de educación financiera.

LAS AUTORIDADES DE SUPERVISIÓN DEBEN CONTAR CON FACULTADES PARA HACER CUMPLIR LAS LEYES Y NORMAS EXISTENTES (*ENFORCEMENT*) TANTO PARA ENTIDADES TRADICIONALES COMO PARA FINTECH

Las facultades más comunes con que cuentan las autoridades para hacer cumplir el marco regulatorio son:

- Medidas de cumplimiento voluntario: A partir de las cuales la autoridad procura que el supervisado acate voluntariamente las normas, de manera que la sanción se convierte en un mecanismo de última instancia. Pueden ser vinculantes (generalmente pedidos) o no vinculantes (advertencias o recomendaciones), y éstas pueden ser emisión de órdenes, recomendaciones, advertencias, amonestaciones o avisos.
- Medidas de disuasión o instrucciones: Se caracterizan por ser disposiciones u órdenes que las autoridades pueden imponer en caso de advertir situaciones o prácticas que supongan la afectación potencial o real de los consumidores. Buscan la adopción obligatoria de medidas o el desarrollo de planes de acción orientados a corregir las falencias detectadas.
- Medidas sancionatorias: Determinaciones supervisoras que, después de un procedimiento (generalmente administrativo sancionatorio) llevan a la imposición de sanciones y medidas ejemplarizantes a los supervisados por incumplir normas en materia de protección de los consumidores. Las sanciones pueden ser institucionales o personales y comprenden llamados de atención, sanciones pecuniarias e incluso la prohibición temporal o definitiva de realizar una o varias operaciones o actividades. En algunas jurisdicciones la infracción al régimen de protección al consumidor es por sí misma una causal de agravación punitiva.
- Meta-regulación¹⁰: Por la cual los supervisados dan aplicación a mecanismos de gestión de los riesgos y la autoridad supervisa el funcionamiento de dichos mecanismos.

10 Cunningham, Neil. *Enforcement and Compliance Strategies*, en The Oxford Handbook of Regulation, Oxford University press, 2010.

CONTAR CON MECANISMOS DE COOPERACIÓN ENTRE AUTORIDADES RELEVANTES, PARA LA PROTECCIÓN ACTIVA DE LOS CONSUMIDORES FINANCIEROS

Existen varias razones para que los supervisores se comprometan y cooperen de manera activa y efectiva con otras autoridades a cargo de la supervisión en relación con las empresas que prestan productos y/o servicios provenientes de innovaciones tecnológicas.

Una de éstas es que ayuda a los supervisores a obtener una visión general de las implicaciones de las Fintech (diferentes sectores, transfronterizos, tecnológicos, lavado de dinero, protección de datos, etc.) y también que puede ayudar a coordinar esfuerzos, evitar solapamientos regulatorios e identificar riesgos potenciales. Por lo que se espera que exista una cooperación o delegación clara de funciones con respecto a:

- Autoridad de protección al consumidor.
- Reguladores relevantes en cada jurisdicción.
- Otros supervisores financieros en cada jurisdicción.
- Autoridad antilavado de dinero.
- Autoridad de protección de datos.
- Otros supervisores fuera de la jurisdicción.
- Autoridad de competencia.
- Regulador de telecomunicaciones.

Por otro lado, se espera que las autoridades muestren un enfoque proactivo en la firma de acuerdos formales de cooperación con reguladores y supervisores en el extranjero por medio de memorandos de entendimiento (MoU), principalmente para el intercambio de información y comités conjuntos para abordar los problemas de supervisión de las Fintech. Así mismo, al interior de cada jurisdicción se requiere la colaboración respecto a temas de ciberseguridad y la posibilidad de apoyar a centros de innovación.

La coordinación de enfoques normativos y de supervisión, así como los análisis conjuntos contribuyen de manera significativa a evitar arbitrajes y sincronizar el tratamiento que se da tanto a incumbentes como a nuevos prestadores de servicios Fintech con presencia regional.

CONTAR CON FACULTADES PARA ADAPTAR LOS REGÍMENES DE LICENCIAMIENTO Y AUTORIZACIÓN

Ante la eventual ampliación del perímetro de regulación y supervisión de nuevas entidades proveedoras de servicios y productos digitales, las reglas generales de licenciamiento deberán poderse adaptar para considerar las oportunidades, retos y riesgos planteados por las nuevas empresas Fintech, aumentando el enfoque en la comprensión de los modelos de negocios y la naturaleza de las nuevas relaciones con los consumidores financieros.

Las autoridades deberán contar previamente con estas atribuciones para que la ampliación del perímetro regulatorio se lleve a cabo de manera sostenible. Por ejemplo, la introducción de *sandboxes regulatorios*, en ciertas jurisdicciones con características particulares, puede desempeñar un papel clave en los procesos de autorización al proporcionar un mecanismo para observar las operaciones del nuevo proveedor Fintech antes de aprobar su licencia.

CONTAR CON ESTRATEGIAS INTEGRALES DE EDUCACIÓN FINANCIERA RELACIONADAS CON LA PROTECCIÓN DEL CONSUMIDOR FINANCIERO, DIRIGIDAS A AUMENTAR LA CONCIENCIA DE LOS CONSUMIDORES SOBRE LOS RIESGOS INHERENTES AL USO DE PRODUCTOS Y SERVICIOS FINANCIEROS Y QUE CONTRIBUYAN AL OBJETIVO DE MITIGAR LOS RIESGOS PARA LOS CONSUMIDORES

La Educación Financiera (EF) es el fundamento de una estrategia robusta de protección al consumidor financiero, toda vez que propicia que el usuario construya desde su propio ámbito una primera línea de conocimiento y protección que le permita escoger los productos y servicios más adecuados a sus necesidades y posibilidades, conocer los atributos, costos y riesgos de determinados productos y prestadores, y, especialmente, conocer sus deberes y derechos en el manejo de éstos.

Se considera una precondition el que el supervisor financiero cuente con programas de EF o participen en el diseño e implementación de estrategias y acciones. Su experiencia en el campo como autoridad de supervisión le concede una posición privilegiada para determinar los aspectos que resultan fundamentales para incrementar los niveles de protección, aquellos en los cuales debe concentrarse la formación a los consumidores y las maneras más adecuadas para construir un enfoque pedagógico eficaz.

Por lo tanto, en los programas de EF las autoridades de supervisión deben evitar que los objetivos del programa sólo se limiten a explicar los riesgos asociados con ciertos productos o servicios tecnológicos, sino que deberán, en mayor medida, promover actitudes preventivas por parte de los consumidores de productos. Es conveniente que los programas que estén establecidos en las jurisdicciones fomenten el desarrollo y divulgación de temas específicos, entre éstos:

- Nuevos productos y servicios financieros;
- Manejo responsable de herramientas y recursos digitales;
- Identificación adecuada de incumbentes y proveedores;
- Presentación y trámite de quejas y reclamaciones;
- Riesgos.

Adicionalmente, las ARS pueden emitir advertencias y avisos a los consumidores respecto a los servicios y prestadores en los cuales se han presentado fallas significativas en la prestación del servicio.

CONTAR CON Y/O CAPACITAR EQUIPOS CON EXPERTICIA DIGITAL APLICADA A LOS CONSUMIDORES Y EVALUACIÓN DE SUBCONTRATACIÓN TECNOLÓGICA

Los supervisores de las Tecnologías de la Información (TI) usualmente no están involucrados en la supervisión de los riesgos del consumidor financiero, y menos a los asociados a las Fintech. Las autoridades que tienen un mandato de supervisión prudencial cuentan con grupos

especializados en la evaluación de TI (riesgo operacional) y no de supervisión conductual, en general. Por lo tanto, para enfrentar el desafío digital Fintech es recomendable que, para desarrollar y aplicar un marco de regulación y supervisión de manera eficaz, los supervisores:

- Capaciten y mantengan actualizado al personal existente para que desarrollen y apliquen el conocimiento técnico suficiente para analizar y controlar adecuadamente la nueva tecnología financiera compleja;
- Aumenten la cantidad de supervisores de TI disponibles para la supervisión de la conducta y garanticen que tengan habilidades específicas relevantes para supervisar los productos y servicios ofrecidos por Fintech;
- Hacer que los supervisores de TI sigan un enfoque que, basándose en el riesgo de TI, analice los riesgos para los consumidores a lo largo del ciclo de vida del producto.

Por otro lado, las entidades tradicionales y las nuevas prestadoras de servicios Fintech subcontratan ciertos procesos o actividades relevantes para la provisión de productos y servicios tecnológicos ofrecidos en línea y estos proveedores de plataformas en línea pueden no estar ubicados en la jurisdicción donde se comercializan los productos y servicios.

Aunque la responsabilidad de las actividades subcontratadas debe permanecer en la entidad financiera supervisada, las autoridades de supervisión suelen revisar los acuerdos a través de un enfoque prudencial, es decir, evaluando los posibles riesgos de TI. En esa evaluación deberán ampliar el alcance para analizar la mayoría de los contratos suscritos, o al menos una muestra relevante, entre entidades supervisadas y proveedores de servicios de tecnología externos en relación con los productos y/o servicios provenientes de innovaciones tecnológicas, buscando establecer, entre otras, situaciones que puedan afectar la adecuada atención y protección del consumidor.

CONSIDERACIONES Y RECOMENDACIONES GENERALES

Para que las Fintech puedan llevar a cabo sus ideas y propuestas de emprendimiento, los reguladores y supervisores enfrentan un desafío: permitir a los proveedores llevar a cabo sus modelos de negocio sin menoscabar la protección de los consumidores, las condiciones de igualdad, la integridad de los mercados financieros y la estabilidad del sistema financiero en su conjunto.

El *European Banking Authority* (EBA) publicó en marzo de 2018 su hoja de ruta sobre las Fintech¹¹, donde propone las siguientes acciones:

- Abordar aspectos de autorización y del perímetro regulatorio relacionados con las Fintech. Esto incluye la evaluación de los procesos de autorización y licencia actuales de las entidades Fintech, y el análisis de los *sandboxes regulatorios* y los centros de innovación.
- Desarrollar temas de protección a los consumidores. Se identificarán cuestiones derivadas de la Fintech que afecten a los consumidores, en concreto, relacionadas con áreas donde no está clara la regulación de las entidades Fintech ni la divulgación de información a los consumidores.
- Analizar el impacto sobre los modelos de negocio de las entidades, así como los riesgos prudenciales y las oportunidades derivadas del uso de la Fintech. Se debe observar cómo las entidades hacen frente a los riesgos y cómo adaptan sus marcos de gobierno interno, control y gestión del riesgo.
- Promover mejores prácticas de supervisión para la evaluación de la ciberseguridad y para el estable-

cimiento de un marco común de evaluación de las amenazas cibernéticas.

- Identificar y evaluar los riesgos del Lavado de Dinero y Financiamiento al Terrorismo (AML/CFT) procedentes de las entidades Fintech, de los proveedores de dicha tecnología, y de las soluciones Fintech.
- Crear un *Fintech Knowledge Hub* que proporcionará un foro general para integrar a las autoridades competentes.

En este contexto, muchos proveedores denominados incumbentes han planteado una problemática según la cual estarían operando en “campos de juego” desiguales y riesgos de arbitraje regulatorio. En tal sentido, para mantener un “campo de juego” nivelado se ha propuesto seguir un principio de **mismas actividades, mismos riesgos, mismas reglas y misma supervisión**, para que todas las empresas que realizan actividades y tienen riesgos similares reciban el mismo trato en términos de regulación y supervisión.

Actualmente, existe un debate acerca de la idoneidad de establecer una regulación diferenciada basada en el tipo, tamaño y complejidad de las operaciones. En este sentido, se debe considerar que los riesgos prudenciales se evalúan teniendo en cuenta la combinación de las actividades emprendidas por una entidad y su modelo de negocio, lo cual hace que la supervisión prudencial esté basada en la entidad y sea posible aplicar requisitos diferenciales.

Sin embargo, a nivel conductual, productos y servicios específicos pueden conllevar riesgos similares para el

11 <https://eba.europa.eu/-/eba-publishes-its-roadmap-on-fintech>

consumidor, cualquiera que sea la entidad que los suministre, y deben regularse en consecuencia.

De esta manera, con el fin de que se garantice la igualdad de condiciones sin recurrir al arbitraje regulatorio, se recomienda a las autoridades considerar las siguientes consideraciones y recomendaciones mínimas:

MISMAS ACTIVIDADES Y SERVICIOS COMPARTEN LOS MISMOS RIESGOS FRENTE AL CONSUMIDOR, POR LO QUE DEBE APLICARSE LA MISMA REGULACIÓN, INDEPENDIEMENTE DEL TIPO DE ENTIDAD JURÍDICA QUE LAS SUPERVISE

Para aplicar este principio las ARS deben idear modos de obtener información adecuada del ecosistema Fintech presentes en sus jurisdicciones a fin de realizar seguimiento de los avances tecnológicos, segmentos de mercado atendidos y el constante análisis de ventajas y posibles riesgos, especialmente en lo que concierne a la protección de los consumidores y los inversores, así como su inclusión financiera.

De esta manera se propone desarrollar y fomentar el conocimiento que las autoridades tienen del ecosistema Fintech, con especial énfasis en los proveedores de estos productos o servicios, aun cuando éstos desempeñen su actividad por fuera de su ámbito natural de supervisión (perímetro). Este conocimiento puede construirse, por ejemplo, a través de un registro electrónico central público, que contenga una lista de todas las empresas Fintech y sus respectivas filiales (ya sea que estén dentro del perímetro de supervisión o por fuera de éste).

El registro puede ser administrado por un organismo diferente a la autoridad de supervisión, como un Ministerio de economía o de industria, o un órgano equivalente a las cámaras de comercio o registrador a cargo de la gestión de registros públicos.

El registro es tan sólo una herramienta de mapeo del ecosistema lo cual **no implica ningún tipo de supervisión.**

Será, entonces, necesario comunicar al público que el hecho de que una empresa se encuentre inscrita en el registro no conlleva ningún tipo de vigilancia sobre estas entidades. Ésta es la razón por la cual es altamente recomendable que el registro no sea llevado por la autoridad de supervisión, pues así se evitaría generar expectativas en los consumidores y se prevendría el uso inadecuado de la expresión “registro” como una forma de dar una aparente condición de supervisión financiera.

Es recomendable que el conocimiento del ecosistema incluya al menos la siguiente información para todas las Fintech existentes (dentro o por fuera del perímetro):

1. Tipo de sociedad jurídica o personal.
2. Nombre de la sociedad.
3. Principales accionistas de la sociedad.
4. Nombre comercial de la sociedad.
5. Dirección, ciudad, país, código postal.
6. Datos de contacto de atención al consumidor.
7. Número de identificación nacional.
8. Fecha de constitución de la sociedad.
9. Una lista pre-definida en donde se tipifiquen los diferentes segmentos Fintech a los cuales puede pertenecer la sociedad.
10. Una breve descripción de los productos y/o servicios ofrecidos junto con la dirección de la página web y/o aplicación móvil.
11. El país o países donde se realizará el servicio o venta de productos, incluida la ubicación (es decir, el país o la región) de los datos recolectados.

Para garantizar un suministro uniforme de información, las ARS financieras y concurrentes deberían coordinarse en el uso de un formato estandarizado para hacer el levantamiento de la información y permitir a los consumidores comprender fácilmente la información contenida en el registro central electrónico de manera clara y sin ambigüedades.

Al aplicarse esta recomendación a las empresas pertenecientes al ecosistema Fintech, será más sencillo identificar e introducir al perímetro de regulación y supervisión

financiera sólo a aquellos proveedores que realicen **las mismas actividades que tradicionalmente son autorizadas** por el supervisor financiero, dejando por fuera del perímetro del supervisor financiero empresas cuyo modelo de negocio no requiera un esquema de licenciamiento financiero.

Dada la evolución constante de las actividades propuestas en el ecosistema Fintech, en adición al criterio anterior los supervisores deberán considerar si nuevas formas de negocio suponen:

- Diferencias significativas respecto de esquemas tradicionales de captación masiva de recursos del público o de otras actividades reservadas a instituciones supervisadas, por ejemplo, en el ámbito de seguros o de mercado de valores;
- Modelos masivos de manejo o acumulación de dinero de consumidores de distintas características, así no se enmarquen en los criterios tradicionales de captación;
- Actividades que generen esquemas de negocio con vinculación masiva de consumidores que tiendan a sustituir la funcionalidad que tradicionalmente presta una institución supervisada, planteando una "desintermediación" o "desinstitucionalización financiera". En estos casos deberá evaluarse cada caso para considerar la conveniencia o no de su incorporación al perímetro.
- Algunas actividades Fintech que por su dimensión y rol se vuelven de importancia crítica en procesos transaccionales, operativos o de gestión en instituciones financieras sistémicas o en varias instituciones financieras.

Los proveedores de productos y servicios que resulten incluidos en el perímetro de regulación y supervisión financiera deberán contar con una guía de licenciamiento. Aquellas empresas que lleven a cabo actividades similares a las instituciones financieras tradicionales entrarían directamente bajo el esquema de licenciamiento tradicional y la regulación presente en cada jurisdicción, como puede ser el caso de neo-bancos y neo-aseguradoras.

Sin embargo, para las empresas Fintech realmente disruptivas en su modelo de negocio y cuya aplicación del esquema tradicional de licenciamiento resulte complicada y costosa en materia de capital, sistemas de gestión de riesgo, operaciones y alcances, entre otras, las ARS pueden considerar trabajar en esquemas de "licenciamiento con requerimientos mínimos prudenciales", para que dichas empresas desarrollen su actividad de forma condicionada y con ciertas restricciones dentro del perímetro de supervisión.

Solo para las Fintech que cuenten con un modelo de negocio nuevo, disruptivo y sofisticado, las ARS podrán considerar poner a disposición espacios de experimentación controlada o *sandboxes regulatorios*, siempre y cuando su contexto y marco legal lo permitan.

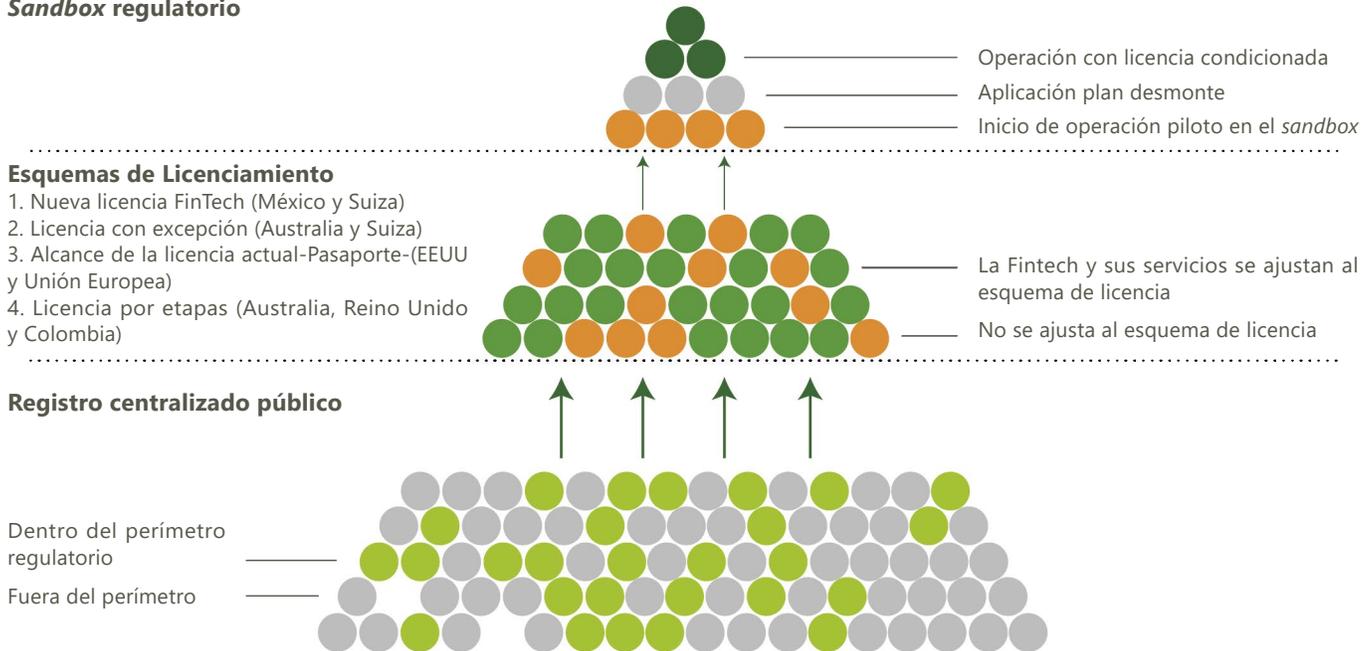
Lo anterior podría permitir autorizaciones temporales por parte de las autoridades para poder implementar productos o servicios innovadores en ambientes controlados, así como ajustes prudentes a la normatividad para impulsar el valor agregado potencial hacia los clientes, la conveniencia y la sostenibilidad en el tiempo de estos nuevos productos o servicios (figura 1).

Al analizar el carácter disruptivo de un modelo de negocio Fintech las autoridades deberán solicitar a las empresas:

- La acreditación de la novedad que plantea la iniciativa Fintech, explicando en detalle en qué consiste su variación material frente a las formas tradicionales de prestación tanto en la jurisdicción como en mercados más desarrollados;
- Deberá indicarse si la tecnología introduce una verdadera novedad en procesos específicos de la entidad vigilada: conocimiento del mercado, segmentación y vinculación con clientes, monitoreo y gestión de riesgos, prestación del servicio, atención de peticiones de quejas y reclamos, entre otras.
- La forma como esa innovación incidirá en el modelo de negocio, especialmente potenciando la capacidad de vinculación con clientes y de prestación novedosa de servicios;

Figura 1. Procesos de registro, licenciamiento y *sandbox* para las Fintech

Sandbox regulatorio



- La forma en la que el esquema o la herramienta disruptiva de prestación incidirá en el modelo de negocio, el apetito de riesgo y la condición financiera y patrimonial de la entidad.

EL ENFOQUE DE SUPERVISIÓN DEBE SER BASADO EN RIESGOS, PERO TENIENDO PRESENTE LA PROPORCIONALIDAD DE LAS ACCIONES DE SUPERVISIÓN OBSERVANDO EL MODELO DE NEGOCIO, TAMAÑO, IMPORTANCIA SISTÉMICA, ASÍ COMO LA COMPLEJIDAD Y ACTIVIDAD TRANSFRONTERIZA DE LAS FINTECH

Para maximizar la efectividad en la supervisión y minimizar un efecto negativo en la innovación tecnológica por parte de las Fintech, cualquier acción supervisora debe, en lo posible, promover un comportamiento deseable y desalentar el comportamiento indeseable por parte de las empresas, y, al mismo tiempo, limitar los costos de cumplimiento.

De no adoptarse un enfoque proporcional en las acciones supervisoras, los innovadores temerán ser castigados por cada error y serán menos asertivos al tratar de

desarrollar la próxima aplicación de tecnología financiera, para dedicar más tiempo y esfuerzo al cumplimiento. Por ejemplo, penalizar a una empresa por una pequeña infracción técnica en la normativa de seguridad de la información o en la de protección al consumidor que causa poco o ningún daño a los consumidores probablemente empujará a la empresa a gastar más recursos en abogados en lugar de mejorar su oferta de servicios.

En caso de identificar una falta por parte de los proveedores de servicios Fintech, se recomienda que las acciones supervisoras se fundamenten en dos criterios: 1) si la empresa actuó de manera intencional o si la empresa actuó de forma negligente y, 2) si la acción de la empresa resultó en un daño real para el consumidor. De esta forma, los supervisores, usando criterios de proporcionalidad, determinarán las sanciones, donde las acciones no intencionales e inofensivas que no generen efectos materiales adversos podrían no recibir ninguna penalización y las acciones intencionales, negligentes y dañinas con el consumidor reciben una penalización severa.

Desde esta perspectiva se disminuirá la posibilidad de bloquear los procesos de innovación, pero al mismo

tiempo se enviarán señales claras a los proveedores sobre comportamientos no deseados que desprotegen a los consumidores.

Es importante resaltar que la aplicación de esta recomendación deberá considerar las posibilidades que los marcos legales les brindan a los supervisores, de forma que siempre debe quedar al criterio discrecional de la autoridad estimar su procedencia, así como definir normas mínimas aplicables y procedimientos para verificar su cumplimiento.

ADOPTAR LA NEUTRALIDAD TECNOLÓGICA EN LA REGULACIÓN DE FORMA QUE NO SE INHIBA EL USO DE DETERMINADAS TECNOLOGÍAS NI SE GENEREN SESGOS EN FAVOR DE OTRAS

Los modelos de negocio de las Fintech no son homogéneos por lo que los reguladores deben adoptar reglas neutrales a la tecnología que no favorezcan ni perjudiquen a ninguna aplicación de Fintech en particular, para crear un campo de juego nivelado para la innovación.

Cuando existen diferencias en las tecnologías, los supervisores deben estar atentos a reconocer los diferentes riesgos en las herramientas y aplicaciones particulares de las Fintech.

PROMOVER LA ARMONIZACIÓN Y REMOVER LA DUPLICACIÓN DE REGULACIÓN QUE AFECTE LA PROTECCIÓN DE LOS CONSUMIDORES FINANCIEROS

En la región, algunas ARS financieras no tienen competencias plenas (o sus facultades son parciales) en temas de protección al consumidor como servicio al cliente, mercadeo (marketing), publicidad, información y asesoría, temas contractuales, quejas y reclamos. Igualmente, se identifican algunas autoridades que regulan el tema de manera general aplicando la normativa a las Fintech no de manera específica sino en virtud de una competencia genérica, por lo que en ciertos casos se puede presentar

un mosaico de normativas que rigen a las compañías de tecnología financiera y pueden crear requisitos duplicados de múltiples reguladores, por ejemplo, en los requisitos de divulgación de información al consumidor que son a menudo la pieza central de las regulaciones de protección financiera del consumidor.

Por lo tanto, es necesario que las autoridades de regulación y supervisión financiera trabajen estrechamente con las autoridades de protección al consumidor en el diseño de un plan de acción para llevar a cabo una actualización de la regulación de protección al consumidor que preste especial atención a las necesidades de los consumidores financieros e inversores minoristas y a los riesgos a los que pueden ser vulnerables.

En el componente regulatorio es fundamental que, en el arreglo institucional, la preparación de la normativa aplicable a las empresas y actividades Fintech radique en una autoridad experta (sea el supervisor u otra que cuente con la colaboración o la participación activa del supervisor financiero). Dicha autoridad deberá tener facultades para monitorear el desarrollo de la industria Fintech, conocer los avances normativos y mejores prácticas en la materia y preparar las iniciativas regulatorias que incorporen aspectos específicos de protección al consumidor.

Además, la autoridad deberá evaluar constantemente la pertinencia del perímetro regulatorio para discernir cuando una actividad que queda fuera de su perímetro tenga que sujetarse a la regulación y supervisión financiera, debido a la realización de una actividad financiera o a la captación masiva de dinero de clientes.

Donde se presente superposición regulatoria, los responsables de formular la regulación deben esforzarse en coordinar y centralizar estas actividades para agilizar el proceso y reducir la carga regulatoria sobre las empresas de tecnología financiera, o solicitar nuevos poderes o atribuciones para atender la creciente expansión de la tecnología financiera en servicios como financiación colectiva, plataformas de pago, préstamos entre particulares y banca virtual.

Según el contexto de cada jurisdicción debe evaluarse la eficacia de la coordinación interinstitucional. Si el marco normativo en el cual se desenvuelven las autoridades lo permite, podrían considerarse asignaciones o delegaciones concretas de actividades que permitan definir autoridades responsables, evitando que, ante el riesgo de solapamiento de competencias, lo que ocurra sea la ausencia de una supervisión efectiva.

LOS SUPERVISORES FINANCIEROS DEBEN FOMENTAR LA COORDINACIÓN ENTRE LOS SUPERVISORES CONCURRENTES, SEGÚN CORRESPONDA, PARA QUE LA SUPERVISIÓN DE LAS FINTECH SEA MÁS EFICAZ

Las empresas Fintech recopilan grandes cantidades de datos sobre sus clientes, incluida información personal confidencial (biometría) y registros financieros. Igualmente, recopilan cada vez más datos alternativos, como los relacionados con el comportamiento de gasto en línea de un cliente y los patrones de redes sociales para rastrear la huella digital. Esta recopilación de información personal usada para productos y servicios financieros conduce a que diferentes supervisores tengan objetivos de supervisión sobre una misma empresa, en este ejemplo, una autoridad de supervisión financiera y una autoridad de protección de datos personales.

Es así como la regulación vigente a nivel regional sobre protección de datos personales, derivada en la mayoría de los casos del reglamento de protección de datos europeo (GDPR, por sus siglas en inglés), ya cubre algunos de los problemas de protección de datos derivados de Fintech. Pero los desarrollos de la tecnología están

expandingo continuamente nuevas áreas en las que reglamentación adicional o refinada puede ser requerida, y, con ello, también la coordinación entre autoridades de supervisión.

LOS SUPERVISORES DEBEN MONITOREAR LA ACTIVIDAD FINTECH POR FUERA DEL PERÍMETRO REGULATORIO, MANTENIENDO LA ATENCIÓN EN LAS TENDENCIAS DE TECNOLOGÍA FINANCIERA Y CONSIDERANDO SU IMPACTO POTENCIAL EN LA PROTECCIÓN DEL CONSUMIDOR

Las autoridades de supervisión son una parte clave del marco general de protección al consumidor y dado el ritmo y la escala de la innovación tecnológica, cada vez es más difícil para los reguladores determinar qué es lo que se regula y lo que queda fuera del perímetro. Por esta razón, cuando la innovación se relaciona con servicios y productos que están fuera del alcance, hay que ser conscientes de los riesgos que pueden suponer para los consumidores y tener una regla para involucrarlos dentro del perímetro.

Una propuesta de regla puede estar relacionada con el escalamiento en el número de clientes por parte de una Fintech fuera del perímetro. Cuando este número alcance un porcentaje por encima de la media de clientes de otras Fintech vigiladas debería entrar dentro del perímetro de supervisión, y esta regla debe ser clara, coordinada con otras autoridades y comunicada al mercado.

En adición a lo anterior, pueden considerarse los criterios previstos en la página 20 de este mismo documento.

CONSIDERACIONES Y RECOMENDACIONES CON RESPECTO A LOS DEBERES Y DERECHOS DE LOS CONSUMIDORES FINANCIEROS DIGITALES

Además de las consideraciones y recomendaciones establecidas en la sección anterior, y de los marcos nacionales de protección al consumidor que aplican a todos los proveedores financieros, sean tradicionales o Fintech¹², las empresas de innovación financiera tienen deberes de protección hacia sus consumidores, que son **transversales** a los segmentos de productos identificados (depósitos y créditos, pagos, seguros, gestión de inversiones, infraestructura y apoyo de mercados y recaudación de capitales). Por su parte, los consumidores tienen derechos, pero también deberes en este nuevo entorno.

DEBERES DE LAS FINTECH HACIA EL CONSUMIDOR

Con el fin de entregar los productos idóneos a sus clientes, las Fintech colocan al consumidor en el centro de todo lo que hacen. Sin embargo, para mantener esta premisa de valor que distingue a estas empresas, se deben considerar los riesgos tradicionales que enfrentan los consumidores: financieros, fraude, uso indebido de datos personales y financieros, perfilamiento, cibercrimen, entre otros.

Asimismo, se deben considerar nuevos enfoques de riesgo relacionados con el tipo de comportamientos que pueden generar las empresas y el mercado en los consumidores, y el posible relajamiento de controles de verificación debido a la personalización de los productos y a la digitalización de los procesos.

A continuación, se desarrolla una serie de consideraciones y recomendaciones mínimas que las autoridades y los proveedores de servicios Fintech deben tomar en cuenta al momento de abordar asuntos relacionados con la conducta hacia los consumidores.

Realizar la evaluación del riesgo de protección al consumidor en todo el ciclo de vida del producto: desarrollo del producto, venta o proceso transaccional y postventa

El riesgo de protección al consumidor parte de la definición del riesgo conductual como el riesgo de que el comportamiento de una entidad de servicios financieros, a lo largo del ciclo de vida del producto, ocasione afectaciones e impactos indeseados a los clientes. Se deberá contar con mecanismos transparentes y efectivos de divulgación de información y asesoría a los consumidores.

Las asociaciones Fintech han planteado de manera casi uniforme la preocupación de que se les exige proporcionar demasiada información, lo que provoca que los consumidores no revisen toda la información que se les presenta y esto puede exacerbarse en un entorno digital. Lo anterior parece estar avalado por análisis llevados a cabo por la *European Insurance and Occupational Pensions Authority* (EIOPA)¹³, que destacan que los consumidores pueden estar menos inclinados a leer la revelación de

¹² <https://www.ftc.gov/policy/international/competition-consumer-protection-authorities-worldwide>

¹³ https://www.eiopa.europa.eu/sites/default/files/publications/opinions/opinion_on_sale_via_the_internetpublished.pdf

información estándar de los documentos que describen los detalles de los productos al comprar en línea.

Por su parte, la Comisión Europea en su Plan de Acción afirma que la retroalimentación recibida de la industria sugiere que los requisitos actuales de divulgación precontractual no se ajustan al mundo digital. En las respuestas entregadas a la EBA por parte de la industria en relación con el *European Commission's Green Paper*¹⁴ sobre servicios financieros minoristas, se sugirió el uso de plataformas más interactivas y atractivas, que estén adecuadas para teléfonos inteligentes o tabletas y que mejoren la comprensión de los consumidores de los productos financieros.

La adopción por parte de los clientes de nuevos servicios digitales requiere que el acceso a estas tecnologías sea explicado en lenguaje entendible, que dichas tecnologías sean popularizadas y validadas por un organismo competente (por ejemplo, que una transacción electrónica cumple con los estándares de un organismo certificador), y que los términos y condiciones con los que se presta esta tecnología estén redactados de manera clara, de modo que brinden confianza al cliente para su adopción.

Por lo tanto, el suministro de información a los consumidores es clave en los marcos de protección al consumidor establecidos y tiende a desarrollarse a través de las diferentes etapas de la relación contractual entre cliente y proveedor. Algunas recomendaciones de divulgaciones innovadoras que se pueden promover son:

i) Durante la celebración del contrato

- Sugerir a las nuevas empresas e incumbentes que ofrecen productos Fintech adoptar los cuatro pasos de diseño de comportamiento en sus productos y servicios¹⁵:
 - a) Capturar atención: alinear el producto y servicio con la necesidad del consumidor; incorporar

recordatorios y alertas inteligentes; interrumpir los hábitos y redirigir la atención; poner a disposición el contacto humano.

- b) Inspirar confianza: dar transparencia al proceso; usar señales visuales y signos de seguridad; cuidar el tono y estilo de comunicación con los consumidores.
 - c) Simplificar la decisión: facilitar el entendimiento de la selección; estructurar la elección de una manera que ayude a los consumidores a decidir.
 - d) Facilitar la acción: eliminar requisitos que puedan involucrar múltiples pasos o pasos inciertos; dar al consumidor una idea del progreso que está haciendo, desde afirmar que ya ha dado el primer paso para recordarle que está cerca de completarse el proceso.
- Hacer uso de infografías y herramientas interactivas para presentar información difícil; o hacer uso de videos para explicar información compleja a los consumidores; creación de guías de tamaño ajustado al medio; hacer uso de citas virtuales, y permitir a los clientes abrir "demos" para probar nuevos productos y servicios. Todo lo anterior, con el objetivo de ayudar a los consumidores a tomar una decisión respecto a la adquisición de un producto o servicio financiero teniendo claridad sobre: el tipo de operación que va a ejecutar, el alcance del servicio que va a recibir, el manejo de los recursos otorgados, los riesgos inherentes y costos asociados.
 - Como se pretende que la información relacionada a términos y condiciones del producto sea leída por un consumidor de manera fácil en un teléfono inteligente o dispositivo móvil, el uso de texto puede no ser práctico, por lo que es más beneficioso para los consumidores si a las empresas optan por presentar la información y las advertencias en las formas antes señaladas, pero debe exigirse a las empresas que obliguen a los clientes a pasar tiempo en las pantallas de términos y condiciones y disminuir la posibilidad de que ignoren esta información.
 - Se debe detallar la totalidad de los costos ordinarios del producto, expresados tanto en una suma de

¹⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0630&from=EN>

¹⁵ Katy Davis, Maddie Kau, and Abigail Kim. Behavioral Design for Digital Financial Services.

- dinero como en tasa porcentual anual, así como los costos de cualquier otro producto o servicio que se incluya en el mismo paquete del producto principal. Igualmente, se deben presentar con claridad las fechas en que se tienen que efectuar los pagos y los montos correspondientes, así como las tasas por mora y el momento en que se aplican.
- Se debe informar de forma simple y transparente al cliente sobre el uso y el manejo de los datos de los consumidores, y desarrollar formas eficaces de informar sobre dicho uso y sobre las prácticas en el manejo de datos antes de que se origine el producto o servicio en cuestión, de acuerdo con las normas de protección de datos personales.
 - La gestión automatizada de inversiones, por sus características, limita la intervención humana, pero se puede y se debe proporcionar acceso a un operador humano para ayudar al cliente a lo largo del proceso, en caso de que así lo requiera. Esto es relevante en particular cuando el conocimiento financiero o digital del cliente es bajo.
 - Debe existir balance entre la apertura de los productos y servicios y el cierre de éstos. En la mayoría de los productos y servicios digitales la promoción y apertura de productos se hace a distancia, sin interacciones personales durante la solicitud de productos y en procedimientos breves. Sin embargo, en el cierre o cancelación de los productos y servicios se introduce un tipo de “fricción” que limita el derecho de los consumidores financieros a dar por terminado los contratos.

ii) Durante la ejecución del contrato

- Las empresas Fintech deben abstenerse de incurrir en conductas que conlleven abusos contractuales o de convenir cláusulas que puedan afectar el equilibrio del contrato o den lugar a un abuso de posición dominante contractual.
- Deben evitarse cláusulas o términos abiertamente abusivos como los relacionados con la posibilidad de dar por terminado el servicio en cualquier momento por parte del prestador; asignarse obligaciones al consumidor mas no al proveedor; exenciones

ex-ante de cualquier responsabilidad al proveedor, en particular, ante fallas operativas y disponibilidad del servicio; falta de estados de cuenta sobre el producto; y términos contractuales en idioma diferente al de la jurisdicción.

- Cumplir con las condiciones anunciadas en páginas web, redes sociales, medios físicos, aplicaciones móviles y en las estrategias de empuje (*push*) no solicitadas por el cliente, frente a las funcionalidades reales del producto o servicio suministrado.
- Abstenerse de usar cifras y testimonios falsos o no comprobables e indebida descripción de las características de los productos financieros digitales.
- Se debe contar con procedimientos para informar a los consumidores sobre los incidentes cibernéticos que se hayan presentado y en los que podrían verse afectadas la confidencialidad o integridad de la información personal y/o financiera, al igual que las medidas adoptadas para solucionar la situación.
- El otorgamiento de información debe distinguirse claramente de la provisión de asesoría para evitar incertidumbre entre los clientes. En particular, los proveedores de servicios Fintech deben distinguir entre herramientas orientadas al consumidor y herramientas orientadas a asesoría. Es decir, deben aclarar cuando una recomendación / información general se convierte en “consejo de asesoría”; distinguir entre procesos parcialmente automatizados y otras herramientas automatizadas, y establecerse requisitos de supervisión iguales tanto para el asesoramiento automatizado como para el asesoramiento proporcionado por un asesor humano.

iii) Durante la terminación del contrato

- Sólo si la naturaleza del producto lo permite, la empresa prestadora debe facilitar el derecho de desistimiento de un contrato al cliente y dejar sin efecto el contrato celebrado, notificándose en el plazo establecido para el ejercicio de ese derecho, sin necesidad de justificar la decisión y sin penalización de ninguna clase. En estos casos procederán los cobros correspondientes según el tipo de servicio y el grado de ejecución de la operación.

- Se debe establecer claramente el procedimiento para la terminación de la relación contractual, que ésta pueda realizarse a través de los mismos canales que se ponen a disposición para la celebración del contrato, y sin imponer a los clientes mayores requisitos a los solicitados al momento de la celebración de éste para terminar el servicio.

Incorporar requerimientos de idoneidad

Existe el riesgo de que los clientes, buscando hacerse con un producto o servicio que desean, respondan de forma sesgada a las preguntas que hacen los proveedores para identificar la opción más adecuada para ellos. En general, se ha observado que los consumidores recurren a esta acción en mayor medida cuando interactúan en línea o en el móvil, en comparación con cuando están frente al proveedor o intermediario financiero.

Por lo anterior, los proveedores de Fintech deben adoptar requerimientos de idoneidad hacia sus clientes para asegurarse de que cualquier producto vendido es adecuado a las necesidades y circunstancias del consumidor. Las disposiciones claves de idoneidad están asociadas con:

- El proceso de conocer al cliente (KYC) por el cual las Fintech deben recopilar información suficiente y verificable para segmentar mejor su clientela actual y potencial, además de evaluar si el producto o servicio es adecuado para un consumidor particular antes de ofrecerlo. Por ejemplo, en el caso de los créditos personales la segmentación debe poner atención a la real capacidad de pago y dirigir los esfuerzos a los casos que muestran un uso adecuado de los fondos.
- Los recursos humanos y técnicos de la industria Fintech deben estar orientados a propiciar que la recomendación que se dé a un cliente o potencial cliente sea la más adecuada para sus necesidades, expectativas y posibilidades.

Disponer de un adecuado proceso de gestión de quejas

Un sistema eficiente de manejo de quejas se considera un indicador efectivo de los procedimientos, controles, necesidades de capacitación y niveles de servicio en todas las empresas. Ejemplos de manejo adecuado de quejas incluyen:

- Centralización de todas las quejas dentro de las empresas con procesos claros al interior de todas las áreas involucradas.
- Implementación de soluciones de software especializado para la gestión de quejas.
- Estrategias de comunicación con el cliente, incluyendo las redes sociales y canales digitales populares.
- Seguimiento proactivo de las quejas a través de notificaciones automáticas.

Sin embargo, en las diferentes jurisdicciones suelen existir regulaciones que dispersan la gestión de quejas y que, en algunos casos, no siempre son coherentes, lo que dificulta el diseño de procedimientos eficaces. Por ejemplo, se cuenta con definiciones diversas sobre qué es una queja, reclamo y solicitud.

Ante la gestión de quejas, las Fintech deben:

- Tratar por igual la entrada de cualquier queja, solicitud o petición del consumidor en relación con el producto o servicio prestado que no se pueda solucionar en un plazo máximo de 24 horas. Ésta debe ser ingresada al sistema de gestión e incluir la identificación de la raíz de los problemas, con el propósito de garantizar que se resuelvan las quejas similares en conjunto en lugar de centrarse únicamente en la queja individual.
- Debe cumplirse con los tiempos de resolución para quejas, mandatorios en la normativa, y comunicarse al consumidor cuando una queja va a requerir más tiempo en su resolución indicando el motivo y la fecha definitiva de respuesta.

- Las empresas deben monitorear las expresiones de insatisfacción en los medios digitales y plataformas donde tienen presencia, y cuando se identifique la expresión de insatisfacción se debe invitar al consumidor a hacer una declaración formal específica e iniciar una queja a través de un proceso formal.
- Debe existir una base de datos con el registro de quejas (*log*) detallando cada queja, fecha de recibido, área a cargo de la solución, acciones tomadas para resolver, fecha de resolución, etc. El mantenimiento de esta base de datos debe estar resguardada en un medio duradero y guardarse en el tiempo indicado por la normativa para demostrar el cumplimiento de la regulación y para usarse en la identificación de la causa raíz.
- Los consumidores pueden tener preferencias diferentes sobre cómo quisieran hacer y gestionar sus quejas. Mientras una parte de la población prefiere entablar comunicación directa con la empresa, otra parte, particularmente aquella perteneciente a una generación más joven, prefiere y espera poder hacer quejas a través de canales digitales. En general, las entidades deberían poder ofrecer ambas opciones a los consumidores: la vía digital y la vía física.

Los proveedores de servicios Fintech dedicados a la gestión de inversiones deberían ofrecer el contacto físico si la queja o el reclamo no pudo ser resuelta por medio digital, o cuando el cliente explícitamente así lo solicite.

Tratar de manera justa a los clientes en cuanto al manejo de reclamaciones

En el componente de atención de quejas y reclamos, el marco normativo debe establecer con claridad la obligación de incumbentes y de nuevos proveedores de servicios Fintech de atender oportuna y eficazmente las quejas y reclamaciones de consumidores. Igualmente, deberá prever la manera como las ARS u otras autoridades competentes en materia de protección al consumidor habrán de atender, desde sus respectivas competencias,

aquellas quejas que los consumidores hagan de su conocimiento. Dichas quejas deberán alimentar constantemente el proceso supervisor.

Desde la perspectiva de protección al consumidor el principio subyacente con respecto al manejo de reclamaciones es que cualquier método innovador utilizado por los proveedores Fintech para atender dichas reclamaciones trate a los consumidores de una manera justa.

Las mismas metodologías que son empleadas en la fijación de precios y la suscripción, no deberían ser utilizadas para “optimizar” las propuestas de liquidación sobre la probabilidad estadística de que el asegurado/reclamante acepte la oferta, en lugar de emplear el valor razonable de la reclamación.

Los procesos existentes actuales, en particular en la industria aseguradora, son pesados en recursos humanos, con tareas administrativas onerosas y algunos pasos de decisión son discrecionales. Esto ha creado espacio para que las Fintech hayan innovado en el uso de aprendizaje automático y el reconocimiento de patrones para obtener ganancias de eficiencia, ahorros de tiempo y costos relacionados, así como precisión y consistencia en el análisis de reclamaciones analizando manuscritos y documentos no estructurados que agilizan y detectan falsos reclamos. Por lo cual, incumbentes y empresas Fintech deben:

- Asegurar que los consumidores reciban asesoramiento de alta calidad especialmente en lo que respecta a productos complejos que podrían ser difíciles de entender para un consumidor promedio, por lo que al cliente se le debe ofrecer asistencia en el proceso de reclamación.
- Debe estar a disposición del cliente el procedimiento escrito y a través de otros mecanismos de comunicación como se menciona en la sección “Asegurar un marco regulatorio y de supervisión para la protección de los consumidores financieros y la oportuna atención de quejas y reclamos” (p. 15) para el manejo efectivo y adecuado de reclamaciones.

- Debe ofrecerse información precisa en cuanto a los tiempos para informar al consumidor sobre el resultado de la reclamación, el plazo para consideración de la oferta de liquidación, y el plazo para la resolución de la reclamación después de la aceptación de la oferta por parte de los consumidores.

En la gestión de reclamaciones, los proveedores están haciendo análisis avanzado (*analytics*) y aprendizaje automático (*machine learning*) con datos personales para crear sistemas de alerta temprana y recopilar información práctica que evite accidentes, y que también simplifique y acelere el procesamiento de reclamaciones. Los ejemplos incluyen el uso de inteligencia artificial para detectar y verificar puntos reincidentes de accidentes, estimar costos de reparación e identificar posibles fraudes.

Por lo anterior, las empresas Fintech deben:

- Adoptar las medidas para proteger los datos personales de los consumidores durante la recopilación, procesamiento, corrección e intercambio, además de garantizar la seguridad de la información y de los datos, ajustándose a las normas de privacidad y normas en seguridad de la información destinadas a proteger estos activos ante incidentes cibernéticos, violaciones o uso no deseado.

Garantizar la retención de registros de los consumidores

A medida que aumenta la cantidad de transacciones digitales de los clientes, también aumenta el riesgo de pérdida de registros de los consumidores: condiciones, instrucciones, decisiones y cualquier otro detalle que demuestre que la empresa obró en el mejor interés del cliente y en cumplimiento de sus deberes. Se ha apreciado que las Fintech que prestan servicios de asesoría digital de inversiones en ocasiones no han podido revisar el consejo financiero individual brindado a algunos de sus clientes porque no han logrado tener acceso a los registros de

los clientes para determinar si fueron afectados con una pérdida financiera.

Asimismo, en la externalización del mantenimiento de registros digitales con proveedores tercerizados y, en particular, con proveedores con infraestructura en la “nube” se ha identificado como riesgo el evento de que los datos se corrompan o estén sujetos a ataques cibernéticos.

Ante las situaciones anteriores, algunos reguladores financieros han dispuesto que las empresas hagan un mantenimiento de registros digitales para garantizar la protección del consumidor en los servicios financieros. En Estados Unidos la SEC 17a-4¹⁶ y MiFID II¹⁷ en Europa requieren la captura y retención del 100% de todas las interacciones digitales y el acceso inmediato a ellas durante un período de hasta siete años.

Por lo tanto, los proveedores de servicios digitales que proporcionan asesoramiento financiero digital deben:

- Contar con sistemas de mantenimiento robustos sobre los algoritmos de asesoría y los registros que se generan. Idealmente, los sistemas que se implementen deberán controlar, monitorear, revisar y registrar de manera efectiva los cambios realizados en los algoritmos. En el mismo sentido, los proveedores de asesoramiento digital deben poder justificar las razones para actualizar el algoritmo que respalda el asesoramiento dado al consumidor y estar en capacidad de generar informes automatizados que se pueden descargar y proporcionarlos al supervisor cuando lo requiera.
- Se espera que cualquier empresa Fintech describa cómo lleva a cabo el registro de operaciones con sus clientes, el procesamiento de transacciones y los controles internos que permitirán a la empresa proteger los datos del consumidor y garantizar la eficiencia del procesamiento. En consecuencia, la

¹⁶ https://www.finra.org/sites/default/files/SEA.Rule_17a-4.Interpretations_0_0.pdf

¹⁷ http://www.cnmv.es/porta/MiFIDII_MiFIR/MapaMiFID.aspx

empresa debe abordar en su plan de negocios: i) programa de tecnología de la información; ii) programa de gestión de cumplimiento; iii) plan para proporcionar pruebas independientes de sistemas y controles y iv) sistema de gestión de riesgos de terceras partes.

DEBERES Y DERECHOS DEL CONSUMIDOR FINTECH

En general, los clientes y usuarios de servicios financieros (Fintech o tradicionales) están amparados con derechos y deberes propios de la regulación de protección al consumidor financiero. Sin embargo, existen derechos y deberes propios del entorno digital que acentúan la confianza de los consumidores en el funcionamiento efectivo de los productos y servicios financieros digitales.

Derechos

- Recibir publicidad e información que sea objetiva, oportuna, completa, imparcial, clara y verificable sobre las características de los productos y servicios recibidos.
- Recibir información que permita y facilite su comparación y comprensión frente a los diferentes productos y servicios ofrecidos.
- Recibir productos y servicios con estándares de seguridad y calidad, de acuerdo con las condiciones ofrecidas.
- Conocer previamente las tarifas (costos) de los productos y servicios ofrecidos.
- Presentar de manera respetuosa consultas, peticiones, solicitudes, quejas o reclamaciones ante la empresa y las autoridades de supervisión.
- Tratándose de clientes inversionistas, que se ejecuten las órdenes en conformidad con las instrucciones entregadas.

- Tratándose de un cliente inversionista, recibir recomendaciones individualizadas con elementos relevantes del tipo de operación que le permitan tomar decisiones con los elementos informados por profesionales debidamente certificados.

Deberes

- Suministrar de manera íntegra y veraz a la empresa la información necesaria para su vinculación, así como la requerida para impartir órdenes de inversiones.
- Atender las entrevistas y/o visitas que se requieran dentro de la política de conocimiento del cliente.
- Suministrar la información necesaria para la prevención y el control de lavado de activos y financiación del terrorismo, antes de suscribir cualquier relación contractual.
- Suscribir los contratos para la prestación de servicios, previa lectura y comprensión de los mismos.
- Manejar de forma meticulosa las herramientas y canales de acceso (seguros) dispuestos por el proveedor.
- Autorizar la inclusión de los datos y reporte del compartimiento crediticio y bursátil a centrales de información o base de datos.
- Pagar oportunamente las cuotas o comisiones que resulten por los servicios prestados, de acuerdo con las tarifas establecidas.
- Constituir las garantías a las que esté obligado en conformidad con las leyes aplicables al producto o servicio.
- Tratándose de un cliente inversionista (no experto), suministrar la información que requiera para establecer su perfil de riesgo.
- Tratándose de un cliente inversionista, dar las órdenes de las operaciones que pretenda realizar por los medios establecidos por la empresa, de manera clara, ordenada y precisa.

CONSIDERACIONES ESPECÍFICAS PARA PRODUCTOS FINTECH DE MAYOR RELEVANCIA EN LAS AMÉRICAS

Con el fin de profundizar en la comprensión de las prácticas de comercialización, de divulgación de información y protección del consumidor de los productos Fintech en las distintas jurisdicciones de ASBA, se circuló una encuesta. El objetivo último de este ejercicio era desarrollar una visión de conjunto sobre las principales características y desafíos que los supervisores pueden enfrentar al hacer una revisión del cuerpo normativo y de las prácticas de supervisión actuales, con el fin de identificar la mejor

manera de incorporar las tecnologías innovadoras en el sector financiero de manera responsable, transparente, y competitiva.

A continuación, para cada producto o servicio Fintech identificado como de mayor uso y/o potencial de uso en el sector financiero de las Américas, se determinan los principales focos de atención con respecto a las prácticas de comercialización, divulgación y protección al usuario.

DENOMINACIÓN	DESCRIPCIÓN	SEGMENTO	FOCO DE ATENCIÓN
Préstamos P2P - consumidores-Préstamos P2B-negocios-Seguro P2P	(i) Plataformas donde personas obtienen préstamos en línea con fondos provistos por otras personas o instituciones, incluyendo financieras- Plataformas donde personas e instituciones proveen préstamos en línea a negocios, (ii) Plataforma que conecta inversionistas con demandantes de seguros.	Depósitos y créditos- Seguros	<ul style="list-style-type: none"> Ofrecer claridad del riesgo inversionista. Dar claridad en cuanto a los costos, tasas y comisiones para el deudor. Informar cómo y cuándo se le devolverá el dinero al inversionista.
Préstamos a consumidores basados en data no financiera	Empresas que utilizan información no financiera para la concesión de créditos. Orientado a excluidos. También ofrecen el servicio a instituciones financieras.	Depósitos y créditos	<ul style="list-style-type: none"> Potencial de ser excluido financieramente. Metodología y criterios empleados para la segmentación y concesión de créditos.

DENOMINACIÓN	DESCRIPCIÓN	SEGMENTO	FOCO DE ATENCIÓN
Banca virtual	Entidades financieras de nueva creación (con licencia bancaria propia o utilizando la de un tercero) con múltiples productos financieros y cuya distribución es exclusivamente digital.	Depósitos y créditos	Ofrecer atención humana presencial en especial en los procesos de apertura y cierre de productos. Respaldo patrimonial de larga duración.
Integración operadora de telefonía celular e institución financiera	Incorporación de varios servicios financieros dentro de la oferta de productos de una operadora de telefonía celular mediante la adquisición de una licencia específica.	Depósitos y créditos	<ul style="list-style-type: none"> • Distinguir entre la operación de la telefónica y la operación financiera para el manejo de productos. • Claridad en los costos de los productos. Impedir la apertura no deseada del producto financiero por contar con el servicio de telefonía.
Ahorros automatizados en redes sociales de cuentas del usuario a un intermediario P2P	El usuario autoriza a una aplicación (bot) que reside en el sistema de mensajería de una red social a que revise sus cuentas bancarias (corrientes). La firma que administra el bot instruye a otra firma para que transfiera los excedentes estimados como inversión en un intermediario P2P o a un monedero digital de una institución financiera.	Depósitos y créditos	<ul style="list-style-type: none"> • Dar a conocer la forma para disponer del dinero. Tener claridad de los topes o límites de transferencia, periodicidad, suspensión del servicio y canales de atención.
Supermercado: comparación de productos financieros	Plataformas en línea que contrastan diferentes productos financieros y sus características, sin proveer asesoría. Ingresos por referencias.	Infraestructura y apoyos de mercados	<ul style="list-style-type: none"> • Informar sobre la independencia del prestador del servicio, quiénes son los patrocinadores y conflictos de interés. Informar cómo se cobra el dinero por el servicio.

DENOMINACIÓN	DESCRIPCIÓN	SEGMENTO	FOCO DE ATENCIÓN
Integración red social-pagos-finanzas-comercio	Consolidación de tienda virtual y física, red social, mensajería, instrumento de pago, banca, inversiones y otras operaciones financieras en un solo conglomerado empresarial.	Pagos	<ul style="list-style-type: none"> • Manejo de temas de ciberseguridad. • Protección de datos personales. • Transparencia en costos y tarifas. Claridad del servicio financiero prestado.
API pagos tarjetas de crédito	Plataforma que ofrece a comercios y empresas integrar los pagos con tarjetas de crédito en sus sistemas de forma transparente para el comprador.	Pagos	<ul style="list-style-type: none"> • Manejo de temas de ciberseguridad. Protección de datos personales.
Portal de pagos-intermediario	Soluciones para comercios para la aceptación, autorización y procesamiento de pagos, a través de múltiples canales, diferentes monedas y países y diferentes instituciones financieras. A su vez constituyen un proveedor de servicios esencial para otros productos Fintech.	Pagos	<ul style="list-style-type: none"> • Manejo de temas de ciberseguridad. • Transparencia en los costos y manejo en los recursos de los comercios • Períodos de transferencia de recursos de comercio. Protección de datos personales.
Open Banking	Apertura de APIs (Application Program Interface o interfaz de programación de aplicaciones abierto) a terceros, es decir, conectores que permiten a terceras compañías integrar fácilmente sus desarrollos con los datos financieros del banco. El consumidor tendrá diversas "App Store" de servicios financieros que ofrecerán servicios de seguros, créditos o depósitos tradicionales junto con novedosos pagos entre pares (P2P), intercambio de criptomonedas,	Pagos	<ul style="list-style-type: none"> • Dejar en claro qué empresas son legítimas. • Brindar claridad y control sobre lo que se va a compartir. • Hacer que los consentimientos sean transparentes y rastreables. • Hacer las compensaciones fáciles y consistentes. • Brindar consistencia y claridad en el consentimiento y acceso a los paneles de control. • Permitir a las personas retirar el consentimiento y volver a autenticarse convenientemente.

DENOMINACIÓN	DESCRIPCIÓN	SEGMENTO	FOCO DE ATENCIÓN
	intercambio de divisas internacionales, financiación de masas y envíos transfronterizos		<ul style="list-style-type: none"> Hacer la protección de los pagos seguros Dar a las personas visibilidad de sus saldos antes de que realicen un pago. Establecer el deber de cuidado de las empresas a sus clientes.
Operaciones de cambio extranjero P2P/B2B	Soluciones de compra y/o venta de divisas extranjeras para personas y empresas, con fijación bilateral de tipos de cambio.	Pagos	<ul style="list-style-type: none"> Realizar el proceso de conocimiento del cliente. Realizar los reportes a la autoridad de LAFT. Ofrecer claridad en costos, comisiones y tasas de cambio.
Distribución de productos financieros sofisticados directamente a usuarios minoristas	Uso de canales digitales tales como redes sociales, juegos en línea y similares para ofrecer productos financieros sofisticados tales como derivados con apalancamiento (contratos por diferencias y similares) a personas sin conocimiento financiero, emulando apuestas o juegos.	Gestión de inversiones	<ul style="list-style-type: none"> Revelación del riesgo de la inversión en productos sofisticados. Ofrecer contacto humano y especializado ante solicitudes y reclamaciones por parte de los inversionistas.
Asesores automatizados (pensiones o inversiones)	Soluciones automatizadas para la gestión patrimonial mediante análisis del perfil del cliente. Conecta con casas de corretaje para el manejo de los activos.	Gestión de inversiones	<ul style="list-style-type: none"> Explicar cómo asesora el algoritmo. Claridad en el perfilamiento de los clientes. Revelación del riesgo de la inversión.
Contratos inteligentes	Protocolo tecnológico que facilita, asegura, refuerza y ejecuta contratos/acuerdos. Aún en su infancia, existen varios proyectos en marcha en instituciones financieras globales.	Infraestructura y apoyo de mercados	<ul style="list-style-type: none"> Dar a conocer que el producto es automatizado. Explicar de manera previa qué ejecuta el contrato y bajo cuáles supuestos.

DENOMINACIÓN	DESCRIPCIÓN	SEGMENTO	FOCO DE ATENCIÓN
Uso de datos de redes sociales para propósitos financieros	Recolección y análisis de datos obtenidos de las redes sociales para ser utilizados por instituciones financieras en la evaluación de clientes.	Infraestructura y apoyo de mercados	<ul style="list-style-type: none"> • Potencial de provocar exclusión financieramente. • Claridad en la autorización otorgada para acceder a datos personales y financieros y realizar perfilamiento. • Manejo de temas de ciberseguridad. Protección de datos personales.
Análisis de datos de comportamiento de clientes	Plataforma que provee a las instituciones financieras con información actualizada sobre el comportamiento de clientes en diversos ambientes: redes sociales, telefonía móvil, otros.	Infraestructura y apoyo de mercados	Revelación de la fuente de información. Autorización expresa por parte de los clientes.
Interacción automatizada con usuarios financieros	Sistema de reconocimiento y síntesis de voz, combinado con inteligencia artificial para servir de primera instancia para atender a clientes que llaman pidiendo asistencia o que desean realizar operaciones.	Infraestructura y apoyo de mercados	<ul style="list-style-type: none"> • Cumplimiento de norma de protección de datos al usarse información biométrica. Presencia de mecanismo de atención de segunda instancia (humano) en caso de que falle el proceso de atención primario.
Micro financiación colectiva	Plataformas que permiten micro inversiones en empresas nuevas o pequeñas que requieren montos moderados de capital. El inversionista pasa a ser accionista de la empresa. Incluye las distintas modalidades de micro financiación colectiva, que incluyen o pueden incluir elementos financieros para ser analizados como pueden ser: (i) Bienes Raíces, y (ii) Capital.	Recaudación de capitales	<ul style="list-style-type: none"> • Dar información del riesgo que se asume. • Información clara del activo, rentabilidad, acceso a los recursos y disponibilidad de los mismos. Transparencia en el manejo de los recursos.

DENOMINACIÓN	DESCRIPCIÓN	SEGMENTO	FOCO DE ATENCIÓN
Seguros paramétricos basados en cadena de bloques	Contratos de seguros documentados en cadena de bloques y con pagos de siniestro ejecutado por un contrato inteligente atado a información obtenida independientemente.	Gestión de inversiones	<ul style="list-style-type: none"> • Claridad en la ejecución del contrato Dar información del riesgo que se asume.
Productos y servicios que involucran criptoactivos	Integración de pagos con criptoactivos - Plataforma de negociación de divisas interbancaria basada en criptoactivos - Operaciones de cambio extranjero usando criptoactivos - Monedero electrónico de criptoactivos - Monedero electrónico de dinero de curso legal y criptoactivos- Plataformas de negociación en línea de criptoactivos - Fondos en criptoactivos - Registro de propiedad a través de criptoactivos	Varios	<ul style="list-style-type: none"> • Revelación de riesgos al inversionista. • Limitación de su uso como activo de curso legal. • Riesgo de lavado de activos y financiación del terrorismo. • Riesgo de que el criptoactivo presente en un monedero digital o físico sea "hackeado". Manejo de temas de ciberseguridad.

ALTERNATIVAS PARA UN MODELO DE SUPERVISIÓN DE CONDUCTA Y PROTECCIÓN AL CONSUMIDOR EN EL NUEVO ENTORNO TECNOLÓGICO

Los productos y servicios financieros pueden ser complejos en el entorno Fintech y las decisiones financieras implican incertidumbre, además, requieren que los consumidores hagan una evaluación de riesgo para la que no tienen experiencia. Las consecuencias de sus decisiones pueden ser significativas. Por lo tanto, los consumidores necesitan asistencia y protección, y deben confiar en los proveedores de servicios financieros tecnológicos cuando toman estas decisiones.

Aunque en principio los proveedores diseñan y comercializan los productos y servicios en el mejor de los intereses de sus clientes, pueden existir situaciones que incentiven una conducta inadecuada de los proveedores hacia los usuarios, incluso involuntariamente. Esto tiene un impacto tanto en la reputación del sector financiero como en la estabilidad. Por lo tanto, una supervisión adecuada del riesgo de conducta y un esquema sólido de protección al consumidor son necesarios para evitar estos riesgos.

Las prácticas de supervisión se pueden enmarcar en dos alternativas. La primera, adoptar un modelo de supervisión basado en riesgo para la protección del consumidor financiero; o la segunda, la implementación de un programa de "Responsabilidad demostrada" (*accountability* en inglés) para la protección del consumidor financiero.

MODELO DE SUPERVISIÓN BASADO EN RIESGO

La primera alternativa parte de la definición del riesgo conductual como aquel en el cual el comportamiento

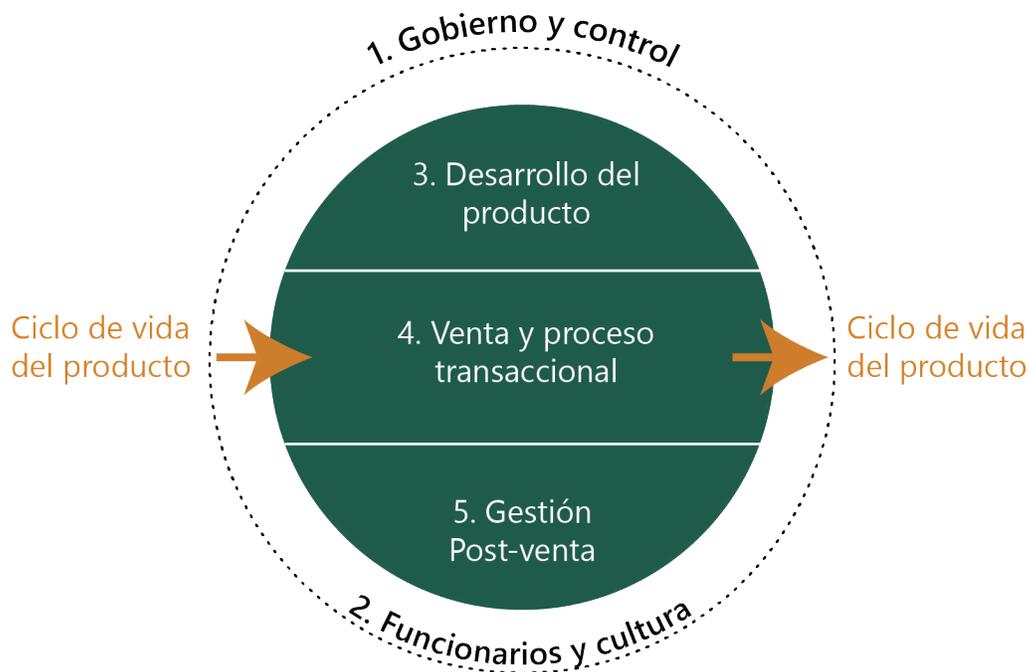
de una entidad de servicios financieros pueda ocasionar impactos indeseados para los consumidores. Los supervisores que han evaluado este riesgo lo han hecho a través del examen de la naturaleza, el alcance de los productos de la entidad y de cómo ésta gestiona los riesgos que sus productos y otros compromisos afectan a sus consumidores.

Las principales autoridades conductuales de Europa, Oceanía, y algunas de las Américas han ampliado su alcance para evaluar el riesgo de conducta, al reconocer que los riesgos para los consumidores pueden provenir de la estrategia, el modelo de negocio, la gobernanza, la cultura empresarial y los colaboradores de la empresa, así como otras estructuras internas de la entidad previstas en la construcción del producto a través de su ciclo de vida.

El modelo de supervisión del riesgo de protección al consumidor puede aplicar para los proveedores de productos y servicios Fintech e incumbentes que se encuentran dentro del perímetro de supervisión bajo cualquier esquema de licenciamiento, ya sea tradicional, licenciamiento con requerimientos mínimos prudenciales (o limitado), o *sandbox regulatorio*. La figura 2 ilustra este modelo con sus elementos.

El modelo de supervisión tiene como características que es intrusivo por naturaleza. Éste evalúa el diseño de un protocolo de control y luego busca evidencia concreta de cuán efectivo es el control; revisa las políticas y procedimientos utilizados en la construcción del producto o servicio; observa las decisiones de la junta directiva y las

Figura 2. Modelo de supervisión basado en riesgo



reuniones del comité clave en el diseño e implementación del producto; realiza un *walk-through* a los sistemas y procesos realizando pruebas sustantivas sobre la consistencia de la aplicación de los controles y; entrevista una selección de personal de diferentes niveles: junta, cumplimiento, funciones de riesgo, recursos humanos, desarrollo de productos, marketing y personal de ventas.

i) Gobierno y Control

Las decisiones que producen afectaciones a los clientes se producen en todos los niveles de la empresa. Sin embargo, en la evaluación de las estructuras de decisión de la empresa se busca determinar hasta qué punto una empresa ha implementado un gobierno y control efectivo y las medidas que permitan la identificación, medición, gestión y mitigación efectiva del riesgo de una inadecuada protección al consumidor.

Entre los temas que se deben evaluar están:

- Que el proveedor de productos y servicios Fintech considere el riesgo de una inadecuada protección del consumidor al desarrollar su estrategia o apetito de riesgo;

- Que las funciones de negocios y de control lleven a cabo la identificación, medición, monitoreo y gestión de riesgos;
- Que los responsables para la identificación, evaluación, mitigación y monitoreo del riesgo estén claramente definidos.

ii) Funcionarios y Cultura

El supervisor debe evaluar si el personal del proveedor de productos y servicios Fintech cuenta con una cultura efectiva enfocada en el consumidor. Para ello se revisa si:

- La junta directiva y la gerencia de la empresa establecen e inculcan una cultura "centrada en el cliente" a través de su compromiso con el trato justo al consumidor;
- La empresa diseña y prueba los servicios y productos, específicamente teniendo en cuenta los intereses de los consumidores;
- La empresa se comunica claramente con los consumidores y les ayuda a tomar decisiones informadas;
- El proveedor de productos y servicios se involucra de manera constructiva con los consumidores cuando

- tienen solicitudes y trata las quejas, reclamaciones y apelaciones de manera justa; y
- Se incentiva a los funcionarios a vender productos adecuados y de forma transparente a los consumidores para los que fueron diseñados.

iii) Desarrollo del producto.

Se revisa entre otros aspectos:

- El grado en que la firma en la etapa de diseño revisa todos los servicios y productos para que cumplan razonablemente las necesidades y expectativas de los clientes; y
- Evalúa si las áreas de marketing y distribución crean adecuadas salvaguardias para proteger a sus clientes.

iv) Etapa de venta y proceso transaccional.

Se pone atención en:

- El grado en que una empresa asegura que un consumidor entiende los productos que se le ofrecen y que satisfacen sus necesidades;
- Si se venden los productos de la manera correcta a las personas adecuadas;
- Si los incentivos de comisiones son ajustados a la venta transparente de los productos;
- Si los canales digitales de distribución son seguros y claros para los consumidores; y
- Si los contratos de los proveedores de productos y servicios Fintech o incumbentes con terceras partes cumplen con las normativas de protección de datos personales y financieros. En caso de que no fuera así, se requerirían modificaciones a estos contratos.

v) Etapa de gestión postventa.

Se valora:

- El grado en que la empresa diseña y revisa los procesos de postventa para cumplir con las necesidades y expectativas de los clientes;
- Los procesos diseñados para la atención de quejas y reclamos, y el número de casos resueltos a favor de la empresa y del cliente; y

- Si los sistemas y controles favorecen una atención expedita al consumidor y no crean barreras poco razonables en la postventa.

MODELO DE RESPONSABILIDAD DEMOSTRADA

La segunda alternativa de supervisión propone implementar un programa de “Responsabilidad demostrada” **siempre y cuando la regulación permita al supervisor ejercer su mandato mediante un modelo de supervisión no intrusivo**. Esta alternativa resulta viable en escenarios de múltiples proveedores que se encuentran por fuera del perímetro y desarrollan actividades que no están sometidas al régimen de supervisión financiera sino a otras autoridades de vigilancia y control; o en situaciones en las que se cuenta con **numerosos sujetos obligados** por una regulación y los **recursos de supervisión son limitados**.

Según una combinación de diversas fuentes, se puede definir el concepto de “responsabilidad” como la obligación o voluntad de un individuo o de una organización de rendir cuentas de sus actividades, aceptar responsabilidad por ellas, y hacer visibles los resultados de manera transparente.

La “Responsabilidad demostrada”, en este sentido, sólo abarcaría los productos y servicios Fintech que quedan fuera del perímetro de supervisión, pero que por sus características están desarrollando actividades que las autoridades consideran cercanas a las tradicionales. En escenarios en donde continuamente aparece un gran número de prestadores de servicios, el uso del “Registro electrónico central público” (descrito en la sección “Consideraciones y recomendaciones generales”, p. 19) sería de gran ayuda para determinar quiénes están realizando dichas actividades, y así poder monitorear la pertinencia de revisar las reglas del perímetro.

El modelo de responsabilidad demostrada contiene tres elementos: responsabilidad, control y evidencia. Cada uno de estos elementos es necesario para poder alcanzar un

estándar de responsabilidad demostrada. En consecuencia, fallar en uno de ellos resultaría en la imposibilidad de que la organización pueda alcanzar dicho estándar y demostrarlo.

El primer elemento es la **responsabilidad voluntaria**, que se alcanza mediante la implementación de un programa efectivo de gestión del riesgo de conducta y protección al consumidor financiero por parte de una empresa Fintech. Esto involucra las políticas, procedimientos, actividades y otras iniciativas ejecutadas de manera permanente en la empresa, elementos que impactan la gestión del riesgo o que se relacionan con el cumplimiento de las normas sobre protección al consumidor financiero.

La evaluación del programa de responsabilidad voluntaria implica las siguientes etapas de gestión del riesgo:

En la **etapa 1** se determina hasta qué punto una entidad ha implementado medidas efectivas de control y gobernanza que permitan la identificación, medición, control y monitoreo efectivo del riesgo de protección del consumidor.

La **etapa 2** evalúa si la entidad cuenta con una cultura efectiva enfocada al consumidor en donde hay apropiación y compromiso con la protección del consumidor desde la alta dirección y a través de toda las áreas; si las entidades diseñan y prueban los productos teniendo en cuenta los intereses de los consumidores; si se comunican claramente con los consumidores y les ayudan a tomar decisiones informadas: si se involucran de manera constructiva con los consumidores que tienen consultas o quejas y tratan las reclamaciones de manera justa, y si incentivan a sus funcionarios a vender productos adecuados a los consumidores para los que fueron diseñados, los errores se corrigen de manera justa y conveniente.

Por su parte la **etapa 3** evalúa el grado en que el proveedor diseña y revisa todos los productos de consumo para cumplir las necesidades y expectativas razonables de los clientes. Por ejemplo, si los acuerdos de mercadeo, publicidad y distribución son adecuados y se han tomado salvaguardias para proteger a los consumidores.

En la **etapa 4** se valora el grado en que la empresa asegura que el consumidor entiende los productos que se le ofrecen y que sus necesidades están satisfechas. Por ejemplo, si se hace la venta de los productos de manera transparente a las personas adecuadas.

En la **etapa 5** se evalúa hasta qué punto la empresa diseña y revisa los procesos de postventa para satisfacer las necesidades y expectativas de los clientes. Por ejemplo, si los sistemas y controles para la atención de quejas y reclamos solucionan los problemas de raíz.

El segundo elemento de la responsabilidad demostrada es el **control efectivo** y es un derivado del elemento de la responsabilidad. Aunque, en una entidad exista un área de atención al cliente, el área en sí misma no es la encargada de gestionar los temas de riesgo de protección al consumidor. Como tal, la efectividad del programa de gestión del riesgo de protección al consumidor recae en el área de gestión de riesgos, que evalúa todos los controles a lo largo de todo el ciclo de vida del producto, desde el desarrollo del producto hasta el proceso de postventa.

El control de algunas actividades de protección al consumidor estará asignado a las unidades operativas de la entidad, por ejemplo: el área de marketing, desarrollo de producto, tecnología de la información, servicio al cliente, entre otras.

El tercer elemento de la responsabilidad demostrada es la **evidencia**. En las entidades responsables, quien asume el control de una actividad de gestión del riesgo de protección al consumidor provee la evidencia de que esa actividad efectivamente se está implementando. Cuando las actividades de gestión del riesgo de protección al consumidor se están llevando a cabo de manera constante, la evidencia se genera como un subproducto de la actividad. En otras palabras, el contar con un programa de gestión de riesgos y cumplimiento de conducta será evidente para el supervisor, aun si necesidad de llevar a cabo una supervisión intrusiva.

La evidencia puede ser documentación formal (políticas, procedimientos o manuales) o incluso información administrativa (comunicaciones internas o externas, agendas o registros de los sistemas de información) que pueden ser utilizados para demostrar que una actividad de gestión de riesgo efectivamente se está llevando a cabo.

Las medidas de responsabilidad demostrada se deben adoptar teniendo en cuenta diversos factores que son propios de cada entidad de servicios financieros, entre los que se encuentran su tamaño y naturaleza jurídica, la naturaleza de los productos y servicios específicos, los riesgos que impliquen para los consumidores, y las interconexiones que puedan implicar riesgo sistémico. Cuando el supervisor identifique que alguna entidad comienza a crecer y a llevar a cabo operaciones más complejas, debería tener la facultad de hacerla elegible para introducirla dentro del ciclo de supervisión intrusiva usual.

Finalmente, es importante mencionar que las alternativas propuestas en este documento no son mutuamente excluyentes. Es decir, las ARS pueden optar por aplicar el modelo de supervisión del riesgo de protección al consumidor en aquellas empresas tradicionales y Fintech

con licenciamiento tradicional y “pleno”, quienes entrarían dentro de la programación de supervisión *in-situ* o *extra-situ*. Por otro lado, las empresas o productos relevantes para las autoridades que queden por fuera del perímetro pueden ser atendidas bajo el modelo de “Responsabilidad demostrada.”

Las empresas Fintech bajo el programa de “Responsabilidad demostrada” no entrarían, en un principio, a formar parte del ciclo de supervisión *in-situ* o *extra-situ* del supervisor financiero. No obstante, considerando que las empresas por fuera del perímetro pueden estar bajo las reglas de un supervisor genérico o transversal de protección al consumidor, ante cualquier solicitud de este supervisor genérico, las empresas deberán revelar la implementación del programa. De no hacerlo o encontrarse deficiencias en el programa, el supervisor debe tener la facultad de aplicar las sanciones correspondientes.

A continuación, se destacan algunas consideraciones que, independientemente del enfoque de supervisión que su contexto y marco legal le permita, la autoridad debe tomar para efectos de alcanzar un adecuado esquema de supervisión en materia de Fintech.

CONSIDERACIONES PARA LA IMPLEMENTACIÓN DE ESTRATEGIAS DE SUPERVISIÓN

Como podrá apreciarse algunas de estas consideraciones ya forman parte de marcos normativos, estrategias y metodologías de algunos supervisores de la región. Se resalta que las consideraciones que se desarrollan surgen tanto de lo manifestado por las autoridades en las encuestas realizadas por la Asociación, como de la experiencia del Consultor y la asesoría del GDT.

ASEGURAR UNA MÍNIMA PROTECCIÓN AL CONSUMIDOR MEDIANTE LA ADAPTACIÓN Y CREACIÓN DE HERRAMIENTAS Y TÉCNICAS PARA ABORDAR LOS RIESGOS DERIVADOS DE LA COMERCIALIZACIÓN DE PRODUCTOS Y SERVICIOS FINTECH

Las ARS se encuentran en diferentes etapas para adaptarse a los desafíos que implica la digitalización de la actividad de supervisión, pero antes de esta adaptación necesitan entender el fenómeno digital para diseñar herramientas de supervisión adecuadas.

En consecuencia, la respuesta inicial por parte de las ARS debe ser la creación de grupos de trabajo multidisciplinarios internos para comprender las particularidades de las Fintech y adaptar las herramientas de supervisión según sea necesario, y luego producir nuevas herramientas y metodologías dedicadas a su supervisión donde sea necesario.

- La creación de grupos de trabajo multidisciplinarios internos (miembros de los equipos de supervisión por actividad, legal, TI, lavado de dinero, riesgos, protección al consumidor) puede ser útil

para obtener una mejor comprensión de las Fintech y determinar las estrategias y herramientas de supervisión que se deben aplicar a ellas. Estos grupos deben analizar los modelos de negocios utilizados por las Fintech, los riesgos asociados a las funciones de protección al consumidor, y luego deberán diseñar las respuestas regulatorias y de supervisión a tales riesgos.

- Los supervisores y reguladores deberán utilizar las herramientas tradicionales de supervisión y adaptarlas para abordar a los proveedores de servicios Fintech, especialmente en aquellos casos en que la legislación no prevé la posibilidad de aplicar diferentes herramientas o tiene restricciones de recursos para llevarlas a cabo. Entre estas herramientas se encuentran:
 - **Evaluaciones *extra situ***: revisiones específicas de archivos de información, publicidad, información precontractual y contractual; celebración de reuniones periódicas con establecimientos financieros; cuestionarios y solicitudes de información; utilización de evaluaciones temáticas sobre las funciones o las áreas a cargo de la atención al consumidor para evaluar el cumplimiento de los requisitos legales.
 - **Indicadores de alerta temprana e indicadores de riesgo**: construcción de indicadores de advertencia que permitan anticipar los nuevos riesgos provenientes de Fintech como lo harían con los productos y servicios financieros tradicionales. Entre las principales herramientas de alerta temprana utilizadas por las ARS para

anticipar los nuevos riesgos relacionados con Fintech se encuentran: monitoreo de redes sociales, entrevistas con representantes de los consumidores, investigaciones sobre la industria, cuestionarios y noticias de prensa.

Para diseñar herramientas regulares y confiables de alerta temprana, dos fuentes de información son importantes siempre que sean recibidas a través de canales formales: manejo de quejas y línea de informantes (*whistleblowers*).

Asimismo, se recomienda el desarrollo de indicadores de riesgo a partir de talleres internos de evaluación de riesgos, equipos internos y herramientas de autoevaluación de información reportada, información de inspecciones in situ y evaluaciones de riesgo operacional.

El ingreso a los sitios o aplicaciones de oferta y la eventual prueba de los productos Fintech permite que supervisores conozcan de primera mano las particularidades funcionales del producto y los estándares de atención.

- **Supervisión de quejas:** Las quejas son un indicador relevante de los riesgos asociados con un producto o servicio y su supervisión todavía está orientada hacia los productos tradicionales. Las quejas se clasifican por tipo de producto, objeto de la queja, proveedor de servicios financieros, etc. Por lo cual, se requiere modernizar el proceso de supervisión para apoyar la identificación de problemas emergentes relacionados con los productos digitales.

Con esto en mente, se propone definir claramente el concepto de queja para adaptarlo a los productos y servicios digitales, de tal manera que una solicitud o petición elaborada por un cliente ante su entidad financiera, que no sea resuelta en 24 horas a partir de su entrada en el sistema de la entidad, deberá clasificarse como queja y aplicarán las disposiciones legales previstas en cada jurisdicción para su atención y resolución.

Por otro lado, es necesario que las ARS construyan la “base de atención de quejas” del sistema financiero. Esta base centralizada es una

aplicación (App) que organiza los productos, subproductos, problemas y subproblemas de acuerdo con la regulación de cada jurisdicción. Cada cliente ingresará su queja en el sistema y la autoridad correspondiente la enviará a cada entidad para que responda y se siga el proceso regulatorio previsto para su atención, incluyendo la participación del defensor del cliente (Ombudsman), de existir esta figura en cada jurisdicción.

La autoridad no verificaría los hechos alegados en estas quejas, pero puede utilizar la información para confirmar y registrar una relación comercial entre el consumidor y la entidad. De esta manera la autoridad de supervisión monitorea en tiempo real la fuente de la queja, la fecha de presentación, la entidad a la que se envió la queja para su respuesta y las acciones tomadas por la entidad en respuesta a la queja. Por ejemplo, si la respuesta de la entidad fue oportuna y qué acciones tomó al respecto, o si el consumidor no aceptó la respuesta y optó por escalarlo al defensor.

Con esta herramienta, las ARS cuentan con estadísticas de quejas como fuente importante de información para análisis de datos que permiten identificar tendencias y problemas en el mercado. Así, es posible realizar una efectiva supervisión extra situ basada en riesgos sobre las entidades, hacer cumplir las leyes de protección al consumidor financiero y redactar normas y reglamentos, además de publicar informes sobre quejas y compartir la información con otras autoridades y centros de estudios. Un ejemplo de esta herramienta se encuentra en *The Consumer Financial Protection Bureau*¹⁸.

- Las **iniciativas de coordinación con otras autoridades** que supervisan empresas y servicios que se encuentran por fuera del perímetro, pero que resultan relevantes para la autoridad financiera son fundamentales. Un aspecto clave

¹⁸ <https://www.consumerfinance.gov/data-research/consumer-complaints/>

de dichas actividades es la evaluación conjunta de peticiones, quejas y reclamos asociados a productos digitales similares a los prestados por instituciones financieras. El análisis de tendencias, tecnologías, innovaciones y la dinámica de competencia en el mercado financiero que plantean estos nuevos oferentes permite ser prospectivo en iniciativas de protección al consumidor.

- Es pertinente que las ARS **evalúen la funcionalidad y eficiencia de sus marcos normativos de atención de peticiones y quejas** frente al nuevo entorno de productos y servicios Fintech. En las actividades de revisión normativa es prioritario evaluar los principios, procedimientos y el rol de la autoridad frente a escenarios en los cuales mayores niveles de inclusión pueden hacer creciente el número de quejas.

Un criterio orientador de dichas revisiones normativas debe ser exigir a los incumbentes y nuevos proveedores Fintech un análisis prospectivo de la protección al consumidor y la adopción temprana de medidas. Por su parte, el supervisor que tenga competencias en la materia debe racionalizar su rol buscando más eficiencia en sus procesos, concentrando sus actividades en la supervisión preventiva y en el seguimiento a la atención eficaz que den los prestadores a las quejas de los consumidores.

- **Reportes de información específica:** son una herramienta importante que pueden proporcionar una visión general de los productos y servicios digitales que se están lanzando en el mercado y sobre sus respectivas características. Deben incluir la notificación de incidentes de seguridad en la información teniendo en cuenta la normativa de datos personales.

También será necesario adaptar el alcance de los reportes para recolectar datos que informen acerca de la conducta de la entidad hacia los consumidores, como nuevos productos ofre-

cidos en el período, los productos retirados en el período, los cambios en los términos y condiciones de los productos en el período y el desarrollo de productos minoristas.

- **Inspecciones *in-situ*:** se requerirá hacer revisiones que permitan el acceso a las plataformas tecnológicas de los proveedores de servicios Fintech en relación con los sistemas de TI, la ciberseguridad, la gobernanza y las capacidades de las empresas, incluidos los controles de seguridad de la información, computación en la nube y robo-asesores. Asimismo, se tendrán que diseñar planes específicos de evaluación de la relación de las Fintech con terceros proveedores financieros.

Los supervisores deben obtener de las instituciones supervisadas la cooperación para simular, en un entorno real, la relación entre el proveedor y el cliente, de acuerdo con las normas de cada jurisdicción, desempeñando el papel de “comprador virtual” que tiene permitido operar las aplicaciones y verificar aspectos como: si la información general y precontractual cumple con las reglas, los aspectos prácticos y operativos de la interfaz digital; si la forma de aceptar los términos y condiciones es técnicamente adecuada; si la app cumple con los requisitos legales para monitorear los cambios introducidos a lo largo del tiempo, así como probar varios escenarios, perfiles y casos de uso, de acuerdo con situaciones reales identificadas en quejas presentadas por los clientes.

- La **divulgación de datos sobre quejas, sus causas y la forma** como evolucionan puede ser un incentivo para la mejora constante. Esto podría contribuir a que la satisfacción del consumidor fuera un factor relevante en la competencia entre actores en el mercado, lo cual es deseable, pero no siempre posible debido a las rígidas reglas de secreto bancario establecidas en diversas jurisdicciones.

- En cuanto a la creación de nuevas herramientas dedicadas a la supervisión Fintech los supervisores deben contar con recursos financieros y técnicos para desarrollar herramientas intensivas en tecnología que faciliten su trabajo. Entre estas se encuentran:

- **Tecnología Supervisora** (Suptech): el desarrollo tecnológico puede mejorar la supervisión mediante la incorporación de tecnologías de vanguardia en los procedimientos de los supervisores tales como machine learning para detectar problemas de calidad en la información transmitida, como brechas de datos, inconsistencias y errores, y automatizar la limpieza, consolidación, validación y control de calidad de los datos.

Otro enfoque es el desarrollo de las APIs para que las entidades supervisadas informen con datos granulares de alta calidad y así aumentar la comparabilidad entre las entidades, crear nuevas vías de análisis y reducir la carga de validar los datos a nivel agregado. El uso de Tecnologías de Registro Distribuido (DLT, por sus siglas en inglés) también está siendo usado por los supervisores de valores para reducir la complejidad y los costos de los informes voluminosos. Esto podría proporcionar un alto nivel de seguridad e integridad de los datos mientras se mantienen los costos de agregación y la transferencia de datos se vuelve más manejable. El uso combinado de tecnologías como ML, aprendizaje profundo (*deep learning*), reconocimiento óptico de caracteres (OCR, por sus siglas en inglés), *natural language processing* (NLP) y análisis de *big data*, permite a los supervisores integrar el análisis de múltiples fuentes y formatos de datos, lo cual era imposible con el software tradicional.

- **Tecnología Regulatoria** (Regtech): son soluciones innovadoras implementadas por proveedores de servicios financieros para cumplir con los requisitos regulatorios y mejorar la gestión

automática de riesgos de manera más eficaz y eficiente. Se han identificado tres tipos generales de soluciones Regtech: (1) las que ayudan a las entidades supervisadas a cumplir con sus obligaciones reglamentarias, (2) las que ayudan a las autoridades a mejorar sus funciones de supervisión y monitoreo del mercado, y (3) las que ayudan a reformular los procesos y sistemas regulatorios actuales. Es recomendable, pues, que los grupos de trabajo multidisciplinarios internos para Fintech se relacionen con la comunidad Regtech, con la finalidad de entender mejor sus modelos de negocio y desarrollos, así como realizar pruebas de tecnología en los campos de análisis cognitivo para analizar páginas web, aplicaciones de aprendizaje automático que evalúan conjuntos de documentos y monitoreo de redes sociales.

AUMENTAR LOS RECURSOS PARA LAS INSPECCIONES ESPECIALIZADAS DE TI Y MANTENERLOS ACTUALIZADOS ANTE LOS CAMBIOS DEL SECTOR

A medida que la transformación digital continúa en la industria, los riesgos de la tecnología de la información aumentan, tanto en términos de probabilidad como de impacto. La industria financiera tiene datos personales particularmente sensibles y hay un historial de ataques cibernéticos bien documentados. Las autoridades de regulación continúan construyendo y mejorando sus enfoques normativos de TI y de ciberseguridad.

Aunque las autoridades de supervisión apoyan en las áreas de auditoría interna y externa, es necesario contar con un equipo dedicado a la inspección de riesgos de TI que sea intrusivo para la valoración de las inversiones en TI, gobernanza y controles especializados para mitigar satisfactoriamente estos riesgos. Este enfoque permitirá enfrentar los desafíos de la tecnología y el cambio de los modelos de negocios asociados con Fintech.

DISPONER DE UNIDADES DEDICADAS AL ANÁLISIS DE ECONOMÍA DEL COMPORTAMIENTO EN LA PROTECCIÓN DEL CONSUMIDOR FINANCIERO

Los entornos digitales son relativamente nuevos y se han hecho muy dinámicos con el advenimiento de nuevas tecnologías (telecomunicaciones 5G, *blockchain*, procesos en la nube, etc), pero el comportamiento humano en tales entornos tiene aspectos particulares que requieren un análisis detallado. La aplicación del análisis conductual a la supervisión de las Fintech tiene un enorme potencial para diseñar políticas y probar su efectividad en la práctica mediante la realización de ensayos controlados aleatorios, ya que el comportamiento del consumidor puede ser diferente al obtener productos financieros a través de canales digitales en lugar de los canales tradicionales. Esta recomendación aplica tanto para las autoridades de supervisión como para los proveedores de servicios.

Un ejemplo de esta práctica, por el lado público, es la llevada a cabo por la *Australian Securities and Investments Commission* (ASIC) que estableció un equipo dedicado a la investigación de economía del comportamiento, es decir, una investigación acerca del consumidor y las políticas de consumo. Las publicaciones de ASIC han dado el soporte para poder implementar detalles regulatorios importantes que benefician al consumidor en el entorno digital (por ejemplo, tamaño de pantalla, tiempo, orden, canal, presentación, etc.) y pueden influir en la atención y el compromiso que los consumidores muestran en la experiencia como clientes.

CONSIDERAR LA EMISIÓN DE MATERIALES REGULATORIOS COMPLEMENTARIOS COMO GUÍAS, MEJORES PRÁCTICAS, Y PRINCIPIOS DE PROTECCIÓN AL CONSUMIDOR

La emisión de materiales complementarios a la regulación, como directrices, notas de posición o advertencias, puede ser una herramienta de supervisión eficaz para disciplinar segmentos de empresas Fintech e incumbentes. Estas herramientas pueden ser una alternativa válida a

modificaciones del marco regulatorio, las cuales pueden requerir un largo proceso legislativo.

Es recomendable que las directrices estén basadas en principios en lugar de reglas prescriptivas, y que aborden temas específicos en relación con cuestiones digitales, o que modifiquen ciertas directrices existentes relacionadas con productos tradicionales para incluir las características específicas de la provisión de estos productos y servicios por medios digitales.

CONSIDERAR Y DAR SEGUIMIENTO A LA EVOLUCIÓN DE LOS NUEVOS CANALES PARA LA PROVISIÓN DE SERVICIOS FINANCIEROS

Los proveedores de productos y servicios Fintech proporcionan nuevas y mejoradas oportunidades de acceso empleando los canales digitales y la omnicanalidad, pero, a cambio, los consumidores pueden tener menos control en términos de inicio en la interacción con su Fintech.

Esto es debido a que el suministro y la cadena de distribución puede fragmentarse por la participación de múltiples especialistas que son responsables de diferentes partes de esa cadena, lo que conlleva a la retención de la trazabilidad de cualquier información que hayan proporcionado los consumidores.

Se pueden identificar los siguientes requisitos que incumbentes y empresas prestadoras de servicios Fintech deben garantizar en favor de los consumidores:

- Contar con una infraestructura segura de claves y cifrado, que garantice el cifrado estándar múltiple de datos almacenados en las infraestructuras de almacenamiento del proveedor y su cadena de suministro.
- Contar con procesos de seguridad de la información y ciberseguridad.
- Revelar los costos asociados al uso del canal.
- Proveer las instrucciones para el uso del canal y las orientaciones en caso de caída del canal.

- El aumento de la automatización del canal no debe eliminar la posibilidad de un contacto personal para los clientes que adquieran ciertos productos y servicios.
- Poner a disposición el mismo canal por el que se abrió el producto o servicio para el respectivo cierre.
- Cumplir con las normativas de protección de datos personales y privacidad vigentes.
- Garantizar la trazabilidad de todos los datos en las infraestructuras de almacenamiento de los proveedores financieros y su cadena de suministro.

Por su parte, cuando los canales digitales se utilizan para vincular a los clientes, surgen nuevos desafíos en relación con la gestión del riesgo de AML/CFT debido a que tradicionalmente la identidad de los nuevos clientes es verificada por los analistas de manera física y contra los documentos de identidad nacionales.

En este escenario, la regulación en diversas jurisdicciones busca permitir la identificación remota de los clientes, delimitando las condiciones para considerar que dichas identificaciones cumplen con los requisitos de diligencia debida establecidos en las respectivas normativas de AML/CFT. Esto implica:

- Permitir la identificación del cliente por medio de video, lo cual debe ocurrir en tiempo real (en vivo), y debe grabarse con el consentimiento previo del cliente. Dichos registros deben permanecer protegidos.
- Utilizar el documento de identificación nacional presentado por el cliente, que debe ser accesible para una comprobación de "legibilidad por máquina". Es decir, adecuado para la lectura óptica de secciones particulares del documento de identificación y poder descifrar las características de información cifrada que posea.

Además, se deben tomar medidas de identificación separadas en paralelo del documento de identificación como son la verificación de características holográficas, elementos de presión con efectos visuales y verificarse

la información de forma cruzada con una base de datos de documentos de identidad oficial y en línea o bases de datos privadas con contenido equivalente.

Estas propuestas pueden estar limitadas por la ausencia de un marco regulatorio nacional transversal coherente que tenga en cuenta los siguientes aspectos relacionados:

- Desarrollar la identificación electrónica: incorporar en los documentos nacionales de identificación componentes de *hardware* y *software* que almacenen de manera segura información personal y características biométricas con potencial relevante para la incorporación y gestión de nuevos clientes.
- Explorar y evaluar el uso de tecnologías de registro distribuido (*DLT*) para la creación de un registro de identificaciones digitales individuales que incluya datos personales tradicionales, y también registros biométricos, verificados por autoridades gubernamentales, que permitan ampliar el procedimiento de conocimiento del cliente en procesos de LAFT.

CONSIDERAR Y DAR SEGUIMIENTO A LA EVOLUCIÓN DE LA INFRAESTRUCTURA DE SOPORTE QUE PERMITE LA PROVISIÓN DE SERVICIOS FINANCIEROS. EN PARTICULAR, AQUELLA INFRAESTRUCTURA RELACIONADA CON LOS SISTEMAS DE PAGO

Actualmente, el trabajo de mayor recorrido en torno al segmento de los servicios de pago ha sido llevado a cabo por parte de la EBA y está dirigido a garantizar que los pagos en toda la Unión Europea sean seguros, fáciles y eficientes; el resultado regulatorio está condensado en las normas técnicas y las pautas de la Directiva de Servicios de Pago (PSD2)¹⁹.

La Directiva ha institucionalizado la actividad de los denominados proveedores de servicio tercerizados o TPP (*Third Party Providers*), por la cual los titulares de una

¹⁹ https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en

cuenta de pago autorizan expresamente a una entidad tercerizada, siempre que esté debidamente autorizada, para que ésta ordene pagos en su nombre y/o consulte cierta información asociada a dicha cuenta.

De esta manera, se tendrán los proveedores que ofrecen al cliente el servicio de conocer de manera consolidada la situación que presentan las cuentas de pago que éste mantenga con diversas entidades, ayudándole a su planificación financiera; y estarán los proveedores que ofrecerán alternativas al uso de las tarjetas, para el pago de las compras que se efectúen en entornos de comercio electrónico. Con ello, el papel tradicional que ejercía la banca como proveedor de servicios de pago único se abre a los nuevos actores TPP, lo que debilitará el grado de vinculación de los clientes y la estabilidad de los ingresos transaccionales.

El desarrollo de las APIs como medios técnicos que permiten compartir recursos entre diferentes entornos abiertos, para su uso masivo por parte de terceros, favorecen el acceso controlado a los entornos bancarios. La banca al igual que los TPP también podría hacer uso de las APIs para prestar servicios equivalentes a los de estos nuevos competidores, diferenciándose de ellos y ofertando servicios de mayor valor añadido.

En este nuevo escenario las autoridades deben concienciar a los consumidores sobre las consecuencias de sus elecciones ante el mayor abanico de opciones para realizar las transacciones y sobre la operativa financiera para que aumenten las precauciones que les eviten ser víctimas de actuaciones ilícitas y usen las herramientas de control que le ofrezcan las entidades. Por lo tanto:

- Las entidades incumbentes como proveedores de productos y servicios Fintech deben esforzarse en comunicar a los consumidores el alcance real de la autorización que esté otorgando a un TPP e informar, de manera explícita, el posible uso comercial de su información más allá de la prestación de un servicio de pago concreto. Los consumidores deben estar conscientes de que pueden terminar autorizando el acceso a un volumen de información personal que, en realidad, preferirían haber conservado en privado.
- Se debe procurar que los consumidores cuenten con un entorno de máxima seguridad cuando opten por efectuar operaciones de pago electrónicas en general, para lo cual es forzoso adoptar medidas que reduzcan la incidencia del fraude y se asegure la continuidad de los servicios de pago para reforzar la confianza de los consumidores.

COMENTARIOS FINALES Y DESAFÍOS PENDIENTES PARA LAS AUTORIDADES

Las consideraciones y recomendaciones hechas a lo largo de este documento proporcionan un marco de acción para regular y supervisar a los proveedores de productos y servicios Fintech desde un punto de vista de conducta y protección al consumidor. Estas recomendaciones fueron desarrolladas tomando en cuenta la diversidad de sistemas regulatorios en la región y no pretenden delimitar estándares dado el constante cambio en las características del entorno.

Cualquiera que sea la estrategia que decidan adoptar las distintas autoridades financieras, es necesario asegurar el cumplimiento de una serie de labores que son esenciales para consolidar un marco de regulación y supervisión de proveedores Fintech que sea efectivo. Aunque estas labores son evidentes, las jurisdicciones de la región han encontrado dificultades al ejecutarlas, por lo que se exhorta a las autoridades a diseñar estrategias según las características específicas de su jurisdicción. Estas labores abarcan:

Comprender los riesgos de las empresas de productos y/o servicios provenientes de innovaciones tecnológicas.

Como reguladores y supervisores, es importante que se vean las innovaciones con suficiente antelación porque las Fintech están presentes en todas las actividades financieras y del mercado de valores, y no es deseable esperar hasta que ya estén en uso generalizado y hayan escalado en dimensión de uso para evaluarlas o entenderlas.

Por lo cual, una alternativa es desarrollar un centro de innovación al interior del órgano supervisor y/o regulador como vía para que las empresas innovadoras puedan ponerse en contacto con las autoridades, con la intención de resolver sus inquietudes y para que el supervisor aprenda de las empresas sobre sus ideas y las tecnologías que están desarrollando, y, por otro lado, obtenga una visión de hacia dónde se dirigen tanto los servicios financieros como los riesgos emergentes.

Generar estadísticas e identificar el alcance de la actividad de Fintech en sus jurisdicciones y en la región latinoamericana, tanto dentro como fuera del perímetro regulatorio.

Uno de los desafíos que presenta el trabajo con Fintech se relaciona con la falta de información estadística para determinar la importancia y el alcance de los nuevos negocios Fintech y para monitorearlos (número de clientes, productos, canal de distribución, canal de atención al consumidor, área geográfica de operaciones, etc.). Esta escasez de información estandarizada y periódica dificulta el desarrollo de herramientas de supervisión y la evaluación de riesgos potenciales.

Por esta razón, para obtener estadísticas propias y confiables, e identificar el alcance de la actividad de Fintech en cada jurisdicción, se han propuesto estrategias para incrementar el conocimiento que puedan tener las autoridades del ecosistema Fintech, incluyendo, de igual forma, a aquellos proveedores de productos y servicios

de esta naturaleza que no formen parte de su entorno natural de supervisión.

Lo anterior, puede alcanzarse mediante la implementación de un registro electrónico central público controlado por una tercera institución, como un ministerio o el equivalente a una cámara o registrador a cargo de la gestión de registros públicos, lo cual reduce significativamente cualquier posible asociación que puedan hacer los consumidores con una actividad de supervisión. Esto implica para las autoridades de regulación y supervisión la coordinación con esta tercera institución y la posible generación de normativa al respecto.

Revisar la claridad de sus mandatos: la regulación superpuesta y los procesos largos de aprobación de una nueva regulación pueden afectar la protección al consumidor.

Debe tenerse en cuenta que la nueva regulación tiene que ser neutral con respecto al cambio tecnológico. Esto significa que las normas de protección al consumidor se aplican por igual a entornos de entrega tanto digitales como tradicionales, y que aseguran que los consumidores están, y seguirán estando, protegidos de los riesgos que surgen de la digitalización.

Por lo tanto, hay que analizar si las actuales normas de protección al consumidor en cada jurisdicción protegen adecuadamente a los consumidores en un entorno de servicios financieros innovadores e impulsados por la tecnología.

Las autoridades de regulación y supervisión financiera tendrán que consultar la opinión de la industria y de las autoridades de protección al consumidor para determinar si las protecciones existentes necesitan ser mejoradas o adaptadas, e igualmente importante, considerar cambios normativos para asumir funciones de supervisión y protección al consumidor en temas concernientes a las empresas del sector financiero.

La velocidad de la innovación tecnológica contrasta con los largos períodos de tiempo necesarios para reclutar el personal adecuado, comprender las nuevas necesidades técnicas y aprobar nuevos cursos de formación.

Los supervisores deben reclutar personal de forma abierta y transparente, que cuente con altas habilidades analíticas y tecnológicas. Al mismo tiempo, el personal que ya se tiene debe mantenerse actualizado al personal. Igualmente, las autoridades de supervisión deben hacer un mayor uso de las tecnologías para impulsar la eficiencia y la eficacia, dado el aumento de datos provenientes de incumbentes y Fintech. La tecnología (Suptech) es un apoyo para hacer el trabajo de evaluación con eficacia y para conformar equipos de análisis con mejor preparación en analítica y auditoría basada en riesgos.

Desarrollar la regulación y metodología de supervisión con enfoque basado en el riesgo de protección al consumidor y lograr una priorización de trabajo y recursos en aquellas áreas donde se considera que existe una amenaza importante para los objetivos de protección al consumidor. Alternativamente, siempre y cuando la regulación lo permita o pueda ampliarse, adoptar la implementación de un programa de "Responsabilidad demostrada" hacia las empresas Fintech que se encuentren por fuera del perímetro.

El desarrollo del modelo de supervisión permite hacer inspecciones temáticas para evaluar los riesgos prioritarios para los consumidores, por ejemplo, al centrarse en un producto, canal o actividad en particular. Las inspecciones temáticas se centran en varias empresas Fintech o incumbentes dentro de una actividad financiera. Esto permite determinar si los estándares, a nivel de la industria, están cerca del nivel que espera el supervisor o si parece haber un problema en toda la industria que puede requerir cambios en las políticas, intervención específica de supervisión o acción de cumplimiento para asegurar el cambio apropiado.

La falta de mandatos adecuados para hacer cumplir la protección del consumidor, cuando las Fintech con sede en el extranjero suministran productos y servicios a través de las fronteras, deberá contrarrestarse con mayor cooperación entre autoridades de supervisión y llevar a cabo inspecciones temáticas.

A través de las entidades tradicionales y Fintech se deben incorporar proyectos de educación financiera, tanto en sus plataformas de internet como en sus aplicaciones móviles. Al interior de las entidades, es necesario producir cambios de conducta culturales en la comercialización y postcomercialización de productos que protejan al consumidor financiero.

Finalmente, las autoridades financieras deberán continuar vigilando la aparición y desarrollo de nuevos actores y modelos de negocio no tradicionales, buscando evitar arbitrajes normativos y procurando que su actividad se dé bajo estándares de protección al consumidor convergentes con los de la industria tradicional.

En resumen, cualquier esquema de regulación y supervisión de conducta y protección al consumidor de productos y servicios Fintech deberá generar los incentivos correctos para que las entidades cumplan con²⁰:

20 Reino Unido, Financial Conduct Authority, <https://www.fca.org.uk/about>; Irlanda, Central Bank of Ireland, <https://www.centralbank.ie/about>; Australia, Australian Securities and Investments Commission, <https://asic.gov.au/>

- Actuar de manera honesta, justa y profesional en el mejor interés de los clientes y de la integridad del mercado;
- Actuar con la debida diligencia, habilidad y cuidado en el mejor interés de los clientes;
- Evitar inducir de manera imprudente, negligente o deliberada las ventajas o desventajas reales o percibidas de cualquier producto o servicio a un cliente;
- Tener y emplear de manera efectiva los recursos, políticas, procedimientos, controles (sobre riesgos operativos, tecnológicos y de cumplimiento) y capacitación del personal necesarios para cumplir con la regulación dispuesta;
- Obtener de sus clientes información relevante para el producto o servicio solicitado;
- Realizar la divulgación completa de toda la información relevante del producto, incluidas todas las tasas y precios;
- Buscar evitar situaciones que generen conflictos de intereses;
- Corregir los errores y atender las quejas de manera rápida, eficiente y justa;
- Evitar ejercer una presión indebida o influencia indebida en un cliente;
- Asegurar que cualquier actividad subcontratada cumpla con la regulación dispuesta;
- Garantizar que sus políticas, procedimientos o prácticas de comercialización no impidan el acceso a servicios financieros básicos, y
- Fortalecer la protección de la información de los consumidores mediante la gestión de riesgos de ciberseguridad.

TÉRMINOS Y ABREVIATURAS

Acceso a la misma variedad de productos y servicios en todos los canales sin perder su calidad	Omnicanalidad
Application Program Interface	API
Aplicación	App
Aprendizaje automático	Machine Learning
Aprendizaje profundo	<i>Deep learning</i>
Asociación de Supervisores Bancarios de las Américas	ASBA o Asociación
Autoridades de regulación y supervisión	ARS
Australian Securities and Investments Commission	ASIC
Banco Interamericano de Desarrollo	BID
Bureau Européen des Unions de Consommateurs	BEUC
Conocer al cliente	KYC
Defensor del cliente	<i>Ombudsman</i>
Directiva de servicios de pago	PSD2
Educación financiera	EF
Empuje	<i>Push</i>
Entidades financieras tradicionales	Incumbentes

European Banking Authority	EBA
European Insurance and Occupational Pensions Authority	EIOPA
Grupo de trabajo	GDT
Productos financieros tecnológicos	Fintech
Reglamento General de Protección de Datos (europeo)	GDPR
Institución financiera	IF
Lavado de dinero y financiamiento al terrorismo	AML & CFT
Línea de informantes	<i>Whistleblowers</i>
Memorandos de entendimiento	MoU
Mercadeo	Marketing
<i>Natural language processing</i>	NLP
Tecnologías de la información	TI
Pago entre pares	P2P
Reconocimiento óptico de caracteres	OCR
Responsabilidad demostrada	<i>Accountability</i>
Tecnologías de registro distribuido	DLT
Tecnología regulatoria	RegTech
<i>Third party providers</i>	TPP

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

Roberto Borrás

Consultor

ASBA

Marcos Fabián

Antonio Pineda

Ricardo Toranzo

JUNTA DIRECTIVA

PRESIDENTE

Paulo Sérgio Neves de Souza

Banco Central do Brasil

VICEPRESIDENTE

Jorge Alexander Castaño Gutiérrez

Superintendencia Financiera de Colombia

DIRECTORA REGIÓN ANDINA

Ma. del Socorro Heysen Zegarra

Superintendencia de Banca, Seguros y AFP, Perú

DIRECTORA REGIÓN CARIBE

Michelle Francis-Pantor

The Central Bank of Trinidad and Tobago

DIRECTORA REGIÓN CENTROAMÉRICA

Ethel Deras Enamorado

Comisión Nacional de Bancos y Seguros, Honduras

DIRECTOR REGIÓN NORTE AMÉRICA

José Antonio Quesada Palacios

Comisión Nacional Bancaria y de Valores, México

DIRECTOR REGIÓN CONO SUR

Juan Pedro Cantera Sención

Banco Central del Uruguay

SECRETARIO GENERAL

Pascual O'Dogherty

MIEMBROS ASBA

MIEMBROS ASOCIADOS

REGIÓN ANDINA

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

REGIÓN CARIBE

Central Bank of Belize
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
Oficina del Comisionado de Instituciones Financieras, Puerto Rico

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

