ASBA
ASOCIACIÓN DE SUPERVISORES BANCARIOS DE LAS AMÉRICAS

Financial Stability Institute
BANK FOR INTERNATIONAL SETTLEMENTS

Aspectos Destacados de la

Reunión de Implementación de Políticas sobre Fintech y Riesgo Cibernético

Montevideo, Uruguay, 14 y 15 de noviembre de 2018

Contenido

Introducción

La Asociación de Supervisores Bancarios de las Américas (ASBA) y el Instituto de Estabilidad Financiera (FSI) del Banco de Pagos Internacionales (BIS) organizaron una Reunión de Implementación de Políticas (PIM, por sus siglas en inglés) sobre Fintech y Riesgo Cibernético en Montevideo, Uruguay, los días 14 y 15 de noviembre de 2018. El objetivo de la reunión fue evaluar el entorno actual de Fintech y los desafíos críticos que la ciberseguridad plantea a los bancos y reguladores en el contexto de una mayor digitalización del negocio bancario.

Tanto los supervisores de las jurisdicciones miembros de ASBA, una selección de países extranjeros, así como expertos del sector privado obtuvieron un mayor conocimiento sobre la evolución de las nuevas tecnologías, su aplicación en las finanzas, su integración en los marcos de regulación y supervisión, y su impacto potencial en la solidez y seguridad del sector financiero. La reunión buscó aumentar la comprensión de los supervisores acerca de estos desarrollos críticos que impactan el panorama financiero de las Américas mediante un diálogo activo. Esta reunión estableció los cimientos para una discusión continua en otra reunión PIM, prevista a realizarse en la Ciudad de México el 26 y 27 de junio de 2019.

La reunión constaba de seis sesiones que abordaron las oportunidades y los desafíos derivados del uso de las nuevas tecnologías en el sector financiero, así como sus posibles impactos en los bancos y los enfoques de supervisión. La discusión reflejó tanto la perspectiva del sector público, como la perspectiva del sector privado.

La primera sesión presentó la perspectiva del sector privado, en la que los bancos y otros participantes del mercado debatieron acerca del desarrollo actual de fintech y los desafíos relacionados que presenta para la intermediación financiera. La segunda sesión desarrolló las amenazas actuales de ciberseguridad para las instituciones financieras y las estrategias que se están desarrollando para contrarrestarlas. La tercera sesión se concentró en la entrada de nuevos competidores fintech y el uso de mejor tecnología en el sector financiero. En particular, esta sesión se enfocó en el análisis de modelos de negocios nuevos y en proceso de cambio, incluyendo las prácticas de gestión de riesgos en los bancos, principalmente impulsadas por los desarrollos fintech.

La cuarta sesión brindó una descripción general sobre el uso potencial de las tecnologías en las actividades de supervisión, aplicaciones típicamente conocidas como "suptech". Estas se encuentran todavía en una etapa temprana, aunque los participantes tuvieron la oportunidad de aprender acerca de una gama de aplicaciones y soluciones actualmente en desarrollo o aquellas que podrían ser operativas en el corto plazo.

Las sesiones quinta y sexta abordaron la perspectiva del sector público en dos temas. El primero examinó las implicaciones de fintech para la regulación y supervisión. Un desafío importante al que se enfrentan varias jurisdicciones, es el desarrollo de un marco proporcional que equilibre la prudencia y la innovación al mismo tiempo que garantice un campo de juego nivelado para los jugadores existentes y los nuevos participantes. El segundo tema examinó las estrategias que está adoptando el sector público para hacer frente al riesgo cibernético en la región.

La siguiente sección presenta un resumen de las experiencias compartidas por los participantes, así como los hallazgos y conclusiones más relevantes de la reunión.

Tecnologías y retos comunes

El grupo clasificó varias tecnologías en base a sus características y su potencial para desestabilizar a las instituciones financieras y al sector público. Se discutieron los beneficios potenciales de las nuevas tecnologías que respaldan la eficiencia del mercado, fomentando los modelos de negocios actuales en los bancos, promoviendo la inclusión financiera y respaldando las actividades de regulación y supervisión. Las siguientes fueron las tecnologías más disruptivas identificadas:

- *Open banking* (Banca abierta). El uso de API (Interfaces de Programación de Aplicaciones) para permitir que terceras personas accedan a los datos de clientes de las instituciones financieras y otra información general para el desarrollo de productos y servicios.
- *Cloud computing* (Computación en la nube). Este es un modelo de tecnología de la información que consiste en la provisión y el uso de recursos informáticos que se configuran a pedido (por ejemplo, servidores, almacenamiento, aplicaciones y más) a través de una red de Internet, en lugar de una conexión física a un servidor local. Los servicios de computación en la nube permiten a los clientes almacenar información, procesos y datos en servidores a los que se puede acceder a través de cualquier computadora con conexión a Internet[1].
- *Blockchain* (Cadena de bloques). Aunque se conoce principalmente por su uso en el desarrollo de criptomonedas, esta tecnología tiene otras aplicaciones relevantes en el sector financiero, por ejemplo, en el sector seguros y en la gestión de contratos. Hasta la fecha, esta tecnología no ha tenido una penetración extensa en el sector financiero; sin embargo, está bajo el escrutinio del sector público y privado debido a sus posibles implicaciones para la introducción de fricciones en el mercado, la identificación de clientes y el lavado de dinero, entre otros.
- Cripto-activo. La tecnología de *blockchain* y criptomonedas no son sinónimos. Algunas criptomonedas se basan en diferentes tipos de tecnologías. Existe un desacuerdo en la opinión sobre este asunto. Si bien algunas autoridades y participantes del mercado promueven el uso de monedas virtuales, los gobiernos y las organizaciones internacionales están destacando los riesgos económicos y sociales que estos instrumentos podrían traer al mercado. No existe consenso sobre la utilidad o repercusión de estas tecnologías.
- Inteligencia Artificial (IA). Actualmente, la mayoría de los modelos de AI se utilizan en el sector privado: el uso de *chatbots* para la gestión de preguntas y respuestas de los clientes, y el *aprendizaje automático* (*machine learning*) para adaptar los servicios y las calificaciones crediticias, entre otros. Sin embargo, si se administra adecuadamente, esta tecnología podría apoyar al sector público, especialmente en mejorar la eficiencia de algunas actividades de supervisión.

Considerando la acelerada evolución e introducción de nuevas tecnologías, los reguladores, supervisores y proveedores de servicios financieros están expuestos a riesgos estratégicos y de reputación. Por un lado, estos riesgos podrían tener un impacto potencial en el desempeño financiero de las instituciones en la medida en que sus decisiones actuales (cambio de los modelos de negocios, asociaciones, subcontratación) se desvíen de la inercia del sector en su conjunto. A pesar de la creciente importancia del riesgo de reputación, la gran mayoría de las entidades parecen no contar con un enfoque estratégico bien pensado para la gestión adecuada del riesgo de reputación. Al contrario, el riesgo de

[1] ASBA, Una Perspectiva General de Fintech: Sus Beneficios y Riesgos, 2017

reputación generalmente se aborda como un tema de gestión de crisis, enfocándose principalmente en las consecuencias de un evento. Por otro lado, las deficiencias de reputación de las instituciones financieras pueden cuestionar indirectamente la credibilidad y competencia de las autoridades reguladoras y de supervisión.

Un tema importante relacionado con los aspectos estratégicos y de reputación es el uso cada vez mayor de los servicios de subcontratación u *outsourcing* que conducen a una concentración potencial de proveedores. Un mayor uso de terceros (proveedores de soluciones tecnológicas, productos basados en la nube y otros) asigna una dimensión adicional del riesgo operacional existente sobre la reputación de la institución de subcontratación, que podría ser tanto una institución financiera como una institución de supervisión. Cuanto menos conocen las instituciones financieras y los supervisores acerca de los proveedores externos, mayor es el riesgo. Un comportamiento negativo de un proveedor de servicios externo puede tener repercusiones y afectar negativamente la reputación de la entidad y de la agencia supervisora, especialmente cuando el público percibe a estos últimos como protectores del cliente (aunque en algunos países esto no sea parte de su mandato). El problema se agrava cuando los proveedores externos ofrecen sus servicios a muchas instituciones, incluso de manera transfronteriza.

La ciberseguridad es un problema importante que afecta a varios sectores económicos. Sin embargo, el sector financiero es más propenso a este tipo de amenaza. La cantidad y sofisticación de los ataques cibernéticos en el sector financiero han aumentado considerablemente en los últimos años. En el sector privado, los ataques se producen a través de retiros significativos de dinero, fraude, robo de identidad y otros. El sector público está expuesto al robo de información sensible sobre las operaciones del sector financiero y al impedimento de las actividades de regulación y supervisión. La creciente dependencia de tecnologías y proveedores externos amplifica el problema. Es fundamental establecer expectativas de supervisión claras sobre cómo lidiar con el riesgo cibernético y capacitar a las entidades, así como aumentar su conocimiento al respecto. Además, los clientes y empleados bancarios deben entender su propio papel crucial en la prevención y denuncia de ataques cibernéticos.

La seguridad cibernética es un tema que debe ser tratado en etapas. En este sentido, se han identificado tres etapas importantes. La primera etapa es crear conciencia y reconocer la existencia del problema. Esto incluye una comprensión de dónde podrían provenir los ataques, la identificación de las áreas más vulnerables y la capacitación del personal (muchos de los ataques tienen éxito porque el personal de las instituciones lo permite, ya sea de manera voluntaria o involuntaria). La segunda etapa es el desarrollo de una estrategia y de herramientas para responder adecuadamente y enfrentar un ataque cibernético. Estas incluyen herramientas tecnológicas y de políticas, así como manuales para prevenir y contrarrestar posiblemente un ataque. En este punto, es esencial mencionar que los proveedores externos deben ser parte de las políticas de resiliencia cibernética. La tercera y última etapa es la implementación y el uso efectivo de las políticas, manuales y herramientas disponibles. Esta es la etapa más desafiante, ya que requiere un esfuerzo colectivo y un cambio posiblemente más radical en la cultura de las instituciones.

El cliente y sus datos se han convertido en elementos críticos del nuevo entorno financiero. Actualmente, existe la percepción de que los bancos, otras instituciones financieras y las fintechs están compitiendo para proporcionar una mejor experiencia para el cliente. Por lo tanto, el cliente se ha convertido en el centro de atención y los datos tanto financieros, como no financieros (redes sociales, ubicaciones y demás) se han tornado más valiosos para el diseño y la provisión de productos y servicios financieros.

Se identificaron dos temas fundamentales relacionados con el cliente y sus datos: la simetría en el

acceso a la información financiera y la falta de definición de los datos públicos y los datos de interés público. Primero, relacionado con el tema del *open banking*, algunas jurisdicciones han emitido regulaciones para promover mecanismos de intercambio de datos, por lo que los bancos estarán obligados a proporcionar acceso a cierta información financiera de sus clientes; los expertos mencionaron que este tema tiene el potencial de agregar riesgos estratégicos y de reputación si se implementa incorrectamente. En segundo lugar, desde el punto de vista de la política pública, todavía existe dificultad en la definición del significado exacto de los datos públicos y los datos de interés público. No existe mucha claridad más allá de reconocer su importancia. Sin embargo, si se acuerda un perfil de datos, el desarrollo de mecanismos que puedan permitir el acceso formal y legal a dichos datos será crítico.

Sector Público

El nuevo entorno puede requerir un cambio en la mentalidad, la cultura y los procedimientos de las agencias reguladora y de supervisión. Sin duda, las autoridades de supervisión necesitan desarrollar nuevos conjuntos de habilidades en su personal de supervisión. Aunque, en general, el mandato y las responsabilidades de los supervisores no pueden cambiar frente a este nuevo entorno, los supervisores deben crear un nuevo perfil de supervisión adicional y desarrollar nuevas habilidades y herramientas haciendo uso de las nuevas tecnologías. En otras palabras, los objetivos de la política pública pueden no cambiar, pero los procedimientos y las capacidades para cumplirlos y gestionarlos cambiarán. El perfil del nuevo supervisor debe ser más prospectivo, proactivo, capaz de utilizar tecnologías innovadoras y debe comprender los aspectos macroeconómicos y las evaluaciones microprudenciales tradicionales de las instituciones financieras.

La disrupción de los modelos de negocios bancarios debido a la entrada de nuevas tecnologías en el sector financiero significa que los reguladores y supervisores que están a cargo de supervisar a los bancos y las instituciones tradicionales tendrán que coordinarse cada vez más con otras partes interesadas. Esta noción va más allá de la idea de supervisar fintechs. La creciente interconexión con las partes interesadas en el sistema financiero, la incorporación de nuevas tecnologías en las instituciones reguladas "tradicionales", el desarrollo de un área importante fuera de la regulación, y la interacción con proveedores externos especializados obligarán ya sea de manera directa o indirecta a los reguladores y supervisores a supervisar otras partes interesadas (por ejemplo, plataformas de pago, proveedores de soluciones en la nube y una gama de diferentes API de soporte). Esto los sacará de su zona de confort: dado que pasarán de supervisar temas prudenciales y de conducta únicamente, a evaluar temas de gobierno corporativo en un entorno empresarial liderado de manera digital, así como gestión de la información financiera, acuerdos sólidos de *open banking*, o gestión de amenazas de ciberseguridad.

En cuanto al uso de la innovación, el sector público ha estado detrás del sector privado. El uso de nuevas tecnologías será esencial en futuras actividades de supervisión. El sector público no ha tenido los mismos incentivos que el sector privado para invertir en desarrollos tecnológicos que pueden hacer que sus actividades sean más eficientes. El sector privado se ha desarrollado de tal manera que ha comenzado a producir grandes cantidades de información, que el sector público tiene dificultades para gestionar. Algunos tipos de tecnologías que podrían ayudar a los supervisores a llevar a cabo sus funciones son el análisis de *big data* y las herramientas de inteligencia artificial.

El desarrollo de soluciones suptech es una inversión a largo plazo y no implica que los supervisores puedan ser reemplazados; sin embargo, un uso más eficiente de los recursos de supervisión es

importante. De hecho, algunas autoridades de supervisión han comenzado a desarrollar herramientas internas de apoyo para la supervisión o las han subcontratado; otras no han iniciado este proceso de modernización. La adopción de enfoques suptech ayuda a los supervisores a ser más proactivos y orientados hacia el futuro. Además, se deberán desarrollar estrategias para atraer y retener expertos en la recopilación, verificación de integridad, análisis e interpretación de la información para responder a los desafíos planteados por el mercado de manera oportuna.

Los reguladores y supervisores aún carecen de claridad con respecto al establecimiento del perímetro regulatorio para los actores y sus actividades. El sector público se enfrenta a un dilema en la búsqueda de un equilibrio adecuado entre regular o no regular algunas innovaciones. Si la regulación comienza demasiado temprano, existe la posibilidad de obstaculizar innovaciones beneficiosas que podrían hacer que los mercados sean más competitivos y eficientes. Por otro lado, si la regulación llega muy tarde, podrían surgir algunos riesgos inherentes a la estabilidad financiera sin contar con los instrumentos regulatorios y de supervisión necesarios para contenerlos; esto es particularmente importante en lo que respecta a los aspectos sistémicos.

Algunos supervisores consideran que las regulaciones de innovación financiera deben desarrollarse en etapas, abordando los problemas más urgentes a través de herramientas de supervisión y regulación actuales (o ligeramente modificadas) y desarrollar nuevos instrumentos de política a medida que el mercado evoluciona. La primera etapa consistiría en trabajar en la construcción de mecanismos que establezcan incentivos correctos a través de las regulaciones existentes. Se deben desarrollar principios básicos para productos y servicios financieros que se desvíen de los incentivos actuales. Finalmente, en algunos casos, puede ser necesario adoptar reglas prescriptivas cuando ciertos modelos de negocios superan los principios establecidos y cuando las reglas deben ser más estrictas para un mejor control y gestión del supervisor.

Una regulación basada en principios en lugar de reglas prescriptivas, como la propuesta por la *Financial Conduct Authority* del Reino Unido, puede dar flexibilidad a la adopción responsable de innovaciones tecnológicas en el sector financiero en las primeras etapas. Todavía hay un debate sobre las ventajas y desventajas del enfoque basado en principios y el enfoque basado en reglas. Un enfoque basado en principios podría ser adecuado por las siguientes razones: los proveedores conocen su negocio mejor que nadie y existe una escasez de expertos en tecnología de la información en las instituciones públicas, así mismo existe una comprensión inadecuada del funcionamiento de las nuevas tecnologías y hay evidencia limitada para entender el impacto de ciertas tecnologías en el sector financiero. En este contexto, la coordinación entre los reguladores y el sector privado es importante en los casos en que el regulador establece los objetivos y el sector privado podría desarrollar propuestas sobre cómo alcanzar dichos objetivos. Sin embargo, un enfoque basado en reglas no se puede descartar en algunos casos o actividades a medida que los mercados evolucionan. La combinación de ambos métodos puede equilibrar los beneficios y riesgos de la innovación financiera.

La discusión sobre el perímetro regulatorio llevó a la idea de que los mismos riesgos deben cumplir con la misma regulación. Si bien algunas jurisdicciones se enfocan en la actividad financiera subyacente, otras consideran que la regulación de la tecnología será fundamental (por ejemplo, *cloud computing*, API, *blockchain*). Sin embargo, parece haber un acuerdo tácito de que los mismos riesgos deberían cumplir con las mismas regulaciones, aunque esto podría ser difícil de lograr en la práctica.

Sin lugar a dudas, en este nuevo entorno, el riesgo operacional ha aumentado y continuará creciendo. Uno de los desafíos más críticos, desde una perspectiva regulatoria, es comprender hasta qué punto algunos asuntos podrían considerarse dentro del marco de gestión de riesgo operacional

existente. Desde el punto de vista del BCBS, los estándares de gestión del riesgo operacional aún son aplicables a los temas de riesgo tecnológico y cibernético. Por otro lado, los bancos y algunos reguladores consideran que los problemas tecnológicos deben abordarse desde una perspectiva diferente, aunque no hay claridad sobre el mejor enfoque. Algunas jurisdicciones, como Alemania, han desarrollado una metodología más amplia y cooperan con expertos para supervisar los marcos de gestión de la ciberseguridad dentro de las instituciones financieras. Otras jurisdicciones, como Chile, han adoptado una postura menos directa, abordando el tema desde una perspectiva más integral en comunicación con otras autoridades (por ejemplo, a través de una Estrategia Nacional).

El regulador/supervisor debe entender su papel dentro del conjunto de estrategias que abordan los riesgos tecnológicos y de ciberseguridad. Algunas actividades trascienden las actividades financieras habituales y los límites jurisdiccionales. Aunque el sector financiero es más propenso a los ataques, el riesgo cibernético trasciende a otros sectores y jurisdicciones. Por un lado, el regulador debe comprender cuál es su función y alcance dentro del grupo de autoridades que podrían tener las mismas preocupaciones y, a partir de ahí, desarrollar una estrategia interna que no entre en conflicto con otras autoridades o mandatos. Por otro lado, ciertos productos y servicios operan en más de una jurisdicción. Si bien no existe una estrategia clara sobre cómo enfrentar el aspecto transfronterizo, la comunicación entre las autoridades de diferentes países y regiones es esencial.

Las empresas fintechs y otros desarrollos tecnológicos pueden apoyar la inclusión financiera cuando se combinan con otros mecanismos de política. Hace un par de años, existía la percepción de que el ingreso de empresas fintech era un sinónimo de inclusión financiera. Los desarrollos actuales han demostrado que estas innovaciones también son útiles para proporcionar mejores servicios financieros a los segmentos ya atendidos del mercado. Sin embargo, muchas fintechs actualmente no están considerando los segmentos desatendidos o no atendidos en sus estrategias, lo que deja un amplio margen para expandir sus modelos de negocios.

Sector Privado

Aunque existen tensiones entre las entidades tecnológicas no reguladas e instituciones financieras reguladas, parece existir una convergencia hacia un entorno más colaborativo. El desarrollo del ecosistema fintech está ocurriendo de manera más colaborativa que competitiva, en comparación con el entorno hace algunos años. Las nuevas partes interesadas necesitan la infraestructura y podrían beneficiarse de la experiencia y confianza que los clientes actuales tienen en el sistema tradicional. Además, las instituciones financieras parecen ser más explícitas sobre el impacto de las fintech en sus estrategias comerciales y se asocian con nuevas partes interesadas o invierten en estrategias digitales que pueden ayudarlas a adaptarse al nuevo entorno.

En el contexto actual, las decisiones sobre estrategias digitales se están llevando a cabo en un entorno de cambios regulatorios significativos. No solo las nuevas partes interesadas son parte del ecosistema conocido como fintech, sino también las instituciones tradicionales que incorporan estas nuevas tecnologías en sus servicios. Sin embargo, la reciente finalización del paquete regulatorio de Basilea III y el proceso de implementación intensiva en curso, plantean un desafío adicional para los bancos, ya que tendrán que equilibrar sus prioridades estratégicas entre el cumplimiento normativo y las innovaciones digitales, entre otros. Lo anterior se ha sumado a la tensión entre los bancos y las exigencias regulatorias.

Un enfoque proporcional, aunque no queda claro cómo se verá, podría ayudar, pero a veces puede tener limitaciones al momento de definir la profundidad y el alcance de este proceso. La adopción

de marcos regulatorios y de supervisión proporcionales en un mundo digital se ve desafiada por el alcance de las nuevas tecnologías, las complejidades de su gestión legal y la insuficiencia de algunos de los marcos legales actuales.

El poder de negociación entre las instituciones financieras y sus clientes se ve perturbado por el ingreso de nuevas partes interesadas. Hasta hace unos años, el poder de negociación de los bancos sobre sus clientes era amplio. La entrada de nuevas partes interesadas ha permitido a los clientes elegir entre otras opciones de servicio que son más fáciles de utilizar y tienen costos más bajos, aunque no son necesariamente las más seguras. Hoy en día, existe una competencia respecto a proporcionar al cliente una experiencia amigable y personal; por lo tanto, las instituciones financieras tradicionales se ven obligadas a desarrollar estrategias para mejorar la experiencia de sus clientes.

Tanto las empresas fintech, como las instituciones financieras tradicionales deben comprender que la transformación del sector financiero se enfoca, en gran medida, en los clientes. Los clientes deben conocer su papel y el valor de su información. Los proveedores de servicios financieros dependerán cada vez más del acceso y uso de los datos de los clientes. El valor inherente de los datos adquiere un valor significativo. Sin embargo, los clientes aún desconocen el costo de su información y la fuerza de su poder de negociación. Cuando los clientes se dan cuenta del valor de sus datos, la dinámica del mercado puede cambiar porque tendrán bajo su control la decisión de con quién, cuándo y con qué fines compartirán su información. En este sentido, el uso actual de herramientas automáticas y la falta de reglas para nuevos competidores representan riesgos de seguridad para los clientes.

El intercambio de información será fundamental en el nuevo entorno. Sin embargo, algunas estructuras de *open banking* podrían representar amenazas a la integridad de las instituciones financieras. Al ingresar a una estructura de información compartida, los bancos podrán acceder a otros API del mercado o del gobierno que les permitirán expandir sus servicios, introducir nuevas soluciones e identificar, con mayor precisión, los cambios en la información de sus clientes. Al contrario, podrían existir algunas discrepancias al acceder a la información porque cuando un banco abre sus API, permitirá que fintechs y otras partes interesadas accedan a datos confidenciales de los clientes. Este acceso no es necesariamente perjudicial; sin embargo, en algunos esquemas, un cliente puede autorizar el uso de sus datos por parte de un tercero que no tiene relación con el banco. Por lo tanto, si el acceso resulta en un conflicto, la responsabilidad y el riesgo reputacional recaerán en el banco. Si bien existen iniciativas privadas (como en los EE. UU.) y públicas (PSD2 en Europa), los impactos y beneficios de las iniciativas emergentes de acceso a la información no están claros.

La entrada de grandes empresas de tecnología (*Big Tech*) en la provisión de servicios financieros podría generar importantes desafíos relacionados con la competencia y el riesgo sistémico y podría afectar el negocio bancario en diferentes dimensiones. Es razonable pensar que las grandes empresas que dominan el mercado de la tecnología también pueden querer proporcionar servicios financieros. Su ventaja comparativa radica en las relaciones existentes con los clientes, incluyendo la disponibilidad de datos de los clientes y en su capacidad de desarrollar las plataformas e infraestructura de TI necesarias para la prestación de servicios financieros. Por otro lado, estas empresas pueden mostrarse tímidas al aceptar el costo y la carga adicional del cumplimiento regulatorio asociado con la recepción de una licencia bancaria. Si las empresas *Big Tech* ingresan al mercado, podría haber un riesgo de concentración en el mercado y tensiones competitivas con el sistema bancario tradicional. Además, su presencia internacional tiene el potencial de generar riesgos sistémicos. Finalmente, si las empresas *Big Tech* se convierten en proveedores externos que prestan servicios al sector financiero, existen preocupaciones obvias sobre la dependencia tecnológica y la concentración de riesgos.