Fintech: servicios financieros digitales en el siglo XXI

DOI: 10.29236/sistemas.n150a6

Reflexiones sobre ciberseguridad y seguridad de la información.

Resumen

En un contexto acelerado de disrupciones e innovaciones, la banca no ha sido ajena a los efectos de la transformación digital de sus productos y servicios. En este escenario, el fundamento de la actividad bancaria como lo son la creación de dinero y los créditos, así como la intermediación entre los clientes y las empresas, se ha venido revaluando y ha dado lugar a un quiebre en sus prácticas vigentes. En tal sentido, este artículo plantea algunos análisis sobre los retos de ciberseguridad y seguridad de la información, a propósito de los nuevos portafolios de iniciativas digitales como las fintech, que buscan desintermediar a la banca de sus oficios tradicionales.

Palabras clave

Fintech, finanzas, tecnología, ciberseguridad, vulnerabilidades

Jeimy J. Cano M.

Introducción

La incorporación acelerada de tecnologías de información y comunicaciones en los diferentes contextos de la vida está cambiando muchos paradigmas de intermediación y negocios, devolviendo el control y las relaciones entre las personas y los diferentes productos y servicios disponibles en la actuali-

dad, a los clientes. En este sentido, el aumento de la densidad digital y de los flujos de información establecen retos emergentes que implican una manera distinta de concretar una experiencia con los usuarios.

La banca no ha sido la excepción y, por lo tanto, enfrenta uno de sus más importantes desafíos, que implica repensar la base fundamental de las relaciones con sus clientes: ser un intermediario o tercero de confianza. "*Durante la era industrial, la banca era una buena forma de organizar los elementos del sistema financiero: el dinero y el crédito*" (McMillan, 2018, p.31); hoy, con la incorporación de tecnologías de información, los elementos clave del negocio financiero entre ellos la asimetría de la información, el seguimiento del crédito y los servicios de pago pueden ser ofrecidos por nuevos terceros, confiables y a bajos costos.

Las fintech surgen como la respuesta a la convergencia entre los retos propios de los servicios financieros y el uso de las tecnologías de información, como una innovación que cambia las reglas de juego del sector financiero. Las fintech proporcionan una plataforma para bancos y entidades no bancarias, orientadas a facilitar las transferencias entre redes, los servicios de pago y el acceso a la información, con lo que "*la actividad bancaria no queda circunscrita a unas entidades concretas denominadas bancos o instituciones financieras*" (McMillan, 2018, p.162).

En consecuencia, las fintech ofrecen a los consumidores beneficios a través de la transparencia, la creación conjunta, la personalización y la optimización del tiempo en redes más descentralizadas y sin la intermediación del sector bancario. Sin embargo, aún no se han aclarado los riesgos asociados a estas nuevas innovaciones (Felländer, Siri, & Teigland, p.154) que cambian el paradigma financiero vigente hasta el momento. Por tanto, es necesario analizar las amenazas y los riesgos emergentes en este nuevo entorno, con el fin de aumentar la confianza de los clientes en el contexto digital actual de los servicios financieros.

Este artículo se desarrolla con el fin de explorar los retos de ciberseguridad, seguridad y control de las fintech, además de establecer algunas reflexiones para que los usuarios puedan comprender la evolución de esta tendencia que, de obtener ventajas competitivas basadas en el flujo de los datos a través de internet, está pasando a la creación de experiencias de usuario basadas en la incorporación de tecnologías de información y las comunicaciones (Lee, Yen, & Hurl-Burt, 2018).

Esencia de las fintech

De acuerdo con Gomber, Kauffman, Parker, & Weber (2018) la revolución de las Fintech descansa

sobre tres pilares claves de innovación. En primer lugar, *los capitales disponibles* para la innovación tecnológica de los servicios financieros como un área altamente productiva de la economía mundial. En segundo lugar, *el desarrollo de servicios novedosos* que abordan las necesidades de los clientes financieros de manera muy directa, valiosa y de cara al futuro. En tercer lugar, *la transformación de los modelos de negocio*, la intermediación financiera y el acceso de los clientes a través de altos niveles de personalización, basados en la detección digital y en la analítica de grandes datos, sustituyendo a los bancos tradicionales y sus servicios por nuevas maneras.

En este contexto, las relaciones de las fintech y los bancos comerciales crean tensiones naturales en las inversiones, las regulaciones, el comportamiento del cliente y las tecnologías emergentes (Vasiljeva & Lukanova, 2016), las cuales terminan afectando la confianza de los individuos respecto del uso y la apropiación de las nuevas apuestas y los servicios financieros que se puedan generar.

Un reciente estudio realizado por la firma A.T Kearney, en nombre de la Cámara de Compensación de los Estados Unidos de América (THC – ATK, 2018), sobre los comportamientos digitales de los clientes bancarios (usuarios de aplicaciones no bancarias), confirma lo dicho previamente y muestra que, casi nueve de cada diez consumidores (89%) declararon estar preocupados por la privacidad de los datos y la forma en que éstos se comparten; y, más de dos tercios (67%), están muy o extremadamente preocupados.

Esta sensación de incertidumbre sobre los usos de las fintech, define agendas de investigación y desarrollo para el diseño de servicios digitales (Williams, Chatterjee, & Rossi, 2008), más confiables y robustos, de tal forma que los usuarios puedan comprender las bondades y limitaciones de los ecosistemas digitales donde se construyen, para potenciar propuestas inéditas, en lo que se refiere a la habilitación de relaciones más fluidas y ágiles entre los particulares y las empresas.

Este ecosistema digital fintech establece un escenario de interacciones entre sus diferentes componentes, detallados a continuación, los cuales advierten un aumento de la dinámica en la desintermediación como fundamento de las nuevas relaciones de los clientes en un contexto digital. Los componentes son:

- Emprendimientos de fintech (pagos, administración de patrimonio, préstamos, crowdfunding, mercado de capitales y compañías de seguros fintech).

- Desarrolladores de tecnología (grandes analistas de datos, com-

putación en nube, criptomonedas y desarrolladores de medios sociales).

- Gobierno (los reguladores financieros y la legislación).

- Clientes financieros (individuos y organizaciones).

- Instituciones financieras tradicionales (bancos tradicionales, compañías de seguros, firmas de corretaje de bolsa y capitalistas de riesgo) (Lee & Shin, 2018).

En el contexto de los servicios financieros como fenómeno disruptivo, las fintech crean relaciones y oportunidades emergentes, para dar lugar a una interacción más cercana entre los individuos, los productos y servicios, motivando un flujo de información para mejorar en cada momento la experiencia del usuario, y así descubrir nuevas fronteras y apuestas digitales, que den cuenta y anticipen expectativas retadoras y confiables para sus clientes (Wonglimpiyarat, 2017).

Retos y vulnerabilidades de las fintech

El desarrollo de los servicios financieros fuera de los límites del marco de supervisión y regulación puede dar lugar a la aparición de nuevos riesgos. La incorporación de tecnologías emergentes aceleran en forma significativa la velocidad y el volumen de las transacciones financieras, lo que necesariamente puede aumentar las vulnerabilidades y la probabilidad de un ciberataque (He, Leckow, Haksar, Mancini-Griffoli, Jenkinson, Kashima, Khiaonarong, Rochon, & Tourpe, 2017). En tal sentido, es necesario establecer un marco de revisión de los retos y amenazas que las fintech incorporan al ecosistema digital financiero, con el fin de tomar decisiones informadas y de manera coherente con los objetivos y las promesas de valor que vienen con estas innovaciones.

De acuerdo con Gai, Qiu, & Sun (2018), son tres los elementos claves para comprender los retos de seguridad y privacidad en las fintech: las operaciones de negocio, el outsourcing y la privacidad financiera.

Las posibles amenazas que se derivan de las operaciones de negocio están relacionadas con el desconocimiento de los detalles técnicos, procesos de implementación poco transparentes y el desarrollo de las estrategias de tecnología de Información (TI). La complejidad de las operaciones e interacciones con diferentes tecnologías y necesidades de los clientes, establece un mapa de riesgos emergentes que se relacionan con el fraude en las transacciones, la suplantación de los clientes, las vulnerabilidades en el software (conocidas y desconocidas), las fallas en la infraestructura y el limitado aseguramiento de controles establecidos, dada la agilidad y eficiencia que se re-

quiere en el despliegue de las soluciones propuestas.

El outsourcing se refiere al uso de terceros confiables que implementan y despliegan las soluciones en un contexto de computación en la nube. Al involucrar un tercero en la apuesta tecnológica y de valor de la empresa, necesariamente se pierde el control de las operaciones. En este sentido, se debe procurar el fortalecimiento de la confianza con el proveedor de servicios en la nube, para lo cual certificaciones como SSAE-18[1] suelen ser referentes hacia un mejor perfil de la gestión de riesgos del proveedor, como quiera que, son los datos y las aplicaciones que usan los clientes los que están en juego, cuando una brecha de seguridad se materializa en un entorno de operaciones externo a la fintech.

La privacidad como derecho fundamental de los clientes es un factor relevante a la hora de proponer servicios novedosos en las fintech. Los flujos de datos personales y financieros, a través de plataformas en la nube, pueden estar expuestos no sólo a vulnerabilidades desconocidas por el mismo proveedor, sino al movimiento de los mismos en distintas jurisdicciones internacionales, creando tensiones con las reglamentaciones vigentes y aumentando las exigencias, tanto para las fintech como para sus proveedores. Un caso particular es el reciente Reglamento General de Protección de Datos[2] en Europa que demanda acciones particulares ante la transferencia internacional de datos en sus artículos 45, 46 y 49.

Sin perjuicio de lo anterior, las fintech, al ser negocios financieros emergentes que han resultado (inicialmente) atractivos para los emprendedores en este tema, deberán facilitar una visión vigilante de escenarios complejos e inciertos de posibles adversarios que, no solamente estarán allí para encontrar formas de concretar fraudes y efectuar robos de activos, sino de terceros no conocidos con intenciones de desestabilizar la dinámica financiera de un país o región, para lo cual las brechas en las fintech son una excusa perfecta que genera desconfianza o el pánico requerido en el manejo de las transacciones entre los bancos y estos negocios.

Seguridad, ciberseguridad y privacidad en las fintech

Dada la estructura distribuida de la configuración e implementación de las soluciones o apuestas de valor de las fintech, establecer o configurar una práctica de seguridad, ciberseguridad o privacidad estándar

[1] SSAE 18: *Statement on Standards for Attestation* No.18 describe los controles del proveedor de servicios y permite a las empresas comprender mejor los procesos y procedimientos que ayudan a construir credibilidad y confianza sobre los procesos de prestación de servicio de los proveedores de nube. Detalles en: https://www.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/ssae-no-18.pdf

[2] Reglamento General de Protección de Datos Europeo disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

resulta algo complejo, considerando los diferentes actores, relaciones, flujos y conexiones existentes cuando se libera una solución de este tipo, sin perjuicio de las prácticas propias de seguridad y control ya instaladas en cada uno de los participantes (Rohmeyer & Bayuk, 2019), por lo general, basadas en normas ISO[3].

Por lo tanto, resulta de interés revisar estrategias o posturas que comprenden las acciones de los adversarios, con el fin de preparar a la organización para responder a los posibles ataques que pueda provocar una arquitectura, en la que cualquier punto o elemento puede ser ocasión de un vector para quebrar los sistemas de protección.

Una forma de avanzar en esta línea es lo que se denomina la Cadena Cyber Kill, desarrollada por la empresa de consultoría Lockheed Martin (2015), que busca detallar los pasos de los atacantes para lograr su objetivo que, a pesar de tener un enfoque militar, resulta atractivo para las organizaciones, con el propósito de avanzar en una postura preventiva o defensiva, frente a una acción dirigida o inocente de un tercero en contra de la arquitectura de negocio de las fintech.

La propuesta consta de siete pasos, en los cuales se analiza tanto la postura del adversario[4] como la del defensor[5], de tal manera que resulta un ejercicio complementario para establecer posibles marcos de actuación que se pueden resolver bien, desde la implementación o actualización de tecnología, pasando por la gestión de los procesos de negocio y su seguridad, la revisión de la cultura organizacional o incluso, desde la generación de escenarios posibles que reten las condiciones vigentes de seguridad y control de la organización.

Las etapas son:

1. Reconocimiento: exploración intencional del objetivo para identificar posibles vulnerabilidades.

2. Militarización: el adversario crea código malicioso o condiciones particulares adaptadas a las debilidades de los objetivos.

3. Entrega: el adversario ubica el código malicioso o configura el escenario en el objetivo.

4. Explotación: se ejecuta el código malicioso o se materializa el escenario estudiado según el plan del adversario.

---

[3] ISO/IEC 29100 Protección de datos personales dentro de los sistemas de tecnología de la información y la comunicación (TIC), ISO/IEC 27032 Tecnología de la información - Técnicas de seguridad - Directrices para la Ciberseguridad, ISO 27002 mejores prácticas en la gestión de la seguridad de la información – Controles de seguridad de la información.

[4] Generalmente asociado con crimen organizado, mercenarios digitales o grupos contratados al margen de las regulaciones.

[5] Ejecutivos y Analistas de seguridad y ciberseguridad disponibles en los diferentes participantes del ecosistema digital.

5. Instalación: la condición adversa se enraíza y conecta en el contexto del objetivo.

6. Mando y control: el código malicioso se comunica con los sistemas del adversario y se crea una condición de control remoto.

7. Acción sobre los objetivos: el código malicioso realiza la acción planeada o el escenario desarrolla y materializa los efectos deseados.

Asumir un enfoque desde el adversario, como la cadena Cyber Kill, permite no solo retar los conocimientos y prácticas estándares generalmente adoptadas en el sector financiero, sino que aumenta la capacidad de las fintech de entender y responder de manera dinámica a las acciones no autorizadas de terceros que quieran resquebrajar la confianza digital requerida para evolucionar hacia servicios digitales ágiles y confiables.

Reflexiones finales

En un contexto cada vez más volátil, incierto, complejo y ambiguo construir parámetros o estándares de confianza digital resulta una tarea que no se puede adelantar de forma solitaria. Este ejercicio demanda que los diferentes actores del ecosistema digital establezcan medidas y acciones para aunar esfuerzos en la creación de un contexto creíble de confiabilidad, de manera que los clientes conozcan y consuman los nuevos servicios diseñados bajo el amparo de las fintech.

Es así, que los atacantes apalancados por datos y análisis, basados en ecosistemas abiertos y disponibles como Apple, Facebook o Google entre otros, están abriendo nuevos escenarios de captura y comercialización ilegal de datos, con el fin de aumentar la adquisición, retención y lealtad de clientes, provisión de crédito y mejoramiento de las ventas cruzadas, capacidades únicas que el sector bancario había construido y mantenido por mucho tiempo (Mckinsey, 2016). Por tanto, el surgimiento de los servicios digitales trae consigo la virtud y las bondades de la conectividad, así como el reto de las vulnerabilidades (a nivel de la tecnología, las personas y los procesos) y sus posibles consecuencias.

Lo anterior demanda que las nuevas iniciativas de innovaciones financiero-tecnológicas desarrollen capacidades digitales relacionadas, no sólo con la generación de conocimiento basado en datos, desarrollo de experiencias en los clientes, marketing digital, operaciones digitalmente habilitadas y tecnología de nueva generación (Mckinsey, 2016), sino alrededor de la ciberseguridad como un elemento natural del negocio, que no sólo sea responsabilidad del área de tecnología de información, sino que haga parte inherente de las apuestas de valor presentadas a

los clientes y una muestra de la forma como la organización responde a los retos de los ciberataques.

En este sentido, tanto las fintech, como los reguladores y los diferentes actores del ecosistema digital financiero deben comprender los nuevos desafíos impuestos por los ciberriesgos, como una lectura sistémica de un entorno asimétrico e inestable, que exige crear escenarios controlados (como los "Sandbox regulatorios") para probar los nuevos servicios y productos financieros (Truby, 2018; Callen & James, 2018); pero igualmente adelantar inversiones significativas en capacidades de defensa cibernética para facilitar el desarrollo de una economía digital (Abbosh & Bissell, 2019), basada ahora en el aumento creciente de una sociedad digital y tecnológicamente modificada.

En esa dirección, crear una lectura de confiabilidad (no de invulnerabilidad) para un negocio digital fundado en un escenario incierto y ambiguo como los nuevos ecosistemas digitales, es una tarea que va más allá del diseño genérico de un sistema de información seguro (Li & Li, 2016). Por tanto, es necesario un trabajo conjunto entre la industria y la academia para adelantar investigaciones concretas sobre las fintech, establecer una plataforma de comunicación entre los actores del ecosistema que conecte expectativas y capacidades de los participantes, además de establecer un punto de encuentro entre los reguladores y los nuevos emprendedores de servicios financieros digitales (Ng & Kwok, 2017).

De esta forma, el emergente universo fintech no sólo tendrá un espacio privilegiado para capitalizar emprendimientos novedosos y financieramente atractivos, sino que podrá generar alianzas estratégicas con los bancos comerciales (Temelkov, 2018), de manera que las ventajas de los dos mundos se complementen. Por una parte, la creación de un entorno resiliente que responda a las agresiones de los ciberatacantes (Ambore, Richardson, Dogan, Apeh, & Osselton, 2017) y, por otro lado, alinear las regulaciones existentes y en desarrollo, para advertir, revelar y comprender los riesgos emergentes y convergentes de un sector con un creciente y diverso portafolio de productos y servicios digitales.

Agradecimientos

El autor agradece a los doctores Jesús Vásquez Gómez, Especialista de Tecnología de Información del Banco Central de México y Alejandro Useche Arévalo, Director del GSB Graduate School of Business de la Universidad del Rosario, y a los maestros Juan Dávila, Director Asociado de Protiviti-Perú, José Luis Mauro Vera, Gerente de Servicios de Asesoría de EY-Uruguay y Francisco Rivas Dueñas, Subgerente General de Ser-

vicios Corporativos del Banco de la República, por sus valiosos y acertados comentarios que permitieron afinar las reflexiones de este artículo.

Referencias

Abbosh, O. & Bissell, K. (2019) Securing the digital economy. Reinventing the internet for trust. Accenture Strategy. Recuperado de: https://www.accenture.com/us-en/insights/cybersecurity/_acnmedia/Thought-Leadership-Assets/PDF/Accenture-Securing-the-Digital-Economy-Reinventing-the-Internet-for-Trust.pdf

Ambore, S., Richardson, C., Dogan, H., Apeh, E. & Osselton, D. (2017). A resilient cybersecurity framework for Mobile Financial Services (MFS), Journal of Cyber Security Technology, 1:3-4,202-224, doi: 10.1080/23742917.2017.1386483

Callen, J. & James, J. (2018). Fintech, Regtech and the importance of cybersecurity. Issues in Information Systems, 19(3), 220-225. Recuperado de: http://www.iacis.org/iis/2018/3_iis_2018_220-225.pdf

Felländer, A., Siri, S. & Teigland, R. (2018) The three phases of fintech. En Teigland, R., Siri, S., Larsson, A., Moreno, A. & Ingram, C. (Editors) (2018). The Rise and Development of Fintech: Accounts of Disruption from Sweden and Beyond. London, UK: Routledge. 154-167

Gai, K., Qiu, M. & Sun, X. (2018) A Survey on FinTech, Journal of Network and Computer Applications, 103, 262-273. doi:10.1016/j.jnca.2017.10.011

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the Fintech Revolution: Interpreting the Forces of Innovation, Disruption, and Transformation in Financial Services. Journal of Management Information Systems, 35(1), 220–265. doi: 10.1080/07421222.2018.1440766

He, D., Leckow, R., Haksar, V., Mancini-Griffoli, T., Jenkinson, N., Kashima, M., Khiaonarong, T., Rochon, C. & Tourpe, H. (2017) Fintech and Financial Services: Initial Considerations. IMF Staff Discussion Note. No. 17/05. Recuperado de: https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2017/06/16/Fintech-and-Financial-Services-Initial-Considerations-44985

Lee, I. & Shin, Y. J. (2018) Fintech: Ecosystem, business models, investment decisions, and challenges. Business Horizons, 61, 35-46. doi: 10.1016/j.bushor.2017.09.003

Lee, M., Yen, D., & Hurlburt, G. (2018). Financial technologies and applications. Guest Editor Introduction. IEEE IT Professional, 20(2), 27-33.

Li, E & Li, J. P. (2016). Information Security Challenges in the New Era of Fintech. En Proceeding of The Sixteenth International Conference on Electronic Business, Xiamen, December 4-8. 367-373. Recuperado de: http://iceb.johogo.com/proceedings/2016/ICEB-2016.pdf

Lockheed Martin (2015) Gaining the advantage. Applying Cyber Kill Chain® Methodology to Network Defense. Recuperado de: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

Mckinsey (2016) Fintechnicolor. The new picture in finance. Mckinsey Insights. Recuperado de: https://www.mckinsey.com/~/media/m

ckinsey/industries/financial%20services/our%20insights/bracing%20for%20seven%20critical%20changes%20as%20fintech%20matures/fintechnicolor-the-new-picture-in-finance.ashx

McMillan, J. (2018) El fin de la banca. El dinero, el crédito y la revolución digital. Madrid, España: Turus - Penguin Random House Grupo Editorial

Ng, A. & Kwok, B. (2017) Emergence of Fintech and cybersecurity in a global financial centre: Strategic approach by a regulator, Journal of Financial Regulation and Compliance, 25(4), 422-434, doi: 10.1108/JFRC-01-2017-0013

Rohmeyer, P. & Bayuk, J. (2019) Financial Cybersecurity Risk Management: Leadership Perspectives and Guidance for Systems and Institutions. New York, NY. USA: Springer – Apress.

Temelkov, Z. (2018) Fintech firms opportunity or threat for banks? International Journal of Information, Business and Management, 10(1), 137-143. Recuperado de: https://ijibm.elitehall.com/IJIBM_Vol10No1_Feb2018.pdf

THC – ATK (2018) Fintech Apps and Data Privacy: New Insights from Consumer Research. Agosto. Recuperado de: https://www.theclearinghouse.org-/media/New/TCH/Documents/Data-Privacy/TCH-Consumer-Research-Report-08-20-2018.pdf

Truby, J. (2018). Fintech and the city: Sandbox 2.0 policy and regulatory reform proposals. International Review of Law, Computers & Technology, 1–33. doi: 10.1080/13600869.2018.1546542

Vasiljeva, T. & Lukanova, K. (2016). Commercial banks and fintech companies in the digital transformation: challenges for the future. Journal of Business Management, 11. 25-33. Recuperado de: http://www.riseba.lv/sites/default/files/inline-files/JBM_09.02 2016_11.pdf

Williams, K., Chatterjee, S., & Rossi, M. (2008). Design of emerging digital services: a taxonomy. European Journal of Information Systems, 17(5), 505–517. doi: 10.1057/ejis.2008.38

Wonglimpiyarat, J. (2017). FinTech banking industry: a systemic approach. Foresight, 19(6), 590-603. https://doi.org/10.1108/FS-07-2017-0026

Jeimy J. Cano M., Ph.D, CFE, CICA. *Profesor Asociado. Escuela de Administración, Universidad del Rosario. Ingeniero y Magíster en Ingeniería de Sistemas y Computación por la Universidad de los Andes. Especialista en Derecho Disciplinario por la Universidad Externado de Colombia. Ph.D en Business Administration por Newport University, CA. USA. y Ph.D en Educación por la Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Es director de la Revista Sistemas de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.*