Universidad Autónoma de Querétaro
Facultad de Contaduría y Administración

ESTRATEGIA INTEGRAL DE ADMINISTRACIÓN DE RIESGOS OPERACIONALES EN INSTITUCIONES DE TECNOLOGÍA FINANCIERA DE MÉXICO.

Tesis
Que como parte de los requisitos para obtener el título de
Maestra en Ciencias Económico-Administrativas

Presenta:
Ana Leticia Servin Loyola

Santiago de Querétaro, Mayo/2019

Universidad Autónoma de Querétaro
Facultad de Contaduría y Administración
Maestría en Ciencias Económico Administrativas

ESTRATEGIA INTEGRAL DE ADMINISTRACIÓN DE RIESGOS OPERACIONALES EN INSTITUCIONES DE TECNOLOGÍA FINANCIERA DE MÉXICO

TESIS

Que como parte de los requisitos para obtener el Grado

maestra en Ciencias Económico Administrativas

Presenta:
Ana Leticia Servin Loyola

Dirigido por:
Dr. Felipe A. Pérez Sosa

Dr. Felipe A. Pérez Sosa Presidente	Firma
Dr. Michael Demmler Secretario	Firma
Dr. Jesús Hurtado Maldonado Vocal	Firma
M. en A. María Elena Díaz Calzada Suplente	Firma
Dr. Martin Vivanco Vargas Suplente	Firma

Dr. Martin Vivanco Vargas
Director de la Facultad de Contaduría y administración

Dra. Ma. Guadalupe Flavia Loarca Pina
Directora de Investigación y Posgrado

Centro Universitario
Querétaro, Qro.
Mayo / 2019
México

Resumen

La presente tesis, tiene como objetivo proponer una estrategia integral de gestión de riesgos operacionales para las Instituciones de Tecnología Financieras (*Fintech*) de México, considerando los aspectos tecnológicos, humanos, organizacionales y normativos; a fin de disminuir el impacto financiero que puedan sufrir dichas instituciones y sus clientes, ante amenazas a sus sistemas operativos. La razón por la que se realiza la presente investigación es porque, actualmente, las entidades *Fintech*, al ser innovaciones tecnológicas en el sector financiero, engloban riesgos potenciales para el sector de consumo, bancos y sistemas bancarios, que se traducen en riesgos operacionales que se presentan como oportunidades que el lavado de dinero, robo de información y el fraude pueden hallar en los procesos no regularizados de estas innovaciones, por esta razón, el papel que juega la administración de riesgos operacionales dentro de una organización es fundamental para mantener la utilidad de las compañías y brindar certeza a sus clientes, enfrentar las pérdidas que puedan presentar; mantener y garantizar el crecimiento; y preservar la continuidad y vida de las *Fintech*. Por ello, se empleó una metodología de tipo cualitativo que consistió en: describir e interpretar el marco normativo de las instituciones *Fintech* a nivel internacional, con la finalidad de hacer un estudio comparativo del contenido de los textos legales vigentes; describir las mejores prácticas a nivel internacional de las acciones en materia de regulación, supervisión y gestión de riesgos operacionales en las actividades bancarias; contextualizar el caso de estudio del Ataque a SPEI de Banxico en el 2018, centrándose en las variables que originaron las afectaciones a bancos y sistemas bancarios; y, elaborar una propuesta de gestión de riesgos operacionales para su aplicación a instituciones *Fintech*, que muestra las relaciones entre los principios gobierno corporativo, supervisión basada en riesgos y un modelo de gestión de riesgo operacional. Conforme los análisis descriptivos y comparativos realizados, se concluye que las entidades *Fintech*, deben desarrollen estrategias, programas y planes para mitigar posibles vulnerabilidades. Estos deben ser coherentes con los criterios de reducción del riesgo, con la participación de entidades regulares, una planificación financiera, y gobiernos locales, el sector empresarial y la sociedad.

(**Palabras clave**: estrategia integral, tecnología financiera, riesgo operacional, marco normativo internacional, mejores prácticas de supervisión bancaria)

Summary

The objective of the present thesis is to propose an integral strategy of operational risk management for the Financial Technology Institutions (Fintech) of Mexico, considering the technological, human, organizational and regulatory aspects; for the purpose of minimize the financial impact that these institutions and their clients may suffer, against threats to their operational systems. The reason because the present investigation is done, is because actually, the Fintech entities are technological innovations in the financial sector, gathers potential risks for the consumer sector, banks and banking systems, which can represent operational risks that have been used by the money laundry, informational steal and fraud. For these reasons, the role that plays the operational risk management inside an organization is of big importance to maintain the company utilities and gain trust to the costumers, face the loses that may happen; maintain and guarantee the growth; and preserve the continuity and life of the Fintech. Therefore, in the present work a qualitative type methodology was used, which consists in describing and interpreting the international regulatory framework of the Fintech institutions, with the final objective of performing a comparative study of the content of the current legal texts; describe the best practices at the international level in the area of regulation, supervision and management of operational risks in banking activities; contextualize the study case of the Attack on Banxico SPEI in 2018, focusing on the variables that originated the affectations to the banks and banking systems; and, developing a proposal for operational risk management for its application to Fintech institutions, which shows the relationships between the principles of corporate governance, risk-based supervision and an operational risk management model. According to the descriptive and comparative analyzes carried out, it is concluded that the Fintech entities must develop strategies, programs and plans to mitigate potential vulnerabilities. These must be consistent with the risk reduction criteria with the participation of regular entities, a financial planning and local governments, the business sector and society.

(**Key words**: integral strategy, financial technology, operational risk, international regulatory framework, best practices of supervision banking)

Dedicatorias

A mi esposo Anuar Jassen, quien ha sido mi ejemplo a seguir, por su incondicional apoyo y por ser un rayo de luz en momentos difíciles.

A mis papas Juan Servin y Petra Loyola, quienes formaron en mí pilares para mi educación, y quienes con su cariño y comprensión me han acompañado incondicionalmente en esta etapa de desarrollo personal y profesional.

A mis nuevos amigos y compañeros de maestría: Lina Marcela Rincón, Luz Juárez, Luz Marín, Claudia Xelja Rodríguez, Oscar Alonso Ordaz, Verónica Beltrán, Luis Miguel Cruz y Bruno de la Garza por su amistad y apoyo desinteresado.

Agradecimientos

Especialmente al Dr. Felipe A. Pérez Sosa, director de esta tesis, por su invaluable guía, soporte y discusión crítica fundamentales para la realización del presente trabajo.

Al Dr. Jesús Hurtado Maldonado Coordinador de la Maestría en Ciencias Económico Administrativas.

A la Dra. Josefina Morgan Beltrán Jefa de Investigación y Posgrado de la Facultad de Contaduría y Administración.

Al Mtro. Martín Vivanco Vargas Director de la Facultad de Contaduría y Administración de la Universidad Autónoma de Querétaro.

A mis profesores: Dra. Julia Hirsh, Dra. Denise Gómez, Dra. Alejandra Urbiola, Dra. Minerva Maldonado, Dra. Graciela Lara, Mtro. Roberto Alejandro García, Dr. Michael Demmler, Mtro. Ricardo Ortiz por sus invaluables enseñanzas.

A Vanessa Rodríguez y al personal administrativo de la Universidad Autónoma de Querétaro.

A la Universidad Autónoma de Querétaro por abrirme las puertas y financiar parte de mis estudios.

Al Consejo Nacional de Ciencia y Tecnología (CONACyT) por financiar mis estudios.

Al Lic. Luis Leyva Martínez, Director de Desarrollo Regulatorio de la CNBV, por dedicar su tiempo para transmitirme su conocimiento y experiencia laboral esenciales para el desarrollo de la presente tesis.

Índice

Índice de Tablas

Página

Índice de Figuras

Página

1. Introducción

1.1. Antecedentes

El año de 1970 marcó el inicio la era digital o era de la información, a partir de entonces, se produjo una adopción integral de computadoras digitales y el mantenimiento progresivo de registros digitales. En aquel tiempo, la era de la información comenzó a asociarse a innovaciones provenientes de la tecnología digital, como el teléfono celular, la infraestructura de redes de computadoras que soporta la transmisión de datos y servicios -como los mensajes de texto, el correo electrónico, entre otros- y especialmente el nacimiento del internet a una escala global, trayendo consigo un cambio de ideas en el uso de tecnología digital en la forma de producir bienes y servicios, cambio que impacto significativamente a la industria financiera (Rojas, 2016).

Sin embargo, no es nuevo que el uso de las innovaciones tecnológicas sean empleadas para la prestación de servicios financieros, por el contrario; este fenómeno, en un primer nivel, comenzó desde finales del siglo XIX, periodo en el que la industria bancaria comenzó a asociarse estrechamente a nuevas tecnologías (Avendaño, 2018). Y, alrededor de 1866, el uso de aparatos analógicos como el telégrafo, el cable transatlántico y después el fax, junto con el desarrollo de medios de transporte, propiciaron condiciones para el crecimiento del comercio mundial, trayendo consigo la globalización de las transacciones financieras, mismas que se situaron en el año de 1967, año en el que se introdujo el primer cajero automático en la ciudad de Londes. Es a partir de entonces que las instituciones tradicionales han aumentado el uso de las tecnologías de información (TI) en sus operaciones, y con ello han automatizado progresivamente sus procesos internos (Ontiveros, Martín, Navarro, y Rodríguez, 2012).

Posteriormente, la aparición de internet en 1991, sentó las bases para el siguiente nivel de desarrollo. A partir de 1995 se comenzó a utilizar el internet y el World Wide Web para

proporcionar cuentas en línea y facilitar el intercambio de información, y para 1994 se fundó la asociación de comercio electrónico Amazon, y un año después la compañía *eBay*. En 1998 se fundó la empresa *Confinity* que posteriormente se transformaría en *PayPal*, para atender las crecientes necesidades de servicios de pago por internet mediante tarjetas bancarias (Silva y Ramos, 2017). De modo que, para el 2005, los primeros bancos *en línea* sin sucursales físicas emergieron, por ejemplo, ING Direct, HSBC Direct, en el Reino Unido (Rojas, 2016).

Como señalan Arnes, Barberis & Buckley (2016), en ese entonces la expectativa era que los bancos continuaran proporcionando servicios financieros. No obstante, la economía de producción y distribución de servicios financieros, cambió con la tecnología digital, facilitando la caída de algunas de las barreras a la entrada en la industria bancaria, propiciada por el surgimiento de la red de distribución física, misma que fue derribada a través de la tecnología digital y teléfonos celulares, dado que estos hacen que sea muy barato comenzar a operar en línea, con costos muy bajos para la adquisición de los clientes y su distribución. Los sistemas y la infraestructura tecnológica como barrera también fueron derribadas con la captura, almacenamiento y procesamiento de datos, facilitando la expansión de la capacidad de los microordenadores, la computación en la nube y los teléfonos inteligentes (Dapp, 2014).

Una última etapa, se presentó particularmente después de la crisis financiera de 2008, que propició un entorno para la entrada de nuevos participantes la industria. Es ahí donde empresas no financieras, empresas de nueva creación (*startups*) y grandes empresas dirigidas a la tecnología y las telecomunicaciones, aprovecharon la oportunidad para entrar al sector financiero, en muchos casos fuera del sector de entidades reguladores y en países emergentes. Especialmente en este último, se ha reflejado un porcentaje de población, cada vez mayor, que tiene acceso a la telefonía

móvil y con tasas de bancarización bajas que han propiciado el surgimiento de entidades *Fintech* (Sánchez, 2016; Silva y Ramos, 2017).

No obstante, falta de regulación de esta industria, en los últimos años, obligó a los legisladores en México a presentar la nueva Ley *Fintech*, el 9 de marzo del 2018, que tiene por objeto regular los servicios financieros que prestan las instituciones de tecnología financiera, así como su organización, operación y funcionamiento. La ley está pensada con la finalidad de reglamentar la industria, proteger al consumidor, preservar la estabilidad financiera y prevenir factores de riesgo operacional (Ley de Instituciones de Tecnología Financiera, ITF, 2018).

1.2. Justificación de la Investigación

En México, la Ley *Fintech*, tiene por objetivo regular los servicios financieros que prestan las instituciones de tecnología financiera, así como su organización, operación y funcionamiento, por medio de inclusión e innovación financiera, la promoción de la competencia, preservación de la estabilidad financiera, protección al consumidor y prevención de operaciones ilícitas. Para el cumplimiento de estas últimas, la Ley *Fintech*, busca que las empresas divulguen la información que permita a sus clientes identificar los riesgos operacionales que presentan a través de ellas.

Entendiendo al riesgo operacional, como una pérdida procedente de fallas o ausencias de controles internos, por errores en el procesamiento y almacenamiento de las operaciones o en la transmisión de información, así como por fraudes o robos y engloba, entre otros, al riesgo tecnológico (ITF, 2018).

Actualmente, las entidades *Fintech*, al ser innovaciones tecnológicas en el sector financiero, engloban riesgos potenciales para el sector de consumo y para los bancos y sistemas bancarios. En este sentido, el Comité de Basilea (2018) señala que los riesgos mayormente identificados en el sector *Fintech*, son los riesgos operacionales que se presentan como oportunidades que el lavado

de dinero, robo de información y el fraude pueden hallar en los procesos no regularizados y gestionados de estas nuevas innovaciones.

Por esta razón, el papel que juega la administración de riesgos operacional dentro de cualquier organización es sustancial para mantener la utilidad de las compañías y brindar certeza a sus clientes, enfrentar las pérdidas que puedan tener; mantener y garantizar el crecimiento; y finalmente preservar la continuidad y vida de la empresa, en este caso, nos referimos a las instituciones de tecnología financiera *Fintech*.

1.3. Importancia

En los últimos meses México ha incrementado su participación en el sector financiero, precisamente para avanzar en el desarrollo de la innovación *Fintech* y situarse como uno de los potenciales a nivel mundial, según señala Finnovista (2018). Así mismo, apunta a que dicho sector incrementa su tamaño hasta alcanzar las 334 empresas de nueva creación para junio del 2018, esta cifra supone un aumento en número de empresas de nueva creación en el sector de 96 en los últimos 12 meses y con crecimiento anualizado del 40%. Así mismo, subraya que las innovaciones *Fintech* se ha convertido ya en un fenómeno global, puesto que se estima que para el sector bancario en México ya existe el riesgo potencial de perder 4.7 billones de dólares en ingresos frente a las empresas *Fintech.*

De igual forma, la Asociación Fintech México (2018) estima que el valor total de las transacciones en el sector para finales del 2018 será de $36,439 millones de dólares, con una trayectoria de crecimiento de más del 17.3% anual para llegar a $69,000 millones de dólares en el 2022. Así mismo, señala que el crecimiento esperado se debe al efecto positivo que la Ley para Regular las Instituciones de Tecnología Financiera (*Ley Fintech*) puede tener en el sector. En este

sentido Fintech México (2018) estima que dicha Ley traerá a más de $5 mil millones de pesos anuales en beneficio de familias y empresas, en ahorros e intereses por mayor competencia.

Por otra parte, el Comité de Estabilidad Financiera, *Financial Stability Board* (FSB, 2017) analiza los efectos del fenómeno *Fintech* sobre el sector financiero, en el que considera que si bien, dicho sector es un tema reciente, es necesario observar su evolución con el fin de identificar todas sus implicaciones. Por lo que señala dos áreas prioritarias que requieren una estrecha colaboración regulatoria y de gestión interna; la gestión de riesgos operacionales vinculados a la prestación de servicios por parte de terceros y la protección frente a ciberataques, que pueden derivar en un futuro incremento en el volumen de las actividades *Fintech*.

1.4. Objetivos de la Investigación

1.4.1. Objetivo general. Proponer una estrategia integral de gestión de riesgos operacionales para las Instituciones de Tecnología Financieras de México, que tenga en consideración los aspectos tecnológicos, humanos, organizacionales y normativos; a fin de disminuir el impacto financiero que puedan sufrir dichas instituciones y sus clientes, ante amenazas a sus sistemas operativos.

1.4.2. Objetivos específicos.

Objetivo particular 1. Describir los factores tecnológicos, humanos y organizacionales que rigen las normativas institucionales *Fintech* a nivel internacional.

Objetivo particular 2. Describir los mecanismos empleados en las mejores prácticas de regulación y supervisión bancaria, y la gestión de riesgos.

Objetivo particular 3. Contextualizar el caso real de una institución financiera con impactos financieros derivados de amenazas en su tecnología.

Objetivo particular 4. Elaborar una estrategia integral de administración de riesgos operacionales para empresas *Fintech* en México.

1.5. Preposición Central

El impacto financiero de los riesgos a los que son susceptibles las Instituciones de Tecnología Financiera, se pueden mitigar mediante una estrategia integral de administración de riesgos operacionales que considere los aspectos tecnológicos, humanos, organizacionales y normativos de estas instituciones.

2. Aspectos Teóricos

2.1. El Sector *Fintech*

2.1.1. Definición y características de las actividades *Fintech*. El término *Fintech* se remonta a principios de la década de 1990, en ese tiempo se refirió al *Consorcio de Tecnología de Servicios Financieros*, un proyecto iniciado por Citigroup, que tuvo como finalidad facilitar los esfuerzos de cooperación tecnológica (Barberis, Arner & Buckley, 2016). Sin embargo, en la actualidad, *Fintech* se utiliza para denominar aquellas empresas tecnológicas de nueva creación (*startups),* en materia de tecnología financiera que plantean competir en algún producto o servicio con la banca tradicional (Noya, 2016).

Etimológicamente, el término *Fintech* es la contracción de dos palabras inglesas: *financiero* y *tecnología,* que describe el uso de la tecnología virtual para ofrecer servicios financieros y productos a los consumidores en áreas de banca, seguros, inversión, y cualquier cosa que se relacione con las finanzas (Joyane, 2015; Fintech México, 2018). Económicamente, representa "un dominio de actividad que se caracteriza por la prestación de servicios financieros mediante infraestructuras basadas en tecnologías de información y comunicaciones por medio de plataformas virtuales" (Yáñez, 2018, p.4). Esta definición surge del cambio que la tecnología ha impuesto en la industria financiera, sin embargo, internet, combinado con el uso de dispositivos como teléfonos inteligentes y tabletas, denota que la velocidad de este cambio ha incrementado en los últimos años, y que a lo largo ha dado origen al término *Fintech* como se conoce hoy en día (Barberis, Arner & Buckley, 2016).

Schueffel (2017), señala que las empresas *Fintech* conforman una nueva industria dentro del sector financiero, que adopta tecnología que se apoya con el enriquecimiento de actividades

financieras. Por lo tanto, *Fintech* son las nuevas aplicaciones, procesos, productos o modelos comerciales en la industria de servicios financieros que se encuentran constituidos por uno o más servicios financieros complementarios y proporcionados, y conformados como un proceso global a través de internet (Sanicola, 2017).

En la actualidad, la generación de nuevos medios de financiación empresarial es originada por la incursión de plataformas tecnológicas financiera y de nuevos sistemas como formas de pago, por ello, las empresas *Fintech* se han constituido en colaboradores de pequeñas y medianas empresas, que a su vez ofrecen herramientas financieras innovadoras, y que utilizan la tecnologías para ofrecer a estas empresas servicios financieros más ágiles, eficientes y de bajos costos (Centro de Innovación BBVA, 2018).

No obstante, en México, al igual que en otros países, la regulación de las *Fintech* se ha desarrollado después de que este sector ha operado durante cierto tiempo, sin embargo, hoy en día existe un Ley que fue aprobada en marzo del 2018 por el Senado de la República. Se trata de una ley de orden público y observancia general que denomina a estas empresas como Instituciones de Tecnologías Financieras (ITF), y que tiene por objetivo regular los servicios financieros que prestan las instituciones de tecnología financiera, así como su organización, operación y funcionamiento, y los servicios financieros sujetos a una normatividad en particular que sean ofrecidos o realizados por medios innovadores. Éstas, deben contar con domicilio en México, tener gobierno corporativo, infraestructura y controles internos, oficinas, tener un capital mínimo necesario para llevar a cabo sus actividades, adecuados sistemas operativos, contables y de seguridad, además de que deben encontrarse al corriente en los pagos de sanciones impuestas (ITF, 2018).

Por otra parte, la característica principal que define a las empresas *Fintech* es que cada una se ha enfocado a un producto o servicio de la banca tradicional en específico, esto se debe a que las *Fintech* han sabido aprovechar las avances de la tecnología digital mejor que los bancos, al desarrollar productos con una mayor facilidad de uso, un menor costo, además de utilizar la optimización a través medios digitales (Noya, 2016).

De manera que, el término *Fintech*, en la práctica, está relacionado con un gran número de actividades que cubren una amplia gama de servicios financieros. El World Economic Forum (WEF, 2015) resalta aquellas que pueden servir para financiar a las pequeñas y medianas empresas. Éstos abarcan préstamos *peer to peer* (P2P), los cuales ofrecen gran potencial para mejorar el financiamiento de pequeños negocios, la gestión de recibos, como el *e-commerce*, servicios financieros de facturación, que representan una herramienta eficaz para superar la necesidad de generar liquidez y mejorar la situación del capital de trabajo de los pequeños negocios y, por último, las finanzas de proveedores en línea, la cual posibilita integrar las cadenas de suministros más profundamente.

Sin embargo, existen multitud de agrupaciones de características *Fintech* que varían en función del plano que se tome de referencia. Alt & Puschmann (2012) presentan una clasificación sobre innovaciones en tecnologías financieras asociadas con el sector de empresas *Fintech* que van en función de proveedores de servicios financieros, los cuales pueden ser establecidos en la industria bancaria u otros proveedores, y los procesos financieros desde la perspectiva del cliente, tales como, planificación y asesorías, pagos, inversiones, financiamiento, etc. No obstante, este sector se distingue de la banca tradicional, ya que, de manera general, presenta características que las diferencian.

Una de ellas, como menciona Igual (2016), se enfoca en la propuesta de algún aspecto concreto de finanzas, como préstamos, captación de recursos, medios de pago, análisis de datos, pagos, asesoramiento financiero automatizado mediante algoritmos, etc. En consecuencia, contrasta con los actuales y complejos servicios de los bancos que son multi-producto, y que ofrecen prestamos que muy comúnmente son difíciles de encontrar y ejecutar en sus sitios en línea, además de ser característicos por su complejidad, prestan problemas de transferencia y entendimiento (Silva y Ramos, 2017).

Otra característica se centra en el uso de nuevas tecnologías, en la que las empresas *Fintech* proponen soluciones a los problemas financieros de sus clientes o bien, a las necesidades que han sido mal atendidas por la banca. Es decir, utilizan plataformas que usan tecnologías innovadoras con aplicaciones fáciles de utilizar, y que son pensadas para un uso no experto, confiable y transparente (Igual, 2016). Esto hace que se refleje su flexibilidad, puesto que, a diferencia de los grandes bancos o instituciones financieras tradicionales, que como menciona Fiinlab, en Silva y Ramos (2017) "con frecuencia se ven limitadas por su estructura operativa, el costo del servicio y su dependencia en una infraestructura enorme, las empresas *Fintech* jóvenes tienen mucha más libertad de diseñar e innovar en la propuesta de sus servicios" (p.8). Por lo tanto, la interacción por parte de los usuarios tiene un componente de tranquilidad y de transparencia, y se centra en cubrir problemas de la menor forma posible (Igual, 2016).

Otro punto es que las empresas *Fintech* proceden de la cultura de la innovación y las *startups* que han sido creadas desde cero con la ideología de romper con las estructuras anteriores. Éstas relacionan y se desarrollan en un contexto de redes sociales, con la cultura de compartir entre iguales más que de seguimiento a un organismo como la que representan los bancos (*Financial Inclusion Innovation Laboratory*, Fiinlab, 2017). Las nuevas tendencias de economía colaborativa

se unen directamente con la filosofía de estas nuevas empresas, y por ello, se acoplan con el perfil de nuevos consumidores (Avendaño, 2018). Es por eso que, la propia opinión de los usuarios sobre este tipo de servicios y la experiencia de los clientes en su consumo se ha vuelto más apreciada, a diferencia de ser un cliente de un gran banco con una marca muy fuerte pero que genera poca confianza.

De esta forma, las empresas *Fintech* se plantean como una alternativa que es desafiante con respecto a la banca tradicional, puesto que su propuesta es combatida con respecto al producto bancario. Uno de los argumentos principales es que se presenta como una opción nueva, más eficiente y transparente, a diferencia de los productos ofrecidos por la banca, que tienen una reputación de caros y opacos (Schatán, 2017).

En el caso específico de México, para realizar operaciones sólo tienen autorización las instituciones de financiamiento colectivo, tales como: deuda, capital, copropiedad o regalías, y las instituciones de fondos de pago electrónico, tales como: emisión, comercialización y administración de instrumentos, prestación de servicios de transmisión de dinero, servicios relacionados con las redes de medios de disposición, otorgamiento de créditos y préstamos, etc., tal como lo establece la Ley ITF. Además, las autoridades del sistema financiero como el Banco de México (Banxico); la Secretaría de Hacienda y Crédito Público (SCHP); la Comisión Nacional Bancaria y de Valores (CNBV); la Comisión Nacional del Sistema de Ahorro para el Retiro (CONSAR); la Comisión Nacional de Seguros y Fianzas la (CNSF) y la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) tendrán la función de Comisión Supervisora, con la finalidad de tener un mayor control sobre estas empresas (Ley ITF, 2018).

2.1.2. Modelos de negocios de empresas *Fintech*. Existen múltiples modelos de negocios dentro del sector *Fintech,* cada uno ofrece productos y servicios distintos; no obstante, la mayoría se define como una *alternativa de la banca tradicional* que brinda servicios complementarios y que compiten con los que ofrecen las entidades financieras. Sin embargo, gran parte de estas empresas presta un servicio colaborativo, tanto con empresas del mismo sector *Fintech* o con entidades tradicionales, destacando la implementación de la tecnología en el mejoramiento, accesibilidad, agilidad y aumento de la capacidad de información del servicio ofrecido por ambas entidades (Holgado y Harizmendi, 2017). Bajo la perspectiva de diferentes alternativas de empresas *Fintech,* estas se clasifican en función del modelo de negocio que ejercen en su actividad (Figura 1).

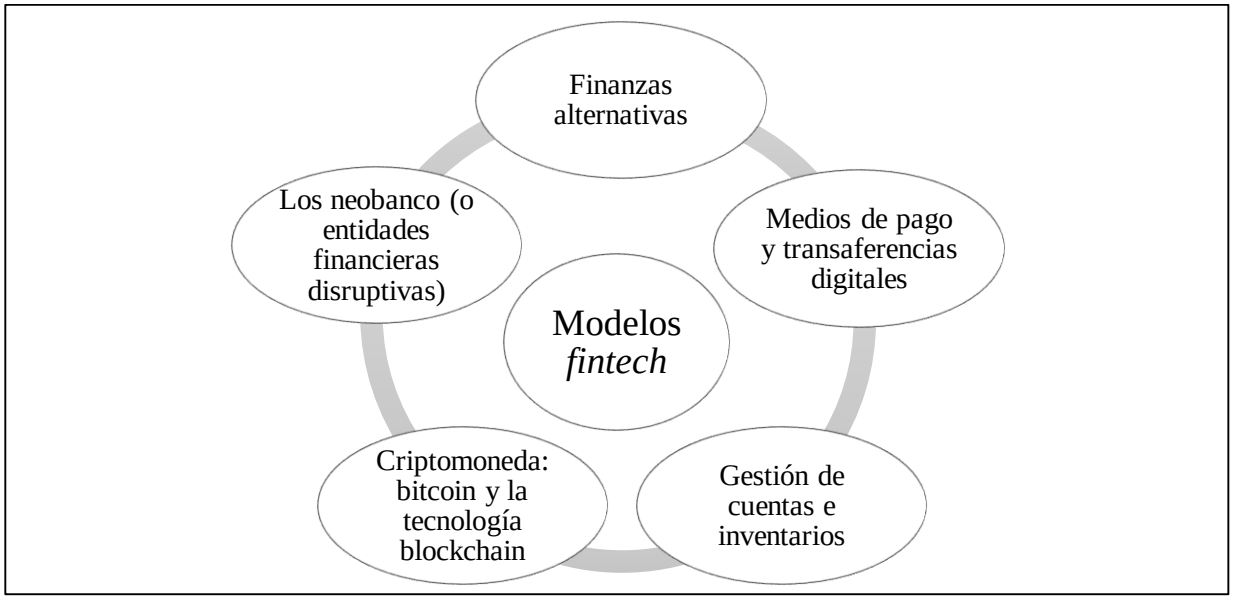

Figura 1. Modelos de negocio de empresas *Fintech*. Fuente: Elaboración propia con base en Finnovista (2017).

Financiación alternativa. Las *Fintech* de finanzas alternativas se basan en crear plataformas o mercados en los que las personas físicas y empresas, encuentran rentabilidad a la hora de invertir

en activos, éstos incluyen transacciones de deuda, capital y recompensas (Fiinlab, 2017). Un ejemplo de ello son las plataformas de *peer to business lending* (P2B), éstas ofrecen créditos de empresas que son financiadas mediante múltiples aportaciones de inversores; las plataformas P2P funcionan de forma parecida con créditos de particulares; las plataformas de *equity crowdfunding* permiten invertir en el capital de empresas y proyectos *startups* (Carrillo, 2007).

Medios de pago y transferencias digitales. Las *Fintech* que entran dentro de esta categoría tratan de ser más eficientes en costos y transparentes, cada uno dentro de su propio nicho. Estas van desde transferencias internacionales a pagos con tarjetas de crédito, que a su vez hacen más eficientes las transacciones en comercios electrónicos, o bien rebajan e introducen transparencia en los costos de cambio de divisas (Gai, 2016). Algunos ejemplos pueden ser plataformas de pagos, comercio electrónico y transferencias internacionales (Fintech México, 2018).

Gestión de cuentas e inventarios. Su objetivo es ayudar a las personas a tener un mayor control de sus finanzas personales, incluyendo crédito, ahorro, seguros (*Insurtech*), inversiones y derivados, así como plataformas de adecuación y cultura financiera (Kiviat, 2015). Adicionalmente, dentro de las innovaciones de los últimos años están entrando al mercado las llamadas *robo advisors*, éstos son asesores en línea que permiten gestionar carteras de activos con la mínima intervención humana, que a su vez, utilizan algoritmos basados en teorías modernas utilizadas por expertos en asesoría financiera (Prieto, 2005).

Criptomonedas: bitcoin y la tecnología blockchain. El *bitcoin* es una *criptomoneda* digital que funciona de forma descentralizada y P2P (Prieto, 2005). La innovación que ha creado el *bitcoin* se encuentra en su tecnología que hoy en día es conocida como *blockchain* (o cadena de bloques). Esta representa "aquella tecnología que permite intercambiar la moneda de forma descentralizada,

sin tener que depender de un emisor central ni tener que confiar en un intermediario para confirmar las transacciones" (Joyanes, 2003, p.34).

La tecnología *blockchain* hace los pagos en *bitcoin* muy similares a un pago en efectivo, puesto que se realiza directamente de una persona a otra, sin contar con los intermediarios que se necesitan en las transacciones, sino que se produce en tiempo real, como las transferencias bancarias o un pago con tarjeta de crédito (Prieto, 2005). La información es, por un lado, transparente, es decir, puede hacerse un seguimiento de cualquier transacción, así como saber a quién pertenece el dinero, en cualquier momento y desde cualquier procesador dentro de la red de *blockchain*.

Los neobanco o entidades financieras disruptivas. Representan aquellos bancos que se encuentran centradas en una banca exclusivamente por internet y que soluciona los problemas financieros día a día, debido a que se enfocan al mercando tanto digital como lo social (William, 2016). De la misma forma, los *neobancos* ofrecen tarjetas de débito, algunas posibilidades de ahorro y algunos productos más, pero su única diferencia es que son propuestas naturalmente digitales.

Por lo anterior, en el caso específico de México, la Ley ITF reconoce los avances tecnológicos que ocurren a una velocidad mucho mayor a la previsión de normas jurídicas, por lo que contempla la figura de Modelos de Negocio Novedosos, es decir, aquellas que para la prestación de servicios financieros utiliza herramientas o medios tecnológicos que aún no se han creado pero que se contemplan por el rápido avance de la tecnología. Así mismo, establece que éstas pueden contar con una autorización temporal, otorgada por la Comisión Supervisora competente de manera discrecional, con el propósito de probar sus modelos de negocio innovadores basados en actividades financieras actualmente reguladas por alguna ley del sistema financiero vigente (Ley ITF, 2018).

2.1.3. Segmentos de empresas Fintech en México. Los segmentos de empresas *Fintech* hacen referencia a grupos de empresas que son semejantes y numerosas, ya que se pueden reconocerse dentro de un mercado debido a que se comportan de manera similar (Chishti & Barberis, 2016). De acuerdo con Finnovista (2017), el 6 de agosto del 2017, en México existían 228 *startups Fintech* asignadas en 11 segmentos diferentes, esto muestra que en el transcurso de los últimos 10 años se identificaron 158 *startups*, que en la actualidad refleja la creación de aproximadamente 80 nuevas *startups* (Figura 2). Para junio del 2017 la distribución de empresas *Fintech* en México se explica en la Figura 3.

Figura 2. Ecosistema de empresas *Fintech* en México. Fuente: Finnovista (2017, párr. 3).

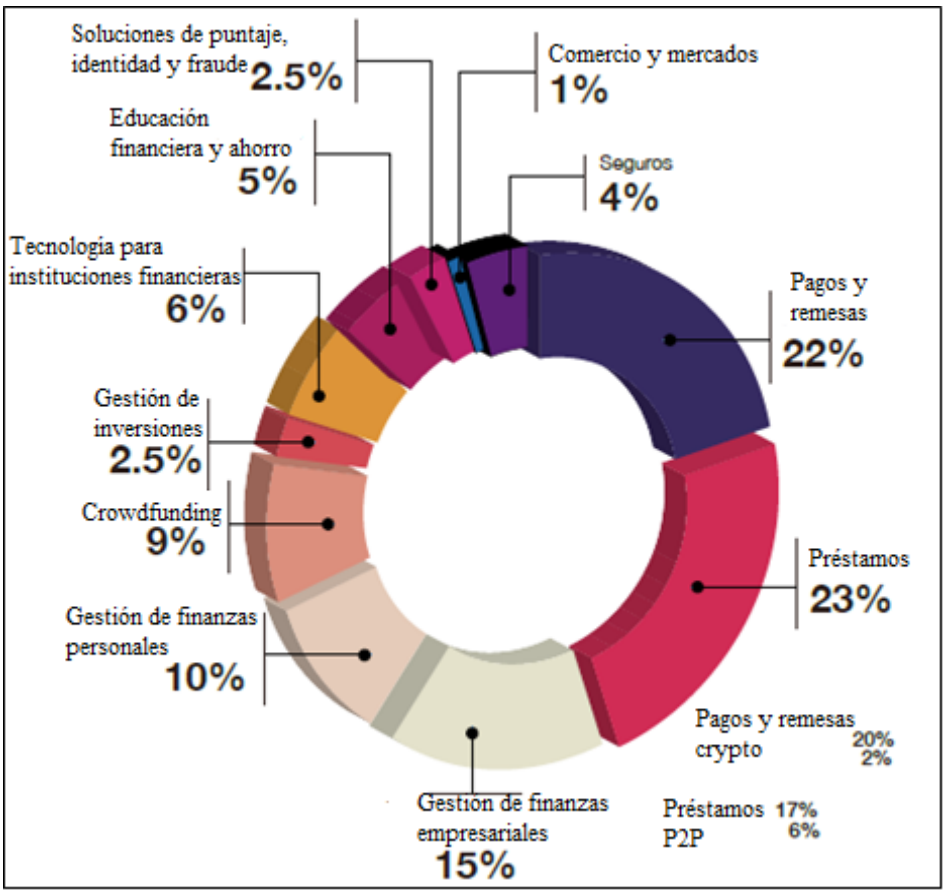

Figura 3. Distribución de segmentos *Fintech* en México. Fuente: Silva y Ramos (2017, p. 25).

Algunas de las características que hacen que México sea un país creciente en el sector de la industria Fintech, según el informe de Finnovista (2017), se debe a un incremento en el número de suscripciones de telefonía móvil y una alta penetración de internet, un comercio electronico fuerte, una baja penetracion en la bancarizacion, y poca refinancion en la oferta de créditos de consumo. En comparación con el año 2016, se destaca el crecimiento en los segmentos de: Préstamos, Finanzas Empresariales y Personales, y Educación Financiera y Ahorro, destacando la duplicación en tamaño del segmento de Seguros, como se observa en la Figura 4.

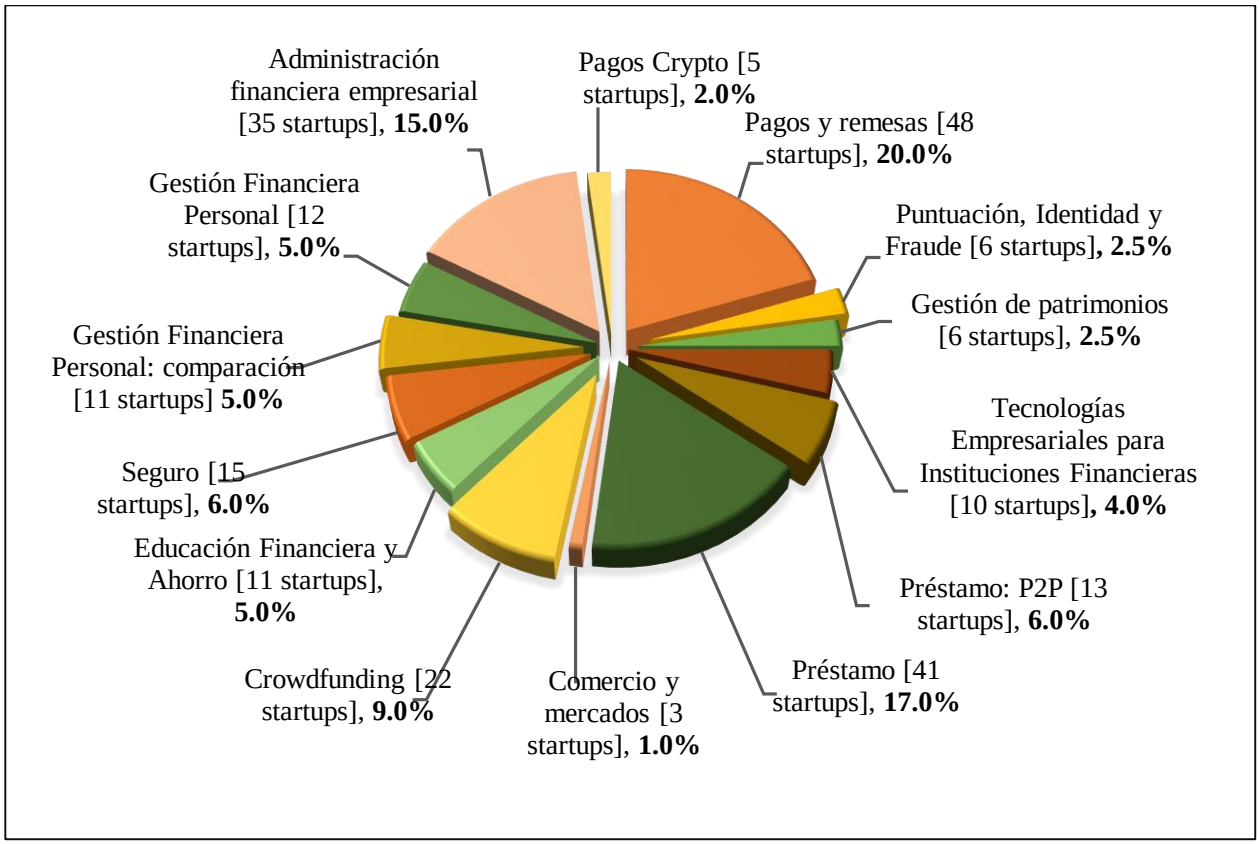

Figura 4. Penetración de empresas *Fintech* en México. Fuente: Elaboración propia con base en Finnovista (2017).

De acuerdo con Finnovista (2017), en México, el 46% del sector de empresas *Fintech* compite por el mercado que se caracteriza por la intersección de las innovaciones digitales en materia del sector *Fintech*, además de la necesidad de aumentar la amplia inclusión financiera del país. Por otra parte, el crecimiento por segmento para julio del 2017, comparado con agosto del 2016 ha mostrado un crecimiento considerable y volátil, y el cual se observa a continuación en la Figura 5.

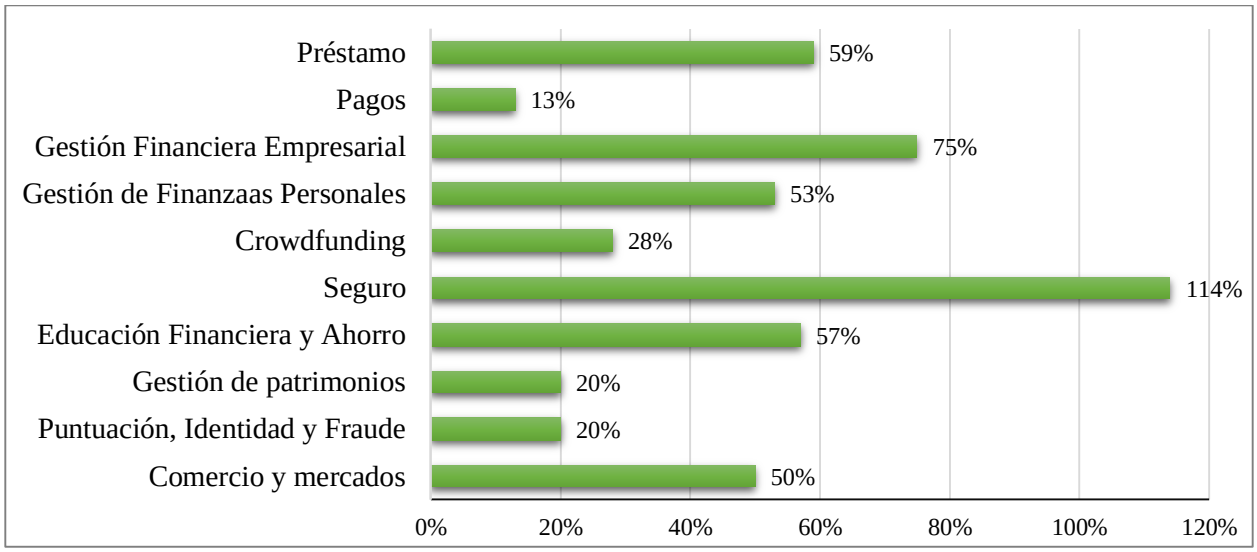

Figura 5. Crecimiento por segmentos *Fintech* en México. Fuente: Elaboración propia con base en Finnovista (2017).

Cabe destacar que ha habido un desarrollo en el segmento de préstamos con un aumento del 60% a julio del 2017, en comparación con el año anterior, seguido de segmento de pagos y remesas con un crecimiento del 13%, sin descontar el segmento de gestión de finanzas empresariales con un crecimiento de 75% y seguros con un 114% (Silva y Ramos, 2017). No obstante, la principal barrera que se enfrenta México en el uso de servicios *Fintech* es la falta de conocimiento de su existencia con un 23%, seguido por la preferencia de utilizar un proveedor de servicios financieros tradicional con un 7%, y el no haber tenido la necesidad de utilizarlos, también con un 7% (Figura 6) (Lozano y Moreno 2016). Así mismo, Finnovista (2017) realizó una encuesta a más de 100 *startups Fintech* en México que proporciono información que muestra que México es la ciudad donde la mayoría de las *startups Fintech* mexicanas han sido constituidas, siendo la ciudad de origen del 71% de ellas, seguido por Monterrey con el 11% y Guadalajara con el 10%, como se muestra en la Figura 7.

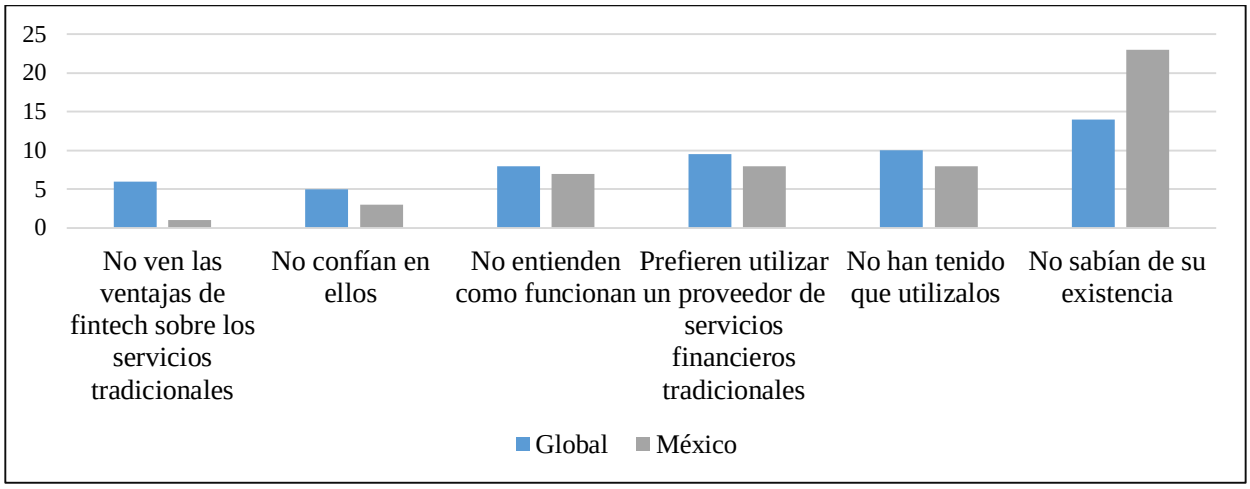

Figura 6. Barreras de adopción *Fintech*. Fuente: Elaboración propia con base en Lozano y Moreno (2016).

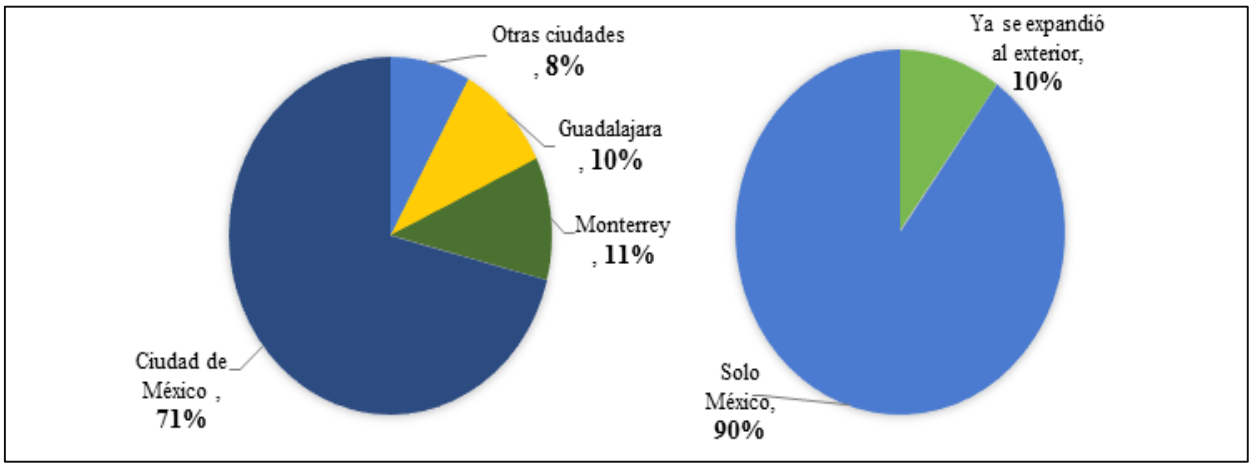

Figura 7. Comparación *Fintech*: México e Internacionalización. Fuente: Elaboración propia con datos de Finnovista (2017).

En materia de internacionalización, el 90% de las *startups* afirma que operan sólo en México, y sólo el 10% de ellas ya opera fuera del país. Sin embargo, en materia de madurez, alrededor del 39% de las empresas *Fintech* de nueva creación afirman estar listas para escalar, mientras que el 22% se describen en etapa de Crecimiento y Expansión, quedando en las etapas iniciales el 39% de las *Fintech* de México de nueva creación (Finnovista, 2017).

2.1.4. Herramientas digitales de las empresas *Fintech*. La *tecnología blockchain* (o cadena de bloque, en su traducción más cercana al español) y, en términos más amplios la *tecnología de contabilidad distribuida* (DLT, por sus siglas en inglés: *distributed ledger technology*) representen una de las innovaciones más importantes dentro del sector de empresas *Fintech*, que se implementa para actualizar el sistema financiero y la banca central (Smets, 2016). La Figura 8 es una representación de su funcionamiento, que, básicamente es una base de datos compartida que se sincroniza en una red que se distribuye en múltiples sitios, y que permite ser actualizada y manejada por una red de usuarios (Seibold & Samman, 2016).

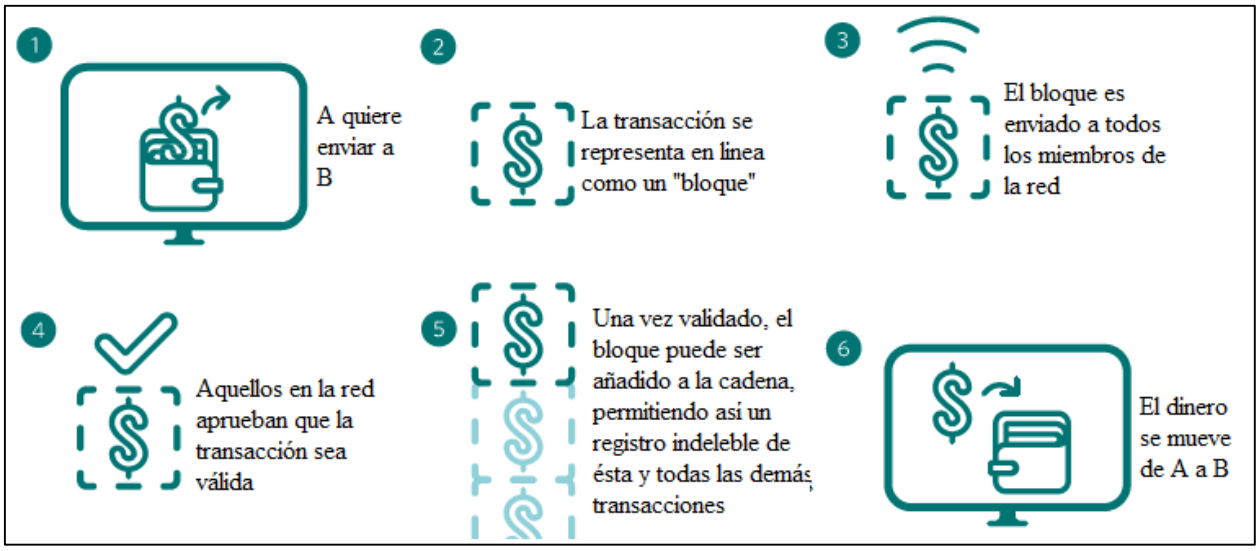

Figura 8. Tecnología *blockchain*: herramienta digital *Fintech*. Fuente: Fiinlab (2017, p. 20).

Furche et al. (2017), sostienen que, para el funcionamiento de esta herramienta debe de haber un participante en cada computadora de la red, dicho participante puede acceder a los registros que se comparten en esa red y puede emplear una copia idéntica de ellos, por lo que cualquier cambio o complemento al sistema de contabilidad se refleja y copia en los registros de todos los participantes en cuestión de segundos o minutos.

La cadena de bloques es un tipo específico de contabilidad distribuida utilizada con las *Fintech*, porque incluye la historia encriptada de todas las transacciones (bloques) pasadas en cada registro actualizado (Furche et al., 2017). Fiinlab (2017) menciona que la importancia de la cadena de bloques en el sistema financiero de empresas *Fintech* se debe a que permite que consumidores y proveedores se conecten directamente sin la necesidad de un intermediario.

Furche et al. (2017) por su parte, señalan que la contabilidad distribuida y la cadena de bloques y pueden ser *privadas, públicas* o *híbridas*. Las privadas son aquellas en las que sólo unos pocos usuarios son administradores y cuentan con los derechos para actualizar las bases de datos; mientras que las públicas, son en las que todos los usuarios son administradores y cualquiera de ellos puede actualizar el registro; y las híbridas son aquellas en las que los usuarios tienen diferentes niveles de acceso, algunos tienen privilegios para actualizar y leer algunos archivos, pero otros no. Sin embargo, algunos de los estudios, como los de Berndsen, (2016) y Malinova y Park (2016), muestran que una infraestructura de contabilidad distribuida con capacidad de acceso, y usuarios con identidades reales, puede llegar a ser más eficiente en aspectos como: la competencia de mercado, los costos para el control de la red, mejor información y cumplimiento con las disposiciones para la prevención del lavado de dinero y para el conocimiento de los clientes.

El funcionamiento de la tecnología de contabilidad distribuida y de cadenas de bloques consiste en mantener en un sólo registro todas las transacciones, así como los títulos de los activos que se encuentran dentro de la red, que, a su vez, son monitoreados por todos aquellos agentes que la conforman, por lo que no es posible engañar a sus miembros con una doble transacción, ni mucho menos realizar una estafa que comprometa al activo. Esto conlleva a que la tecnología de contabilidad distribuida pueda ser utilizada para crear cualquier tipo de contrato financiero, activo

o monea digital, ya que dichos activos en la red pueden ganar la confianza de los miembros dentro de la red (Berndsen, 2016).

Algunos de los beneficios de la contabilidad distribuida son los que incluyen procesamientos de información más rápidos y confiables, bajos costos de operación, así como una mayor capacidad de resistencia frente a fallos en su sistema (Cuesta, Ruesta, Tuesta, y Urbiola, 2015). La tecnología de contabilidad distribuida puede tener distintas aplicaciones en los distintos rubros de empresas *Fintech*, como las que operan con la tecnología de cadena de bloques, lo hacen con el modelo de divisas digitales, siendo el *Bitcoin* la más utilizada hasta el momento, además de que la cadena de bloques puede funcionar para casi todo tipo de transacciones de valor, como dinero, propiedades y otros bienes (Fiinlab, 2017).

Fiinlab (2017) menciona que la mayoría de los modelos de empresas *Fintech* serán construidos por la inteligencia artificial debido al cambio tecnológico en el que se encuentra inmerso, puesto que con la integración de la cadena de bloques y su importancia en el sistema financiero se debe a que permite que consumidores y proveedores se conecten directamente sin la necesidad de un intermediario, y si se adoptara de manera global, representaría la culminación del sector *Fintech.*

2.2. La Administración de Riesgos Financieros en Empresas *Fintech*

2.2.1. Administración de riesgos. La palabra *riesgo* tiene varios significados, el diccionario de la Real Academia Española (RAE, 2017) afirma que es “una contingencia o posibilidad que suceda un daño, desgracia o contratiempo” (párr.1). Sin embargo, aun cuando en el lenguaje moderno el término riesgo ha llegado a significar posibilidad de pérdida, la teoría financiera lo define como “la dispersión de resultados financieros o flujos de efectivo, que son inesperados debido a movimientos en las variables financieras” (Morales, Morales, y Alcocer, 2014, p.264).

Gitman (2007) se refiere a este término como "la posibilidad de pérdida financiera, o en sentido más definido, el grado de variación de los rendimientos relacionados con el activo específico" (p.196). Así mismo, el riesgo está relacionado con "la posibilidad de que ocurra un evento que se traduzca en pérdidas para los participantes en los mercados financieros, como pueden ser inversionistas, deudores o entidades financieras" (Banco de México, Banxico, 2005). No obstante, el riesgo es una parte necesaria dentro de los procesos de toma de decisiones en general, así como de los procesos de inversión en particular, puesto que el beneficio que se pueda obtener por cualquier decisión o acción que se realiza, debe asociarse necesariamente con el riesgo relacionado a dicha decisión o acción (Holgado y Harizmendi, 2017).

Morales et al. (2014) sostienen que el objeto de la administración de riesgos es asegurar que una inversión no sufra pérdidas económicas inaceptables, además de mejor el desempeño financiero de dicho entorno económico, tomando en cuenta el rendimiento ajustado para el riesgo. Esto se logra cuando se entienden los riesgos que toma un organismo, ya sea midiéndolos, estableciendo controles y/o comunicando dichos riesgos a los organismos correspondientes. En contraste, las instituciones financieras toman riesgos naturalmente, y bajo ese contexto, asumen riesgos más conscientemente anticipándose a los cambios negativos, protegiéndose de eventos inesperados y logrando obtener experiencia en el uso y manejo de riesgos.

Gitman (2017) menciona que para caracterizar completamente el riesgo es necesario considerar todos los escenarios futuros, asignándoles una probabilidad y determinando los posibles resultados económicos que se derivan de los mismos. En consecuencia, se han desarrollado grupos de metodologías que de forma general abarcan el análisis de escenarios y técnicas de probabilidad. El análisis de escenarios consiste en seleccionar unas pocas situaciones que se consideran desfavorables (como las entradas y salidas de efectivo, y el costo de capital) y, posteriormente

estimar las pérdidas asociadas, en general, sin tener en cuenta la probabilidad de ocurrencia (Gitman, 2007).

Van Horne y Wachowicz (2010) destacan que las metodologías que se emplean en la medición del riesgo se basan en técnicas de probabilidad, que han ayudado a construir tablas en las que se recoge el costo de cada una de las posibles pérdidas, junto con la probabilidad de que se alcance dicho nivel, a través de técnicas de distribución de probabilidad en términos de rendimientos esperados y desviaciones estándar.

Sin embargo, recientemente una de las metodologías más empleadas es la que se conoce como Valor en Riesgo (VaR por sus siglas en ingles *Value at Risk*), misma que fue promovida y difundida por JP Morgan en 1994, y que es una medida estadística de riesgo que estima la pérdida máxima que podía registrar un portafolio, en un intervalo de tiempo y con cierto nivel de probabilidad o confianza (Lara, 2008). En términos estadísticos, corresponde al cuartil asociado al nivel de confianza que se fija para una distribución de probabilidades de pérdidas y ganancias que pueden tener los activos en conjunto y en un periodo de tiempo dado, tal como se muestra en la Figura 9 (Banxico, 2005).

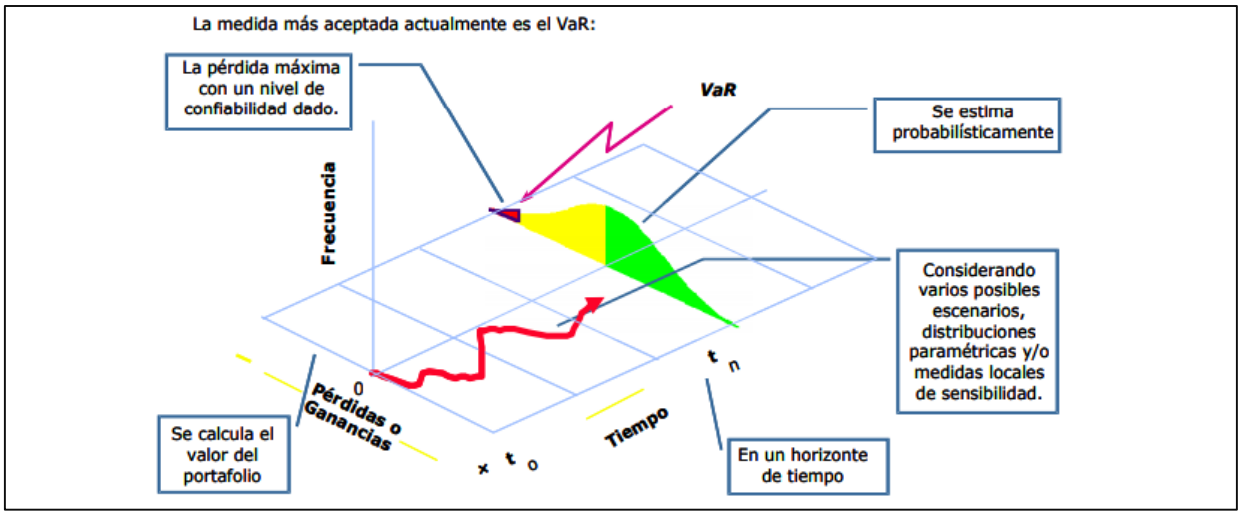

Figura 9. Valor en Riesgo (VaR). Fuente: Banxico (2005, p. 4).

En una empresa o en una institución financiera los miembros del consejo de administración son quienes deben definir dos los fundamentales para el cálculo de VaR, como el nivel de confianza que desean tener para determinado VaR y el horizonte de tiempo que se va a medir. No obstante, el JP Morgan recomienda un 95% de confianza de probabilidad que cubra un horizonte de un día para operaciones en mercados líquidos (Lara, 2008). Y, a pesar de ser un concepto meramente estadístico, el VaR es más común expresarlo en términos o unidades monetarias (Benavides, 2007).

Recientemente, la preocupación por la gestión de riesgos ha incrementado, principalmente por la necesidad de tener un marco de referencia sólido, que contribuya con la identificación, evaluación y gestión de los riesgos en las empresas de forma efectiva. Por ello, en el 2009, la Organización Internacional de Normalización (ISO) crea la norma ISO 3100:2009 para Gestión de Riesgos, Principios y Directrices, destinada a ayudar a cualquier organización a gestionar los eventos riesgosos, así como, proporcionar una estrategia para el control de riesgos y la creación de una organización más flexible. Su marco de trabajo busca, básicamente, estructura las actividades para la implementación y mejora continua del proceso de gestión de riesgos (Casares y Lizarzaburu, 2016).

Por lo anterior, el análisis de la investigación se basa en estructurar todas las actividades, con el propósito implementar y mejorar continuamente el proceso de gestión de riesgos, por lo que integra el compromiso de la dirección para la existencia de un compromiso más firme y mantenido por parte de la dirección de la organización; el diseño del modelo de la gestión de riesgo, con el fin de contextualizar a la organización y crear políticas de gestión de riesgos, y la rendición de cuentas y recursos que integran los procesos de la organización; el mejoramiento continuo del modelo en el establecimiento de una política y modelo de mejora continúa, incluyendo el plan de

tratamiento de riesgos; y la implementación del marco de Gestión de Riesgos e implementación del proceso de Gestión de Riesgos (Figura 10).

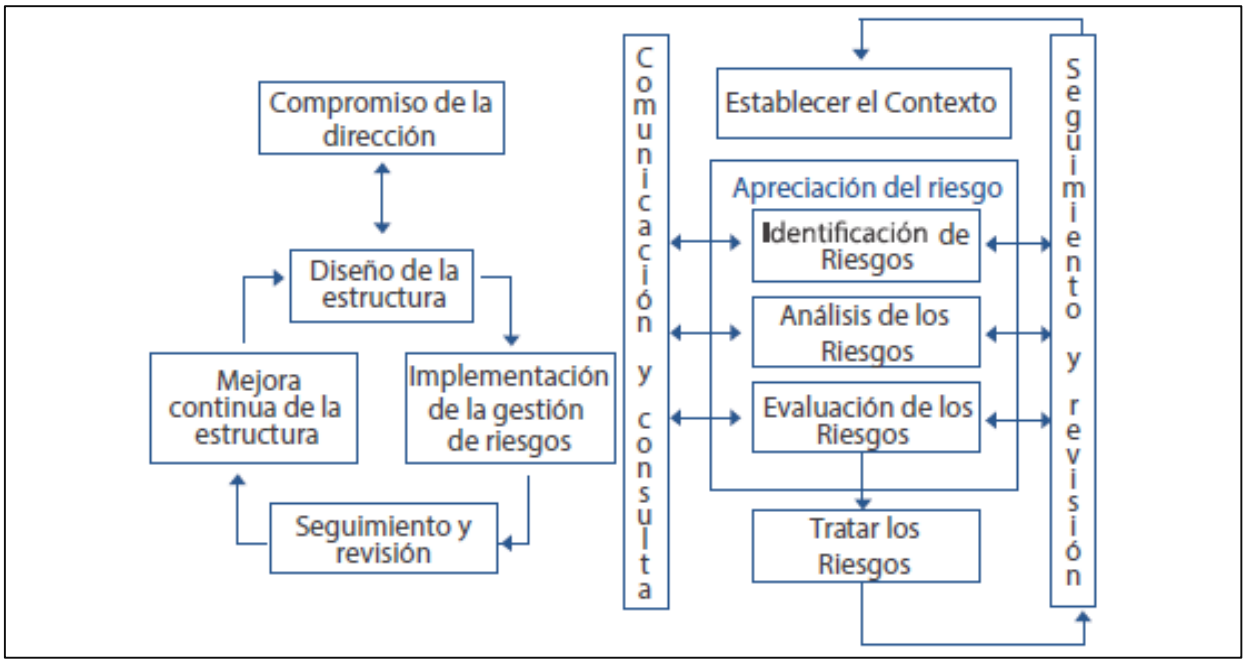

Figura 10. Principios y directrices de la gestión de riesgos. Fuente: Casares y Lizarzaburu (2016, p. 58).

El proceso de gestión del riesgo comprende cinco etapas para su aplicación, como la evaluación de riesgo que contempla la identificación, análisis y evaluación cualitativa y cuantitativa de los riesgos; el tratamiento del riesgo para la toma de decisiones; la comunicación y consulta; el monitoreo y revisión.

Así mismo, Casares y Lizarzaburu (2016) señalan que, además, contempla procesos de control extensos, con el objetivo de que dicha norma sea empleada como una guía de consulta y referencia para las empresas, así como por el comité de administración integral de riesgos y/o de la unidad de riesgos, con la finalidad de establecer el desarrollo de controles internos, considerando el marco legal existente, así como la situación actual de la empresa. Así mismo, busca establecer una

metodología con técnicas de control en las áreas de la empresa de forma práctico y proponer formatos, cuestionarios y calendarios de aplicación, a los responsables del control de riesgos de la empresa, con la finalidad de que se puedan aplicar a la actividad cotidiana.

2.2.2. Clasificación de riesgos financieros. El aspecto más importante del riesgo es el *riesgo general* de la empresa, según lo ven los inversionistas en el mercado, ya que el riesgo general afecta significativamente las operaciones de inversión y, de manera más importante, la riqueza de los propietarios. Dado que la única forma de evitar el riesgo es que no exista, la necesidad de administrar y gestionar es fundamental. Por lo tanto, en el área de finanzas se deben identificar todos los factores que pueden ocasionar la obtención de rendimientos distintos a los esperados, es decir, los factores de riesgo, donde cada factor distinto define en sí mismo (Gitman, 2007).

Existen diferentes naturalezas de riesgo, las cuales derivan del *riesgo financiero,* que hace referencia la incertidumbre que se asocia al rendimiento de la inversión o la variabilidad en cuanto a los beneficios que esperan obtener los accionistas, debido a la posibilidad que la empresa no pueda hacer frente a sus obligaciones financieras (Martinez, Medina, y Colmenares, s.f.). De acuerdo a los estándares regulatorios del sistema financiero mexicano establecidos en las *Disposiciones de carácter general aplicables a las instituciones de crédito*, también llamada *Circular Única de Bancos (CUB),* emitida por la CNBV se puede visualizar en el artículo 66 la clasificación de riesgos financieros, como se muestra en la Figura 11.

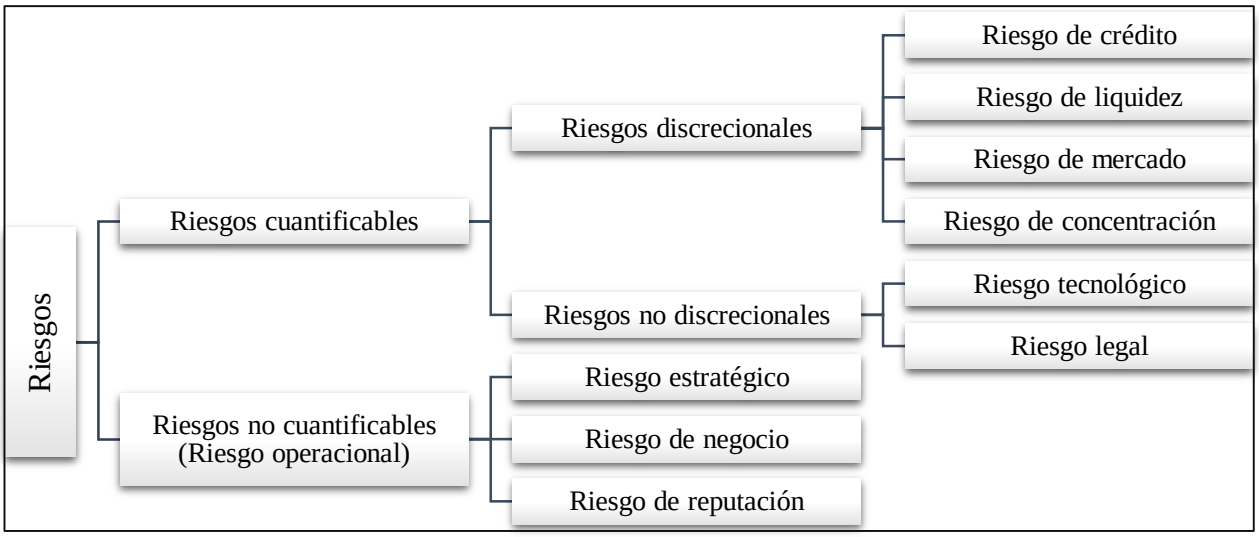

Figura 11. Clasificación de riesgos financieros por CNBV. Fuente: Elaboración propia con base en CNBV (2005).

Dentro de esta clasificación se establecen en su primer nivel *riesgos cuantificables* y *no cuantificables.* El primero, los *riesgos cuantificables* representan aquellos riesgos para los que es posible conformar bases estadísticas que permitan medir sus pérdidas potenciales, posteriormente, en su segundo nivel se encuentran los *riesgos discrecionales* que son los resultantes de una toma de posesión de riesgo, tales como; riesgo de crédito, liquidez, mercado y concentración. Cada uno se describe a continuación:

Riesgo de crédito. Es el más antiguo y probablemente el más importante que enfrentan los bancos, se puede definir como la pérdida potencial, producto del incumplimiento de la contraparte en una operación que incluye un compromiso de pago en alguna institución, es decir, si se debe al incumplimiento de los contratos por insolvencia (Lara, 2008). Estos pueden ser, garantías reales o personales que les sean otorgadas, así como cualquier otro mecanismo de mitigación utilizado por las instituciones CNBV (2005).

Riesgo de liquidez. La CNBV (2005) lo define como "la incapacidad para cumplir con las necesidades presentes y futuras de flujos de efectivo; la perdida potencial por la imposibilidad o

dificultad de renovar pasivos, así como, por el cambio en la estructura del balance general de la Institución" (p.262). Se refiere también a la imposibilidad de transmitir en efectivo un activo o portafolio, es decir, la imposibilidad de vender un activo en el mercado. Este riesgo se presenta en situaciones de crisis, cuando en los mercados hay únicamente vendedores (Lara, 2008).

Riesgo de mercado. Se entiende como aquella pérdida que puede sufrir un inversionista debido a las diferencias en los precios que se registran en el mercado o en movimientos de los llamados factores de riesgo, como las tasas de interés, tipos de cambio e índices de precios (Lara, 2008; CNBV, 2005). En palabras formales, este refleja la posibilidad de que el VaR de un portafolio se mueva contrariamente por cambios en las variables macroeconómicas que determinan el precio del instrumento que compone una cartera de valores (Soler et al., 1999).

Riesgo de concentración. Es un tipo de pérdida que se otorga por la creciente exposición a factores que ponen a alguna institución en riesgo, y que caen dentro de unas mismas o distintas categorías de riesgo (CNBV, 2005). El riesgo de concentración puede surgir en activos, pasivos o añadiduras fuera de la hoja de balance a través de la ejecución o el procesamiento de una transacción, como productos o servicios, o a través de una combinación de exposiciones en estas categorías grandes. El capacidad de pérdidas se refleja en el tamaño de la limitación y el alcance de la pérdida en caso de cierta circunstancia adversa (Comité de Supervisión Bancaria de Basilea, Basilea, 2011).

Por su parte, los riesgos *no discrecionales* o riesgos operacionales son los que surgen de la operación en marcha del negocio, sin tomar posición de asumir riesgos y comprende, entre otros, el riesgo tecnológico y legal CNBV (2005). Estos se describen a continuación:

Riesgo operativo. Se asocia con las fallas en los sistemas, procedimientos, en los modelos o en las personas que manejan dichos sistemas. También se relaciona con pérdidas por fraudes o por la

falta de capacitación de algún empleado en la organización (Lara, 2008). Así mismo, este tipo de riesgo se atribuye a pérdidas en que puede incurrir una empresa o institución por la eventual renuncia de algún empleo o funcionario, quien durante el periodo que laboró en dicha empresa concentró todo el conocimiento especializado en algún proceso clave. Es decir, si se debe a errores humanos o de los medios de producción o gestión (Soler et al., 1999). Otros aspectos del riesgo operacional incluyen caídas importantes de los sistemas tecnológicos de información o sucesos como incendios y otros desastres (Martinez et al., s.f.).

Riesgo tecnológico. Es la posibilidad de que se presenten efectos indeseables o inconvenientes acerca de un suceso que se relaciona con el acceso a la utilización de la tecnología y cuya aparición no se puede diagnosticar previamente (Tapia, 2014). En otras palabras, es la pérdida potencial por daños en los sistemas tecnológicos, tales como el hardware, software, aplicaciones, seguridad, recuperación de información y redes por errores de procesamiento u operativos, así como, fallas en procedimientos, capacidades inadecuadas e insuficiencias de los controles instalados, entre otros (Hidalgo, León, y Pavón, 2013; CNBV, 2005).

Riesgo legal. Se define como "la pérdida potencial por el incumplimiento de las disposiciones legales y administrativas aplicables, la emisión de resoluciones administrativas y judiciales desfavorables y la aplicación de sanciones, en relación con las operaciones que las instituciones llevan a cabo" (CNBV, 2005, p.263). O bien, si se debe la capacidad para ejercer para considerar los derechos que se consideraban como propios, o si se derivan del propio incumplimiento de la ley (Soler et al., 1999).

Por otro lado, los *riesgos no cuantificables,* son aquellos que se originan por eventos imprevistos para los cuales no se puede constituir una base estadística que permita medir sus

pérdidas, entre los que se encuentran; el riesgo estratégico, de negocio y de reputación CNBV (2005), tal como se describe a continuación:

Riesgo estratégico. esta enfocado a la mala toma de decisiones, puesto que genera fallas o deficiencias que provocan pérdidas potenciales a la hora de la implementación de procedimientos y acciones pertinentes a las estrategias del negocio, así mismo, al momento de perseguir el plan estratégico del negocio, se cae en el error de no tener en cuenta los riesgos a los que se puede exponer en el desarrollo de su actividad, que por ende, inciden en los resultados que la institución se plantea para el logro de sus objetivos (CNBV, 2005).

***Riesgo de negocio*.** Se refiere a una pérdida que se abribuye a características relacionadas al negocio y a los cambios en el ciclo económico o entorno en el que opera la institución (Van Horne y Wachowicz, 2010; CNBV, 2005). Por otra parte, Gitman (2007) destaca la posibilidad de que una empresa no sea capaz de cubrir sus costos operativos, puesto que tal nivel dependerá de la estabilidad de ingresos de la empresa y de la estructura de sus costos operativos, así mismo, señala que cuando mayor sea el riesgo de negocio de una empresa, mayor precaución debe tener ésta al establecer su estructura de capital.

Riesgo de reputación. Es el referente a las pérdidas que podrían resultar como consecuencia de no concentrar oportunidades de negocio atribuibles a un desprestigio de una institución por falta de capacitación de personal clave, fraude o errores en la ejecución operacional (Lara, 2008). Así como a la pérdida potencial por el deterioro tanto interno o externo en las instituciones, referentes a su solvencia y viabilidad y que se derivan por las partes interesadas (CNBV, 2005).

En contraste, los autores como Gitman (2007); Van Horne y Wachowicz (2010), reducen esta clasificacion a dos tipos básicos de riesgos, tales como, el *riesgo no diversificable* (o riesgo

sistemático) y el *riesgo diversificarble* (o riesgo no sistemático), dando como resultado el riesgo total de un portafolio.

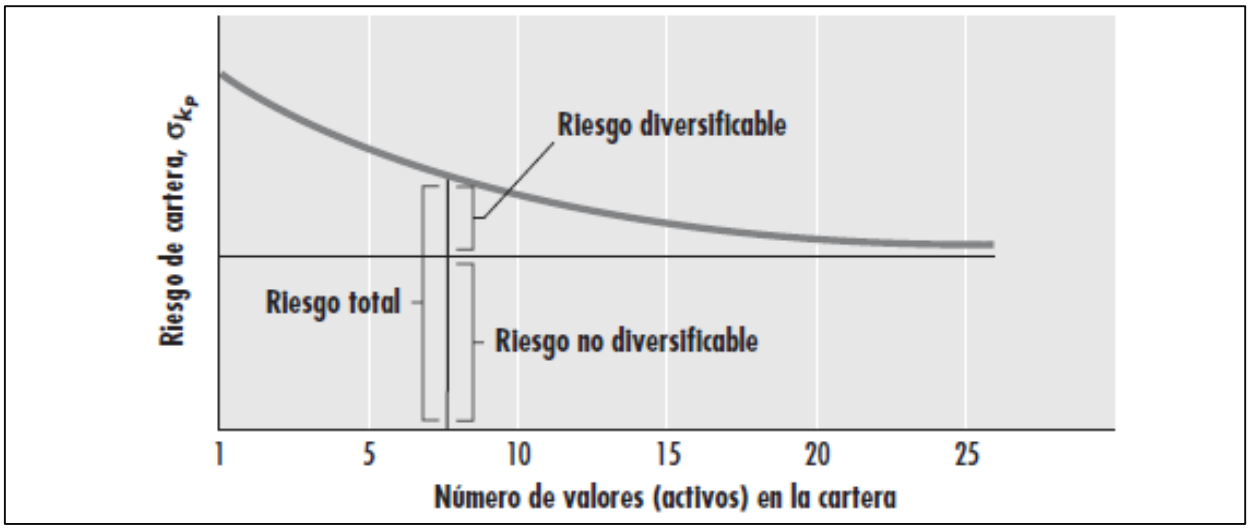

Figura 12. Riesgo de cartera y diversificación. Fuente: Gitman (2007, p. 212).

Para comprender los tipos básicos de riesgo es necesario describir al riesgo de un portafolio como su desviación estándar, como se observa en la Figura 12. Conforme aumenta el número de acciones del portafolio seleccionadas al azar, el riesgo total de éste se reduce, debido a los efectos de diversificación aproximándose a límites más bajos. De tal forma que, una proporción esencial del riesgo del portafolio se pueda eliminar con una cantidad parcialmente moderada de diversificación (Van Horne y Wachowicz, 2010).

La primera parte, el *riesgo no diversificable* se deriva de factores de mercado que afectan a todas las empresas, ya que no se puede eliminar a través de la diversificación. Se les atribuye a factores de riesgo que perjudican al mercado global, puesto que afectan los valores en su conjunto y son originandos por los cambios en la economía del país, las reformas a la ley fiscal del Congreso o cambios en la situación de la energía mundial, o bien, son resultados de factores como la guerra,

inflación, incidentes internacionales y acontecimientos políticos, etc. (Gitman, 2007; Van Horne y Wachowicz, 2010).

El segundo componente, el *riesgo diversificable*, representa "la porción del riesgo de un activo que se atribuye a causas fortuitas que pueden eliminarse a través de la diversificación" (Gitman, 2007, p.211). Es un riesgo único para una compañía o particularmente de una industria, puesto que es independiente de los factores económicos, políticos y otros que afectan a todos los valores de forma sistematizada (Van Horne y Wachowicz, 2010). En otras palabras, es causada por acontecimientos específicos de una empresa, como huelgas, demandas, acciones reguladoras y/o pérdida de una cuenta clave, fraudes o robos, etc. (Gitman, 2007).

Para la mayoría de las acciones, el riesgo no diversificable puede explicar aproximadamente el 50% de la desviación estándar. Sin embargo, en el riesgo diversificable, si la variación es eficiente, este tipo de riesgo puede reducirlo o eliminarlo. Esto se debe a que todo el riesgo participe en la posesión de una acción es relevante porque parte de este riesgo se puede diversificar a hacia otro lado, lo que importa en una acción es el riesgo no diversificable o inevitable, ya que los inversionistas pueden esperar ser compensados por correr este riesgo no diversificable, y, sin embargo, no necesariamente se debe esperar que el mercado brinde una compensación adicional por correr el riesgo evitable (Van Horne y Wachowicz, 2010).

2.2.3. Marco normativo de los riesgos cuantificables, no discrecionales. El marco normativo de las Instituciones de Tecnologia Financiera (ITF) señala que para que éstas sean autorizadas para realizar sus operaciones con activos virtuales y sujetas a moneda extranjera, deben apoyarse en las medidas y políticas en materia de control de riesgos operacionales, así como la seguridad de la información, con la evidencia de que cuentan con un soporte tecnológico seguro y preciso para sus

clientes, y de conformidad con lo establecido en las Disposicones de Carácter General (DOF) que emite la CNBV (Ley ITF, 2018).

Por ello, de acuerdo con la CNBV, los riesgos cuantificables no discrecionales son un tipo de riesgo operativo, que contempla a los riesgos tecnológicos y legales. Este es un concepto muy amplio puesto que agrupa una gran variedad de riesgos relacionados con diversos aspectos institucionales, tales como, deficiencias de control interno, procedimientos inadecuados, errores humanos y fraudes, fallos en los sistemas informáticos, etc. (Soler et al., 1999). Así mismo, Casares y Lizarzaburu (2016) señalan que lo importante para los bancos respecto del riesgo operacional es contar con un proceso de gestión de riesgos operativos o riesgos operacionales. Este proceso de análisis de riesgo operacional es el que va a garantizar al banco la buena administración de los riesgos en el marco de los estándares internacionales.

En este sentido, la CNBV (2005) fija las funciones mínimas a desarrollar respecto a la administración de riesgos operacionales, tecnológicos y legales que abarcan la identificación y documentación de procesos que describen las tareas a desarrollar por cada institución. A continuación, se describen las funciones de los riesgos mencionados anteriormente:

Riesgos operacionales. Las funciones a desarrollar para la administración de riesgos operacionales se centran en políticas de control interno encaminadas a optimizar el proceso de administración de riesgos, como son, la identificación de procesos institucionales y operacionales, que describen y tipifican el riesgo operacional y la línea de negocio, así como los procesos, el producto y su cuantificación, y los controles y panes de mitigación. De la misma forma, establece la evaluación y proporción de informes del perfil a la exposición al riesgo operacional, el establecimiento de niveles de tolerancia al riesgo, la implementación de políticas y procedimientos para los riesgos operacionales, la elaboración de la calificación de las unidades de negocio que

cuenten con criterios, políticas y metodologías y el mantenimiento de una base de datos histórica, así como el establecimiento de indicadores e informes de riesgo que incluyan inventarios de riesgos operacionales prioritarios y mapas de perfil de riesgos y su calificación.

Riesgos tecnológicos. En este apartado se fija la vigilancia permanente de aquellas circunstancias que pongan en materia de riesgos tecnológicos, a las operaciones ordinarias de la institución, tal como se resumen las funciones a desarrollar en la Figura 13.

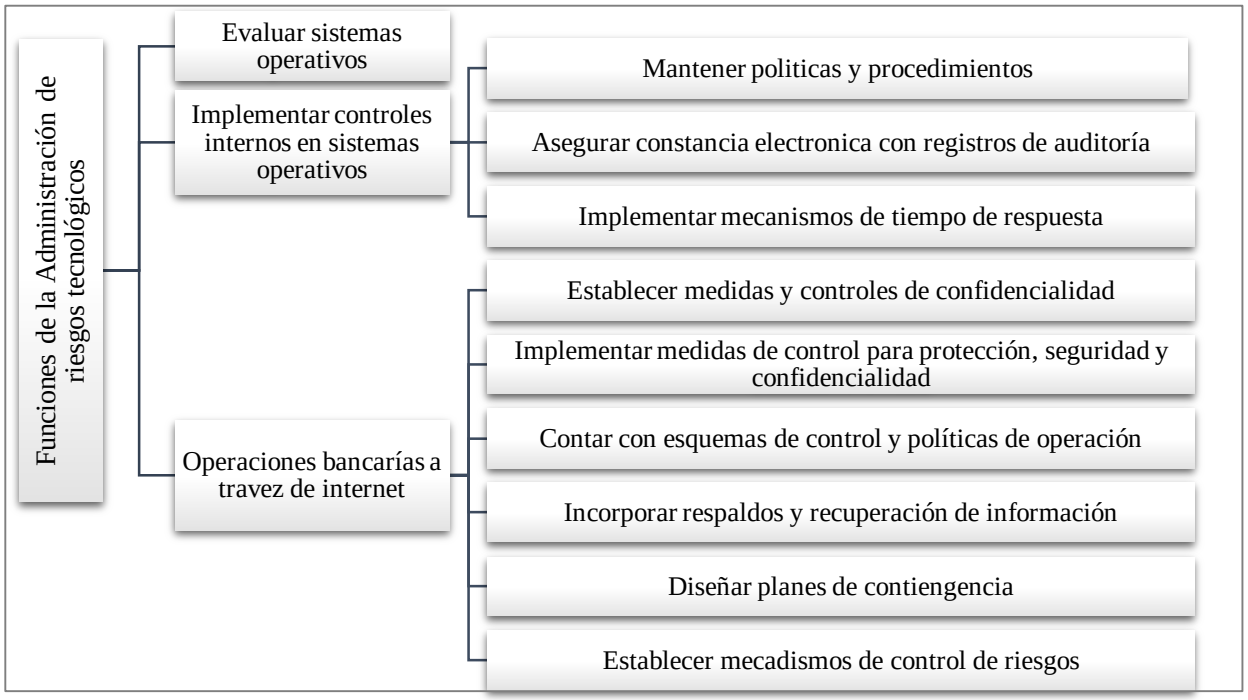

Figura 13. Funciones a desarrollar para la administración de riesgos tecnológicos. Fuente: Elaboración propia con base en CNBV (2005).

En primera instancia, establece la evaluación de vulnerabilidades y la implementación de controles internos presentes en hardware, software, sistemas, aplicaciones, seguridad, recuperación de información y redes, por errores de procesamiento u operativos, fallas en procedimientos, capacidades inadecuadas e insuficiencias de los controles instalados, entre otros. Así mismo, contempla cajeros automáticos, banca telefónica, sucursales, entre otros, para

mantener los canales de distribución para operaciones bancarias con los clientes realizados a través de internet CNBV (2005). No obstante, dependerá de las características de cada una de las instituciones, del tipo de tecnología que este empleando y de los procesos a los que ésta esté relacionada dentro de la operación en marcha del negocio (Soler et al., 1999).

Riesgo legal. Dentro de las funciones de la administración de riesgos legales se fija el establecimiento de políticas y procedimientos para una adecuada instrumentación legal, así como las estimaciones de pérdidas derivadas de resoluciones jurídicas, el análisis de actos que realiza la institución cuando se rijan por un sistema jurídico distinto al nacional. De la misma forma, establece que se debe proporcionar a directivos y empleados las disposiciones legales y administrativas, realizar auditorías legales internas y el mantenimiento de una base de datos histórica sobre las resoluciones jurídicas y administrativas (CNBV, 2005).

2.2.4. Riesgos financieros en empresas *Fintech.* Silva y Ramos (2017) sostienen que las empresas *Fintech* a través de los servicios financieros que ofrecen, pueden contribuir a promover la inclusión financiera en aquellos segmentos que no han sido atendidos por los organismos financieros tradicionales. No obstante, sostiene que son susceptibles porque pueden incurrir en riesgos que implican actividades financieras que propician "un apalancamiento excesivo de las empresas y los hogares, y que, por no ser parte de los acreedores del sistema financiero formal, esta situación no se refleje de manera adecuada en las estadísticas y calificaciones de crédito, lo que podría afectar a otros oferentes de crédito" (p.26).

Por otra parte, Holgado y Harizmendi (2017) mencionan que los riesgos financieros en entidades bancarias y empresas *Fintech* no se tienen en cuenta de la misma forma. En las empresas *Fintech*, los riesgos se centran principalmente en atender riesgos que suponen una amenaza aun mayor, en primer lugar, por la especialización por parte de estas empresas al ofrecer determinados

servicios financieros, y, en segundo lugar, a la inclusión de los avances tecnológicos. Es por esto que los riesgos no son los mismos para ambas entidades, sino que cada una se centra en los escenarios en los que se desarrolla el sector financiero, mitigando los riesgos a los que en mayor medida quedan expuestos.

De modo que, la *Financial Stability Board* (FSB, 2017), subraya la importancia de riesgos dentro del dominio de empresas *Fintech*, destaca los riesgos microfinancieros asociados con la dependencia de proveedores externos, otros asociados a la ciberseguridad y algunos otros macro-financieros. De forma más específica, el Comité de Supervisión Bancaria de Basilea (Basilea, 2018) señala que, los riesgos que se han asociado con la aparición de empresas *Fintech* incluyen el riesgo estratégico, riesgo operacional, riesgo cibernético y riesgo de cumplimiento. Además del aumento de empresas *Fintech*, como sostiene Basilea (2018) presenta una amplia variedad de riesgos que abarcan varios sectores y con frecuencia se mezclan ambos elementos de riesgo tanto táctico y estratégicos, y algunos de estos riesgos predominan en escenarios específicos, como se muestra a continuación:

Riesgo estratégico. Los riesgos en la obtención de mayor rentabilidad en los bancos individuales aumenta por la separación de los servicios bancarios a empresas *Fintech*, puesto que las instituciones financieras ya existentes pueden llegar a perder una parte sustancial de su aportación de mercado o ganancia, debido a que si los nuevos participantes son capaces de utilizar la innovación tecnológica de manera más eficiente y ofrecer servicios menos costosos, los clientes encontraran mejores expectativas (Basilea, 2018).

Riesgo operacional. Por una parte, se asocia con la entrada de las empresas *Fintech* a la industria bancaria, puesto que aumenta la complejidad del sistema e introduce nuevos participantes que pueden tener conocimientos y experiencia en la gestión de riesgos de Tecnologías de

Información (IT por sus siglas en inglés *Information Technology*). Por otra parte, el desarrollo de productos y servicios innovadores pueden aumentar la complejidad de la prestación de servicios financieros, por lo que es más difícil de gestionar y controlar el riesgo operacional, ya que, los sistemas IT heredados por el banco pueden no se suficientemente adaptables a las prácticas de implementación, tales como la gestión del cambio que pueden ser inadecuadas (Basilea, 2018).

Riesgo cibernético. Está ligado a pérdidas financieras, interrupción o daño en la reputación de una organización por fallas en sus tecnologías de información en red, en general, entre sea mayor el uso de tecnologías de información y las soluciones digitales, se amplía el rango y el número de puntos de acceso que los hackers cibernéticos podrían atacar (FSB, 2017). Adicionalmente, las nuevas tecnologías y modelos de negocio pueden aumentar el riesgo cibernético si los controles no mantienen el ritmo del cambio en el entorno (Basilea, 2018). Por su parte FSB (2017); Kopp, Kaffenberger y Wilson, (2017) señalan que quizás el mayor riesgo de las empresas *Fintech* es el nivel de ciberseguridad, ya que mientras más dependan los sistemas financieros de plataformas electrónicas y de registros digitales, más expuestos estarán a los ciberataques que pueden alterar el flujo de los fondos en la economía. Por ende, persuadir a los inversionistas comunes para que diversifiquen sus portafolios y adopten prácticas de inversión más seguras puede representar un gran desafío para las empresas *Fintech*. Además, existe la gran necesidad de que las empresas de *Fintech* y supervisores promuevan la necesidad de una gestión y control de los ciberataques eficaz (Basilea, 2018).

Riesgo de cumplimiento. Se centra en la privacidad de los datos, puesto que representa el riesgo de no cumplir con las normas de protección de datos, ya que puede aumentar con el desarrollo de *big data*, más *outsoursing*, debido a acuerdos con empresas *Fintech* y a la competencia asociada a la propiedad de la relación con el cliente (Basilea, 2018).

Adicionalmente Furche et al. (2017) señala que también es necesario considerar al riesgo derivado de las *divisas digitales*, indicando que a pesar de que éstas son seguras a la hora de realizar transacciones directas entre usuarios, existen fallas operacionales y de seguridad con terceros que actúan como intermediarios, además de que pueden facilitar la evasión de impuestos, los fraudes y transacciones ilegales.

Por lo anterior, FSB (2017) apunta a que hay beneficios claros provenientes de los desarrollos de las empresas *Fintech*, pero ésta nueva innovación no se puede justificar sin tener en cuenta la seguridad, solidez, y la protección del consumidor, sino que es tarea de los bancos y los supervisores del sector financiero, mantener el mismo nivel de gestión de riesgos, las normas de control y la protecciones a los nuevos canales y servicios de entrega emergentes que las instituciones financieras introducen a través de *Fintech*.

De acuerdo con la Ley ITF, en México estas instituciones estan obligadas, de conformidad con lo que establezcan las disposiciones de carácter general que emite la Secretaría de Hacienda y Crédito Público, con la previa opinión de la CNBV, a establecer una metodología, diseñada e implementada, que sirva para llevar a cabo la evaluación de los riesgos operactivos por los cuales pudieran ser utilizadas para realizar actos, omisiones u operaciones, de robo, sabotaje, ataques a las vías de comunicación, etc., derivados de los productos, servicios, prácticas o tecnologías con los que operen (Ley ITF, 2018).

Dentro de la administración de riesgos financieros, la ley les solicita un nivel de capitalización y montos máximos de operación, con la finalidad de que permita afrontar los riesgos relacionados a su actividad y escala partiendo de un índice de riesgo operacional (Ley ITF, 2018). Así mismo, fija mecanismos de transparencia, defensoría y protección de los clientes, básicamente, por medio de la CONDUSEF. Por lo que las empresas *Fintech* que operan activos virtuales, deben divulgar

los riesgos a los que están sujetos sus clientes en sus contratos y medios de publicación. Con lo que respecta, la CNBV tiene la autoridad para anular la licencia con forme a las cláusulas incluidas en la ley, dentro de los que destaca la incapacidad de mantener el capital mínimo que se requiere para poder operar, malas prácticas o incumplimiento de contrato, además de tener la facultad de multar por hacer caso omiso de las observaciones y la entrega de documentos, entre otros (Ley ITF, 2018).

2.3. Factores que Influyen en del Desarrollo de la Actividad *Fintech*

2.3.1. Estructura organizacional y área de riesgos. La organización, fundamentalmente nace por la necesidad humana de cooperar. En ella, los hombres reflejan la necesidad de cooperar por fines personales, por razones de sus limitaciones tanto físicas, como biológicas, psicológicas y sociales. Así mismo, en la mayor parte de los casos, esta cooperación puede presentarse de forma más productiva o menos costosa, si se dispone de una estructura organizacional (Casares y Lizarzaburu, 2016).

En efecto, para muchos, la estructura organizacional es considerada como un sistema formal de tareas y relaciones de autoridad, que controla cómo las personas coordinan sus acciones y utilizan los recursos para lograr las metas de la organización con la finalidad de que puedan controlar los medios que utilizan para motivar a las personas como medio para lograr sus objetivos (Gareth, 2008). No obstante, Lawrence y Lorsch (1967) y Scott (1981), señalan que, para cualquier organización, una estructura adecuada se puede considerar como aquella que facilita las respuestas eficientes a los problemas de coordinación y motivación, es decir, es una respuesta a contingencias, que pueden involucrar o surgir por un sinnúmero de razones, como lo pueden ser por motivos

ambientales, tecnológicas o humanas, además de que a medida que las organizaciones crecen y se diferencian, la estructura evoluciona de la misma manera.

En este mismo sentido, la estructura organizacional se puede administrar por medio de un proceso de diseño y cambio organizacional. Para ello, existen componentes clave en la definición de estructura organizacional. Por una parte, la estructura organizacional crea relaciones formales de subordinación, como el número de niveles en la jerarquía y el tramo de control de los gerentes y supervisores, funciones, decisiones y tareas específicas. Por otra parte, identifica el agrupamiento de individuos en departamentos y el de departamentos en la organización total. Por último, incluye el diseño de sistemas formales e informales que conecten y garanticen la comunicación, la coordinación y la integración de los esfuerzos entre departamentos (Child, 1984; Hodge, Anthony y Gales, 2003).

Sin embargo, para Fombrum (en Hall, 1996) la estructura se encuentra en surgimiento debido a que existe una aproximación de soluciones de aspecto tecnológico, intercambio político e interpretaciones sociales en las organizaciones y alrededor de ellas que dan como resultado medidas de estructuración. Por el lado contrario, Chiavenato (2007) considera que la estructura organizacional son elementos que se agrupan y se mantienen parcialmente estables relacionan con el tiempo y espacio dando como resultado una totalidad.

No obstante, la aportación más representativa sobre este tema, es proporcionada por Mintzberg (1995). Para él, la estructura de una organización son todas las formas de división de trabajo en su conjunto y su coordinación posterior. Así mismo, señala que la estructura organizacional es una estructura de roles relacionados entre sí, donde cada persona es la que asume un papel que se espera que cumpla con el mayor rendimiento posible. Por ello, introduce cinco partes fundamentales como elementos organizacionales, los cuales se muestran el la Figura 14.

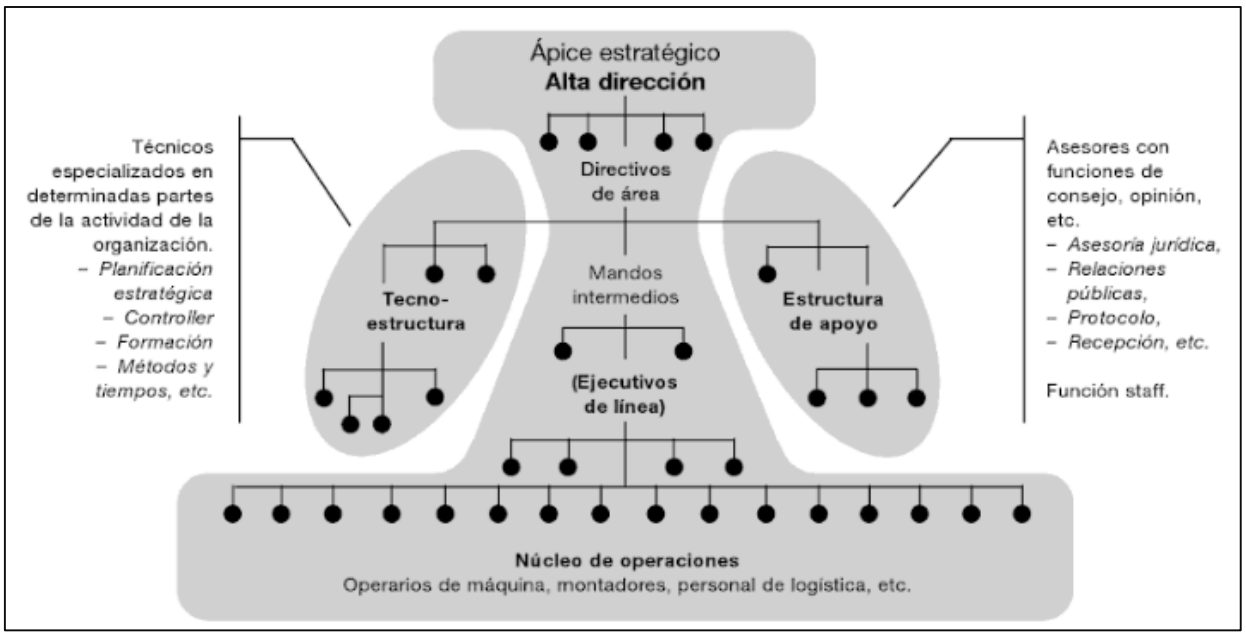

Figura 14. Partes fundamentales de la organización. Fuente: Mintzberg (1995, p.98).

La primera de ellas representa el *núcleo de operaciones*, ésta comprende lo que normalmente se denomina como mano de obra directa, es decir, quienes realizan el producto o servicio directamente con su esfuerzo físico, herramientas o máquinas. La segunda, se refiere a los *directivos medios*, quienes representan a las personas que tienen responsabilidad inmediata sobre el personal del área operacional. La tercera se refiere la *alta dirección*, quien es responsable de todas las personas con responsabilidad general en la organización, y comprende tanto al director general y su equipo de apoyo, comunmente es el que lleva a cabo el proceso de toma de desiciones. La cuarta representa la *tecnoestructura*, es el área que representan los analistas, especialistas o expertos en las distintas actividades funcionales. Por último, las *estructuras de apoyo*, quienes se ocupan básicamente de apoyar a los responsables en la jerarquía de la organización, mediante consejos, informes, opciones, etc.

En el mismo sentido Mintzberg (1995), citado en Padilla y Águila (2003), distingue agrupamientos funcionales para el diseño estructural, dentro de las cuales se identifican estrucuras

básicas, como la estructura funcional, comúnmente conocida por su forma U; la estructura divisional, por su forma en M, y la estructura matricial, que se distingue por agrupaciones con estructura vertical o en columna, y agrupaciones horizontales o en fila.

En este concepto también se pueden incluir componentes que delimitan la estructura organizacional. Reimann (1973) identifica tres componentes como el nivel de división de las actividades entre áreas funcionales (complejidad), el proceso de toma de decisiones (centralización), y el conjunto de normas, políticas y procedimientos que guían las actividades (formalización) de la organización.

Complejidad. El concepto de complejidad en la teoría de Hall (1996) y Robbins (2004), se entiende como las partes en que está dividida la organización, los problemas de control, la concentración de poder y de coordinación.

Formalización. Esta variable se entiende como el grado en el que los trabajos de una organización son estandarizados y el comportamiento de los empleados es intervenido por reglas y procedimientos, hasta llegar incluso a predecirlo (Hickson, 1966). Mintzberg (1995) reconoce que la formalización se puede definir de tres formas, según el puesto, el flujo de trabajo y las normas.

Centralización. Hace referencia a la distribución del poder al interior de las organizaciones. Usualmente se entiende como la concentración del poder para tomar decisiones. Robbins (2004), asegura que la centralización se refiere al grado en que la toma de decisiones está concentrada en un sólo punto en la organización. No obstante, Hall (1996) la define como “el nivel y variedad de participación en las decisiones estratégicas por grupos en relación con el número de grupos en la organización” (p. 65).

En el orden de ideas anteriores, Casares y Lizarzaburu (2016) señalan que las personas que desean cooperar entre sí en el interior de la organización, trabajarán más efectivamente si todos conocen el papel que deben de cumplir. Así, la estructura de una organización debe estar diseñada de tal manera que sea claro para todos quien debe realizar determinada tarea y quien es responsable por determinados resultados, puesto que de ésta forma se eliminan las dificultades que ocasionan vaguedades en la asignación de responsabilidades, y se logra un sistema de comunicación y de toma de decisiones que refleja y promueve los objetivos de la empresa.

Por otra parte, en la actualidad se plantean nuevas formas de estructuración organizacional que han evolucionado las jerarquías directivas y las estructuras divisionales que son reemplazadas por estructuras más flexibles, mismas que han sido denominadas como *formas organizativas complejas nuevas* (Padilla y Águila, 2003). De este modo, surgen aproximaciones o modelos que intentan recoger la idea de las nuevas formas organizativas. Como señalan Hodge et al. (1998) existen muchos autores que sugieren tendencias nuevas, referentes al diseño y que han llevado a sobreponer considerablemente los planteamientos de la mayoría de estos autores que utilizan términos distintos para describir una misma o similar forma organizativa.

Hodge et al. (1998) en el mismo orden de ideas, señalan que en años recientes, la tendencia del diseño más generalizado ha sido la estructura de red virtual, en la que la empresa funciona por medio de la subcontratación de la mayoría de las funciones o procesos principales a empresas por separado, y la coordinación de sus actividades desde pequeñas oficinas corporativas de la organización, es decir, en lugar de encontrarse bajo una estructura sólida o dentro de una organización, los servicios como contabilidad, diseño, marketing, finanzas, etc., se encargan a empresas por separado que están conectadas electrónicamente a una oficina central. En este sentido, Fernández (1994) señala que las estructuras de redes virtuales pueden ser redes temporales

de empresas independientes, como proveedores, clientes y competidores que se encuentran unidas por las Tecnologias de la Información y la Conumicación (TICs) para compartir capacidades, costos y acceso a un mercado nuevo.

En el contexto anterior, Levine, Lin, y Wang (2017) afirman que las nuevas formas de estructuración organizacional actualmente se centra en el empleo de medios electrónicos y las transformaciones digitales que han sido un factor determinante en la competitividad, especialmente del sector financiero y de los negocios que hacen uso de las nuevas tecnologías, como las empresas *Fintech,* quienes atribuyen a dichos cambios al incremento de la competencia y la eficiencia. No obstante, la evolución del uso de la tecnologia ha hecho el sector financiero sea incesante, puesto que gracias a ello continúan naciendo y desarrollándose compañias de base tecnologica que desarrollan su actividad en el mercado (Olivencia, 2007).

En este sentido, como menciona Foncillas (2017), se observan distintos tipos de adaptación al cambio digital en las organizaciones, donde la mayor parte de éstas instituciones de tecnología han desarrollado nuevos departamentos orientados a exponer una agenda o estructura de red virtual, mientras que otras instituciones han optado por impulsar estos cambios desde áreas funcionales ya existentes, como marketing, tecnología, etc.

Por tanto, se destaca que las transformaciones digitales y las innovaciones de este tipo de instituciones u organismos no pueden realizarse de forma aislada, sino que es necesario actuar de manera transversal, de forma que se pueda involucrar a toda la organización. La transversalidad, según Foncillas (2017), se consigue enfocando la totalidad del modelo de negocio de las instituciones hacia plataformas adaptadas a la era digital, centrándose en la automatización de procesos, modelos analíticos o el desarrollo de nuevas funcionalidades y áreas de negocio a través del canal de digitalización.

Guibert (2016) menciona que el ámbito bancario se encuentra ante un cambio indudable de modelo de negocio, donde se cuestiona la sostenibilidad del modelo de estructura tradicional, puesto que el desarrollo de la banca tradicional, el uso de monedas alternativas y criptomonedas, o los pagos y transferencias digitales, contribuyen a cambios estructurales sobre el tradicional modelo de negocio bancario. Asi mismo, menciona que varios autores entienden que lo más probable a mediano plazo, tanto los sujetos tradicionales, como bancos y los sistemas internacionales de pago con tarjeta y las instituciones *Fintech* colaborarán de forma conjunta.

Con respecto al área de riesgos en la empresa, Cañas (2009) citado en Casares y Lizarzaburu (2016), menciona que en la práctica, la gestión de riesgos implica cambios en la toma de decisiones presentes en el quehacer de la alta dirección, en la eliminación de paradigmas y posteriormente, en la creación de una cultura de gestión de riesgos, abarcando todos los niveles de la organización que inician en la alta dirección, hasta el último nivel de la organización, y en este sentido, también es indispensable establecer procesos formales. En consecuencia, es necesario señalar que diversas regulaciones internacionales muestran que el gobierno corporativo es un sinónimo de gestión de riesgos, en donde se establecen normas, políticas, procesos y procedimientos con la finalidad de destacar como una organización se puede dirigir, gestionar y controlar. Además, la estructura de un gobierno corporativo, especifica cómo se distribuyen los derechos y responsabilidades entre los distintos grupos de interés, así como proporciona las herramientas para el establecimiento de objetivos y el seguimiento del desempeño.

Por esta razón, y, para una adecuada gestión de riesgos, es necesario crear dentro de una organización un comité de administración integral de riesgos, que esté compuesto por un presidente, un responsable y un gerente de riesgos. El comité, necesariamente debe de contar con especialistas de cada uno de los riesgos, si es que existen, y cuyas funciones de manera general

sean, diseñar y proponer estrategias, políticas, procesos y de la administración integral de riesgos (Casares y Lizarzaburu, 2016).

2.3.2. El factor humano en la organización y la gestión de riesgos. Las organizaciones dependen del factor humano o de la persona para que las dirijan, controlen y para que operen y funcionen, de forma que toda la organización se constituye de ellos, pues de ellos depende su éxito y su permanencia. Por tal razón, el concepto de factor humano o de la persona como parte una organización, ha evolucionado tras diversas teorías o indagaciones a lo largo de los años. Entre las que más destacan, se encuentra la teoría de las relaciones humanas, la teoría de la jerarquía de las necesidades de Maslow, la teoría de la motivación-higiene de Herzberg y la teoría de la motivación de la experiencia establecida por Vroom, entre las principales (Romero y Alvarado, 2014).

De lo anterior, y de acuerdo con la contribución al enfoque humanista de Chiavenato (2007), la teoría de la administración de recursos humanos cambia en su concepto. Anteriormente, a las personas se les trataba como objetos, como recursos productivos semejantes a las máquinas o a las herramientas de trabajo y elementos pasivos que debían ser administrados, mientras que, recientemente, se procura por tratar a las personas como tales y no sólo como recursos organizacionales importantes. Cabe señalar que, entre las características de la teoría antes mencionadas, la organización es entendida como el conjunto de personas, enfocándose principalmente en las personas e inspirada en sistemas de la psicología, la delegación de autoridad, la autonomía del empleado, la confianza y apertura, así como enfatiza las relaciones entre las personas, la confianza y la dinámica grupal e interpersonal.

Por una parte, se observa la teoría de la jerarquía de las necesidades de Maslow, donde la principal aportación del psicólogo fue argumentar que las necesidades, una vez que han sido satisfechas, dejan de ser un motivador para el recurso humano, por lo que propuso una pirámide

en orden de importancia ascendente, jerarquizando, primeramente, las necesidades fisiológicas, y posteriormente, las necesidades de seguridad, de afiliación o aceptación, de estima y la necesidad de autorrealización. Esta propuesta, destaca los pasos que sigue la persona para cubrir su necesidad primordial que es la autorrealización, y señala que es complicado que una persona logre obtenerla sin antes tener cubiertas el resto de sus necesidades (Maslow, 1953).

Por su parte, Afful-Broni (2012) establece la teoría en el ambiente externo, la cual se basa en una modificación a la jerarquía de Maslow, quien apoya su teoría de la motivación en diferentes necesidades humanas. Ésta, en primer lugar, destaca los factores de mantenimiento, higiene o contexto del trabajo, destacando la política y la administración, la supervisión, las condiciones de trabajo, las relaciones interpersonales, el salario, el estatus, la seguridad en el empleo y la vida personal de la compañía. En un segundo lugar elabora un listado de satisfactores relacionados con el contenido del trabajo, que incluyen, el logro, el reconocimiento, el trabajo desafiante, el avance y el crecimiento en el trabajo.

Por su parte, Chiavenato (2007) sostiene que el concepto de motivación personal, conduce al clima organizacional, puesto que los seres humanos están continuamente implicados en la adaptación a situaciones que tienen como objetivo satisfacer sus necesidades y mantener su equilibrio emocional, ya que no sólo implica la satisfacción de necesidades fisiológicas y de seguridad, sino también, a la satisfacción de las necesidades de pertenecer a un grupo social. A esto se refieren Romero y Alvarado (2014) a que el clima organizacional está íntimamente relacionado con el grado de motivación de sus integrantes. Así, el clima organizacional es favorable cuando proporciona satisfacción de las necesidades personales de los integrantes y eleva su moral, de lo contrario proporciona frustraciones de esas necesidades.

Bajo el mismo orden de ideas, la gestión de riesgos se relaciona directamente con el factor humano, puesto que la norma ISO 31000 incluye este factor como un principio para una gestión eficaz del riesgo, ya que, permite identificar las aptitudes, percepciones y las intenciones de las personas externas e internas que pueden facilitar u obstruir el logro de los objetivos de la organización. En este sentido, el principio de gestión del riesgo considera los medios para obtener opiniones de las partes interesadas, y se entiende que dichas opiniones pueden estar influenciadas por las características humanas y culturales, al igual que factores que incluyen conceptos políticos y sociales, tal como los conceptos de tiempo (Casares y Lizarzaburu, 2016).

Así mismo, cuando se diseña el marco de referencia y cuando se aplican todos los aspectos del proceso de gestión del riesgo, son necesarias acciones específicas con el fin de comprender y aplicar dichos factores humanos y culturales, es decir, al asignar los objetivos se considera la capacidad y las objeciones que tienen los colaboradores, de tal forma que se maneje el riesgo de los factores humanos desde todos los niveles de la organización (Lizarzaburu, Barriga, Noriega, Lopéz y Mejía, 2017).

2.3.3. Capacidades tecnológicas. En la actualidad el ritmo rápido de la tecnología, la competencia y la globalización de los mercados ha creado un ambiente donde sólo las empresas que son capaces de emprender a un ritmo acelerado y continuo, logran mantenerse con éxito. En este mismo sentido, las transformaciones en las organizaciones impactan fuertemente el comportamiento de la demanda, en cómo se desarrollan los procesos de innovación y el uso efectivo de las tecnologías (Ngwenya-Scoburgh, 2009). Por ello, Fagerberg (2004) indica que hoy en día existe la aprobación sobre la importancia de la innovación cuando se crean *ventajas competitivas* en las empresas, puesto que las empresas que tienen éxito a la hora de innovar, pueden prosperan a expensas de sus competidores menos capaces.

En efecto, el desarrollo de ciertas capacidades de acceso a recursos es esencial para tener ventajas competitivas. Así mismo, la capacidad de una nación para fomentar y generar un cambio tecnológico es esencial para crear capacidades dentro de las empresas, así como para subsistir y crecer en el mercado internacional. Por lo que, el desarrollo de capacidades tecnológicas se debe a los resultados de las inversiones realizadas por las empresas, en respuesta a estímulos externos e internos, y la interacción con otros intermediarios económicos (Lall, 1992).

En relación con éste último, el concepto de capacidades tecnológicas fue definido a principios de los años ochenta en el trabajo de Kim y Dahlman (1992) como "aquella habilidad para hacer un uso efectivo del conocimiento tecnológico" (p. 85). De acuerdo con ellos, la capacidad tecnológica reside en el uso que se hace del conocimiento, es decir, en la capacidad para utilizarlo en la producción, inversión e innovación. Más tarde, organismos internacionales como la Organización para la Cooperación y el Desarrollo Económicos (OCDE) definen las capacidades tecnológicas como "los aprendizajes acumulados por las empresas, que les permiten mantener una dinámica innovadora y que teóricamente están estrechamente relacionadas con el desempeño organizacional" (De Olso, 2005, p.15). Así mismo, este concepto fue intercambiable con otros usados con la misma idea, tales como esfuerzo tecnológico (Lall, 1992; Bell, 1984), o habilidad tecnológica (Scot-Kemmis y Bell, 1986), hasta convertirse en un término ampliamente aceptado en la actualidad.

Por tanto, estas definiciones introducen a la idea de que las diferencias en el nivel de capacidades tecnológicas acumuladas se deben en mayor parte a los procesos de aprendizaje, que comprenden tanto procesos como resultados (Bell, 1984). Es decir, las empresas van aprendiendo a lo largo de tiempo, de tal forma que acumulan conocimiento tecnológico y sobre esa base, logran emprender actividades nuevas de forma gradual, de tal forma que pueden adquirir nuevas

capacidades (Hernández y Vera-Cruz, 2003). Por ende, el proceso de aprendizaje ocurre de forma multivariada, puesto que se ven influidas por diferentes factores asociados a cada empresa, como pueden ser, su origen en particular, las actividades organizacionales utilizadas en su gestión, las condiciones del sector en el que desarrollan sus actividades, la manera en la que interactúa con otras empresas, y a diferente nivel y rapidez en cada función (Lall, 1987; Bell y Pavitt, 1993; Kim, 1999).

Los procesos de aprendizaje permiten a las organizaciones acumular y extender sus capacidades tecnológicas centrales, en donde el aprendizaje representa la forma en que se obtiene los nuevos conocimientos, se acumula conocimiento previo y se crean condiciones para retroalimentar el proceso. El aprendizaje en el interior de las empresas, se genera en las actividades desarrolladas por la organización, como es el caso de la producción, investigación y desarrollo (I+D), el marketing, entre otros (Dutrénit, 2000).

En relación a lo último, Bell y Pavitt (1995) basados en el trabajo de Lall (1992) construyeron una clasificación de las principales capacidades tecnológicas a partir de cuatro funciones técnicas que van en relación a funciones básicas y de apoyo (Figura 15). Dentro de esta clasificación, las actividades básicas, representan actividades de inversión y de producción, la primera de ellas se refiere a la generación de cambio técnico y a la forma en la que se administra durante grandes proyectos de inversión; la segunda se refiere a la generación y administración de cambio técnico en los procesos, productos y en la organización. Por su parte, las actividades de apoyo derivan en las funciones de vinculación externa e interna y producción de bienes de capital que se consideran funciones de respaldo que pueden contribuir con la acumulación de capacidades utilizando el intercambio de información, tecnología y destrezas entre empresas.

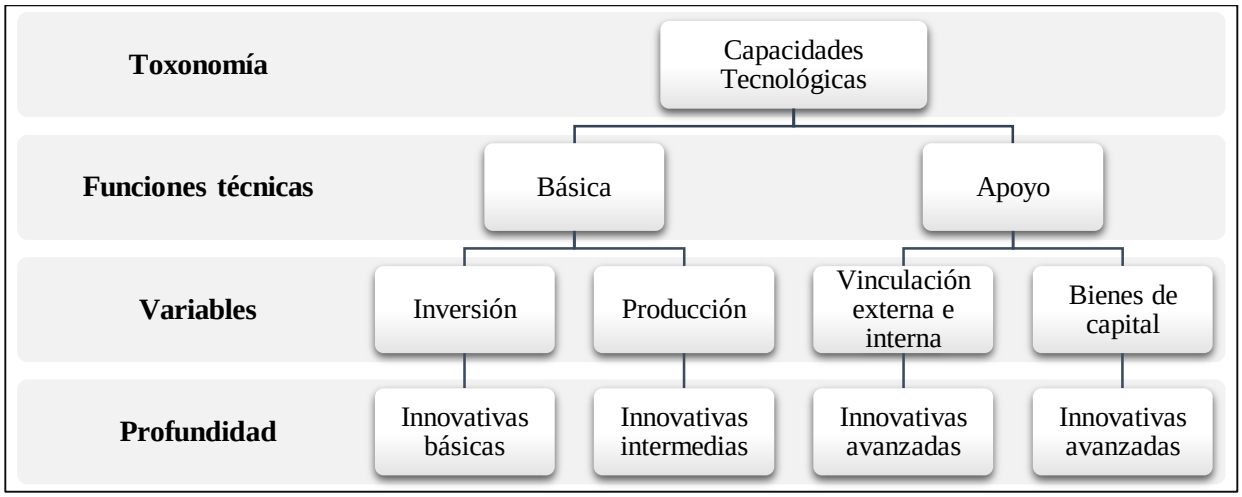

Figura 15. Clasificación de principales capacidades tecnológicas. Fuente: Elaboración propia con base en Bell y Pavitt (1995).

Fundamentados en la clasificación de Bell y Pavitt se han realizado distintos estudios sobre los procesos de aprendizaje al interior de las empresas, dando como pauta la apertura de una importante línea de investigación que se basa en estudios de caso y de encuestas, que tienen como finalidad buscar los procesos clave de aprendizaje y los factores que pueden estimular y limitar estos procesos, y el los cuales se han podido documentar los procesos de aprendizaje (Arias, 2004).

En el estudio de Cohen & Levinthal (2000) sobre la innovación y el aprendizaje, se resalta la importancia para generar innovaciones y desarrollar capacidades en la empresa, que ayudan a generar aprendizaje o capacidad de absorción, es decir, la unión del nivel de educación y de la absorción de los empleados, la infraestructura tecnológica y el apoyo a la gestión. Por ello, distinguen tres fuentes de conocimiento tecnológico utilizado por una empresa, la primera, son las actividades de I+D propias de la empresa, posteriormente, es el conocimiento originado por la distribución de actividades de I+D de los competidores, y por último, el conocimiento que se origina fuera de la industria. En efecto, señalan que la facilidad del aprendizaje o capacidad de absorción es la suma del dominio del gasto en generado por I+D, así como de la absorción de

conocimientos y la delimitación de las condiciones de oportunidad tecnológica y ventaja competitiva de la empresa.

Por su parte, Hernández (2017) plantea que las empresas innovadoras extraen conocimiento de una gran variedad de fuentes y vínculos externos, y los integran a sus propias rutinas y procesos de aprendizaje, para posteriormente lograr capacidades tecnológicas más avanzadas, las empresas *Fintech* son un ejemplo de ello. El concepto de Sistema Nacional de Innovación (SNI) busca exponer las dinámicas de desarrollo, haciendo hincapié en las interacciones entre instituciones, tanto pública y privadas, en donde sus actividades e interacciones inician, importan, modifican y difunden nuevas tecnologías (Freeman, 1989). Asimismo, tienen influencia el tamaño de la empresa, el acceso a las competencias del mercado, la capacidad de organización y de gestión en la empresa y su capacidad de cambio en las estructuras para absorber nuevos métodos y tecnologías (Katz, 2007).

2.3.4. Factores normativos. En la actualidad, los esfuerzos para crear un marco regulatorio adecuado para los servicios y productos que ofrecen las instituciones *Fintech* se deben a factores que han impulsado las actividades que éstas desarrollan, principalmente propiciadas por el incremento en el número de participantes que se encuentran innovando en el sector de servicios financieros y sumado a la creciente penetración de los diferentes servicios ofrecidos por las *Fintech* entre los consumidores, y aunado a la ausencia de políticas en la mayoría de los países que fomenten el desarrollo del sector (Finnovista, 2017; Basilea, 2018).

En este sentido, el Consejo Nacional de Inclusión Financiera (CONAIF), asegura que, gracias al resultado de la discusión entre los emprendedores y empresas del sector, se ha promovido la creación de asociaciones que se orientan a representar los puntos de vista de la nueva industria de servicios financieros ante los reguladores, así como promover el conocimiento sobre las *Fintech*

entre el público general y coordinar actividades para impulsar mejores prácticas en la industria. Es así como surgieron, por ejemplo, la Asociación de Fondeo Colectivo (AFICO) en México en 2014 (que contó con el apoyo del Fondo Multilateral de Inversiones del grupo BID), la Asociación Brasileña de *Equity Crowdfunding* en 2014, la Asociación *Fintech* México en 2015, y la Asociación Brasileira de *Fintechs (ABFintechs*) y la Asociación Colombia *Fintech*, ambas creadas a finales de 2016, por último, en México se crea la Ley ITF en México creada en el 2018 (CONAIF, 2016).

De esta última, se aprueba el 9 marzo del 2018 la Ley para Regular a las Instituciones de Tecnología Financiera, donde se establecen, dentro de las Disposiciones Preliminares, los principios fundamentales que fomentan la inclusión y la innovación financiera, promocionan la competencia, la protección al consumidor, la preservación de la estabilidad financiera, la prevención de operaciones ilícitas, así como la neutralidad tecnológica, con el objeto de regular los servicios financieros que prestan las instituciones de tecnología, así como su organización, operación y funcionamiento, y los servicios financieros sujetos a normativas especiales ofrecidas a través de modelos novedosos, entendidos como aquellos que para la prestación de servicios financieros utilizan herramientas o medios tecnológicos con modalidades distintas a las existentes en el mercado (Ley ITF, 2018).

En general Ayón y Pérez (2017), señalan que los reguladores de esta ley se interesan por prevenir el abuso y el fraude a consumidores y a los inversionistas, y a que sean utilizadas como instrumento para el lavado de dinero y el terrorismo. No obstante, en algunos otros casos, señala que también se interesan por otorgar flexibilidad para que sigan innovando y apoyando en la inclusión financiera. Y dependiendo de la tolerancia al riesgo y del nivel de apoyo al desarrollo

del sector, los gobiernos pueden facilitar la prestación de servicios y la innovación, o por el contrario puede restringirlos.

Por ello, en México dicha Ley se encarga de la supervisión y verificación, que en el cumplimiento de sus obligaciones se encuentran a cargo de la CNBV, Banxico, la CNSF, la CONSAR y la CONDUSEF, cada una en el ámbito de su competencia. De tal forma que para que dichas instituciones puedan organizarse y operar, deben contar con autorización, además, deben estar obligadas a tomar medidas que eviten la difusión de información falsa o engañosa, con la finalidad de que dichas alertas se difundan por las ITF y con sus clientes, en relación a los riesgos en las operaciones que celebran con o a través de ellas (Ley ITF, 2018).

De lo anterior, el Basilea (2016) destaca que es necesario tomar este tipo de medidas, ya que la presencia de un posible colapso potencial de la plataforma debido a un fallo en sus sistemas, controles, red o infraestructura es un tema que sin duda se enfrentan a las empresas *Fintech*, ya que al gestionar una gran cantidad de datos valiosos en sus plataformas digitales procedentes de sus operaciones, ponen en riesgo el patrimonio de sus clientes, así como el de la misma organización, puesto que estas abarcan grandes brechas en materia de seguridad.

Por otra parte, la Ley ITF expresamente establece que las ITF están obligadas a agregar a su denominación las palabras *Institución de financiamiento colectivo* o *Instituciones de fondo de pago electrónico*, según corresponda. Por lo que las expresiones *Institución de Tecnología financiera (ITF)*, *institución de financiamiento colectivo* o *instituciones de fondo de pago electrónico*, o cualquier otra que refiera ideas semejantes, no podrán ser usadas en el nombre, denominación, razón social o publicidad de personas y establecimientos, interfaces, aplicaciones informáticas, páginas de internet, o cualquier otro medio de comunicación electrónica o digital distintos de las ITF autorizadas (Ley ITF, 2018).

Adicionalmente el Basilea (2018) sostiene que es necesario que la regulación *Fintech* señale por separado las actividades bancarias y financieras, su alcance y prohibiciones, incluyendo las actividades que puede realizar una plataforma, tales como la suscripción de contratos de préstamo y de equidad; la participación y otros tipos de emisiones de valores; proyectos de selección, clasificación, puntuación, publicación y promoción; el uso y desarrollo de los canales electrónicos; y cualesquier otras actividades consideradas por el regulador. Esta es una decisión muy importante debido a las implicaciones para la protección del consumidor y la posibilidad de la mala conducta de plataformas.

Por lo anterior, la finalidad de la Ley *Fintech* es regular a las *instituciones de financiamiento colectivo* y a las *instituciones de fondo de pagos electrónicos*, las primeras son aquellas que están destinadas a poner en contacto a personas del público en general, con el fin de que entre ellas se otorgue un financiamiento en las operaciones que realicen de manera profesional y habitual, por medio de aplicaciones informáticas previamente autorizadas por la CNBV. Se les denomina inversionistas y solicitantes quienes intervengan en estas operaciones, por una parte, el inversionista es quien aporta y puede ser una persona física o moral, mientras que el solicitante, persona física o moral, es quien requiere a través de esta institución, financiamiento colectivo, por lo que realizan operaciones en moneda extranjera o con activos virtuales, por lo que las instituciones de financiamiento colectivo, pueden actuar como mandatarias o comisionistas de sus clientes (Ley ITF, 2018).

Así mismo, se establece, dentro de las *Disposiciones generales aplicables a las Instituciones de Tecnología Financieras*, emitidas el 18 de septiembre del 2018, que las *instituciones de financiamiento colectivo*, están obligadas a proporcionar a sus clientes los medios necesarios para lograr la formalización de las operaciones, incluso establecer esquemas para compartir con los

inversionistas los riesgos de las operaciones de financiamiento colectivo de deuda, por lo que deben de incluir el pacto de cobro de la proporción de las comisiones y esquemas de incentivos entre las ITF y el inversionista, previa autorización de la primera. En consecuencia, las comisiones por financiamiento a morosos no podrán ser superiores a las que cobren por financiamientos vigentes, incluso si así lo acuerdan, tienen permitido realizar la cobranza extrajudicial respecto de los créditos otorgados a los solicitantes por cuenta de los inversionistas (Diario Oficial de la Federación, DOF, 2018a).

Respecto a las instituciones de fondo de pago electrónico, estos representan servicios de emisión, administración, redención y transmisión de fondos de pago electrónico por medio de los actos de aplicaciones informáticas, interfaces, pago por internet o cualquier otro medio de comunicación electrónica o digital, servicios que sólo se prestarán por las personas morales autorizadas por la CNBV.

En ella, se pueden abrir y llevar cuentas de fondos de pago electrónico, emitidos contra la recepción de una cantidad de dinero en moneda nacional, extranjera o incluso con activos virtuales determinados, entendiéndose por fondos de pago electrónico los que estén contabilizados en un registro electrónico de cuentas transaccionales que al efecto lleve una institución de fondos de pago electrónico y que queden referidos a un valor monetario, equivalente a una cantidad determinada de dinero, o bien a unidades de activos virtuales previamente determinados por el Banco de México (DOF, 2018a).

De la misma manera, se autoriza a estas instituciones para operar con activos virtuales, pero únicamente los activos que sean determinados por el Banco de México mediante las Disposiciones de carácter general aplicables a las ITFs, y en todos los casos deben difundir entre sus clientes los riesgos que conlleva la celebración de operaciones con este tipo de activos a través de su página

de internet o cualquier otro medio que utilicen para prestar su servicio, y señalando claramente que operan con activos virtuales, mismas que al ser solicitadas las cantidades de lo que este sea titular, deben estar en posibilidad de ser entregados a los clientes respectivos, o bien, el monto en moneda nacional que corresponda al pago recibido de la enajenación de los activos virtuales que le corresponden.

Es relevante señalar que las ITF podrán agruparse en asociaciones gremiales por el desarrollo e implementación de estándares de conducta y operación, mismas que deberán cumplir sus agremiados e incluso podrán emitir estatutos por normas para ingreso, o bien, para adoptar mejores prácticas y estándares de conducta, así como verificar su sano cumplimiento.

En el mismo orden de ideas, las Disposiciones de carácter general aplicables a las ITFs contemplan sanciones administrativas que pueden ser impuestas a aquellas entidades financieras, ITF o sociedades autorizadas para operar con modelos novedosos, mismas que pueden se acreedoras a multas de 30,000 a 150,000 UMAS, y a personas distintas de las autorizadas que usen la palabra ITF con multas de hasta 1,000 a 5,000 UMAS. Así mismo, las ITF están obligadas a prevenir y detectar actos u omisiones de operaciones que puedan encuadrar en el artículo 139 de la presente ley.

El Comité de Supervisión Bancaria de Basilea (Basilea) ha permanecido ajeno a esta regulación, ya que sostiene que las áreas que deben de ser consideradas por la regulación y supervisión deben seguir centrarse en atender a la evolución de la innovación tecnológica, señalando que los supervisores deben continuar reforzando sus capacidades para la supervisión de los cambios que la tecnología está provocando en el sector financiero. La tecnología y los servicios financieros han superado las fronteras, de modo que la cooperación internacional ha devenido en esencial (Basilea, 2018a).

No obstante, Uría (2017) sostiene que el desarrollo de la regulación tanto en México como el mundo, debería ser capaz de garantizar neutralidad, de modo que los prestadores tradicionales de servicios financieros y los nuevos entrantes, empresas *Fintech*, puedan beneficiarse por igual de las medidas que se introduzcan para favorecer la innovación en el ámbito de los servicios financieros y, al mismo tiempo, proporcionar a todos los agentes la seguridad jurídica para que puedan aprovecharse todas las ventajas derivadas de la tecnología.

3. Metodología

3.1. Descripción General del Diseño Metodológico

En el presente capítulo se exponen los fundamentos que justifican la decisión de utilizar una metodología cualitativa para contestar la pregunta de investigación central: ¿De qué manera se puede mitigar el impacto financiero de los riesgos a los que son susceptibles las Instituciones de Tecnología Financiera? Así mismo, como se señala el primer capítulo, la preposición central sobre lo que se parte en esta tesis para responder a la pregunta de investigación es: "El impacto financiero de los riesgos a los que son susceptibles las Instituciones de Tecnología Financiera, se pueden mitigar mediante una estrategia integral de administración de riesgos que considere los aspectos tecnológicos, humanos, organizacionales y normativos de estas instituciones".

Para comprobar dicha preposición central, el objetivo que se persigue es: "Proponer una estrategia integral de gestión de riesgos operacionales en las Instituciones de Tecnología Financieras de México, que tenga en consideración los aspectos tecnológicos, humanos, organizacionales y normativos; a fin de disminuir el impacto financiero que puedan sufrir dichas instituciones y sus clientes, ante amenazas tecnológicas".

Por ello, se considera abordar un diseño de investigación con un enfoque cualitativo el cual, según Hernández, Fernández y Baptista (2006) es un enfoque que utiliza la recolección de datos sin medición numérica para descubrir o afinar preguntas de investigación en el proceso de interpretación, y en donde se emplean descripciones detalladas de situaciones, eventos, personas, interacciones, conductas observadas y sus manifestaciones. En las investigaciones cualitativas, la reflexión es el puente que vincula al investigador y a los participantes (Mertens, 2014).

Con base en lo anterior, esta tesis pertenece a la línea de investigación *Toma de decisiones estratégicas y financieras,* y su metodología puede resumirse en los siguientes pasos:

1. Análisis e interpretación del marco normativo de las instituciones *Fintech* a nivel internacional, con la finalidad de hacer un estudio comparativo del contenido de los textos legales vigentes.
2. Análisis de mejores prácticas a nivel internacional de las acciones en materia de regulación, supervisión y gestión de riesgos operacionales en las actividades bancarias.
3. Estudio de caso del Ataque a SPEI a Banxico en el 2018, centrándose en las variables que originaron las afectaciones a bancos.

Por último, la investigación se centra en la creación de una estrategia integral de gestión de riesgos operacionales, que toma en cuenta aspectos tecnológicos, el factor humano y la estructura organizacional, con la finalidad de permitir a la dirección de estas instituciones, el entendimiento de los riesgos y adoptar las medidas necesarias para identificarlos y mitigarlos a través de un sistema de control interno acorde a la naturaleza, complejidad y riesgos operacionales. Entendiendo como estrategia a todo aquello que implica elegir, dentro de un conjunto de acciones ordenadas y destinadas a abordar las problemáticas identificadas en un diagnóstico, y que tienen que ver con los principales desafíos que enfrenta una empresa o institución (Tarziján, 2007).

3.1.1. Análisis de marco normativo internacional. En el presente apartado se estudia el contexto a profundidad bajo el cual se rige el marco normativo vigente en México y a nivel internacional para las Instituciones de Tecnología Financiera (ITF). En consecuencia y conforme a las clasificación de Olliver y Thompson (2017) se utiliza un enfoque cualitativo, no experimental, a través de la técnica del derecho comparado, el cual según Sirvent (2008) es un método que tiene como finalidad confrontar las semejanzas y diferencias de los diversos sistemas jurídicos vigentes en el mundo con el propósito de comprender y confrontar los ordenamientos jurídicos

institucionales entre sí, y como consecuencia entenderlo mejor. La Tabla 1 muestra el diseño metodológico empleado.

Tabla 1

Diseño del método para el análisis del marco normativo internacional.

Elementos del método	Método de investigación empleado
Enfoque	Mixto: Cualitativo
Tipo de Investigación	No experimental
Temporalidad	Transversal
Nivel de Profundidad	Comparativo
Diseño del Método	Análisis e interpretación de *Sandbox* Regulatorios
Sujetos o unidades de análisis	Aspectos tecnológicos, humanos, organizacionales y normativos
Técnica	Derecho comparado
Instrumento	Normatividad internacional de la regulación y supervisión *Fintech*
Alcance	Desarrollo de categorías conceptuales
Limitaciones	Fuentes de información
Procedimiento	Recopilación de documentos oficiales, comparación, interpretación, discusión de resultados, elaboración de reporte final

Fuente: Elaboración propia con base en Galeano (2012).

El contenido y las categorías a observar se centran especialmente en iniciativas y medidas de regulatorias y de supervisión *Fintech*, representadas por *Sandbox* regulatorios como variables, tomando en cuenta los *Sandboxes* que a la fecha han realizado una declaración formal por un regulador o cuerpo gubernamental, después, se identifican diferencias y similitudes con las normativas jurídicas a nivel internacional, se desarrollaron categorías conceptuales y se analizaron las relaciones entre las variables. Por lo tanto, el nivel de profundidad que se aplica es de carácter comparativo, puesto que se enfoca sólo a comparar las funciones que enmarcan las iniciativas, las herramientas y los objetivos perseguidos.

La información se recopila de documentos oficiales, plataformas web gubernamentales, artículos e informes de las normativas institucionales existentes a nivel internacional. Para el análisis de la información se utiliza el software Atlas.ti versión 7, el cual permite extraer, categorizar e inter-vincular segmentos de datos cualitativos desde los documentos mencionados anteriormente, y se crea una red semántica con las categorías mencionadas anteriormente.

Los *Sandboxes* representan plataformas habilitadas en entornos de prueba controlados por organizamos reguladores, en el que los proyectos innovadores o entidades que se encuentran en estados iniciales de desarrollo, pueden emprender su actividad bajo la modalidad de extensión, para el caso de actividades que sí pueden situarse bajo el paraguas del regulador con la normativa actual, o bien bajo la modalidad de no sujeción para el caso de actividades aun no expresamente reguladas por su estructura innovadora (García, 2018).

Por tal motivo, los *Sandboxes* regulatorios que se comparan correspondieron a países como España, Reino Unido, Canadá, Hong Kong, Malasia, Argentina, Singapur y Australia. Estos países han impulsado iniciativas, tanto públicas como privadas para el estímulo y apoyo en el campo de la tecnología financiera. Según el informe de Deloitte (2017) uno de los aspectos clave del sector *Fintech* es la regulación, en el mencionado informe incluyeron iniciativas regulatorias como un indicador que sirvió para determinar el *Inditex Performance Score* de la cuidad, un índice que señala la importancia del sector *Fintech* en un panorama mundial. Dentro de las mejor valoradas se encuentran aquellos países que tienen sus propios *Sandboxes* regulatorios en marcha, mismos que se analizan en la presente investigación.

3.1.2. Análisis de mejores prácticas internacionales. Este apartado se centra en analizar las mejores prácticas a nivel internacional en el estudio de acciones, políticas y propuestas que en la actualidad implementan organismos como: el Comité de Supervisión Bancaria de Basilea (BCBS);

La Organización para la Cooperación y el Desarrollo Económicos (OCDE); el Fondo Monetario Internacional (FMI); El Banco Interamericano de Desarrollo (BID); y el Banco de México, con la finalidad de conocer el contexto general de las acciones que se implementan en materia de regulación, supervisión y gestión de riesgos operacionales en las actividades bancarias. La Tabla 2, muestra el diseño metodológico que se persiguió.

Tabla 2

Diseño del método para el análisis de mejores prácticas internacionales.

Elementos del método	Método de investigación empleado
Enfoque	Mixto: Cualitativo
Tipo de Investigación	No experimental
Temporalidad	Transversal
Nivel de Profundidad	Descriptivo
Diseño del Método	Análisis de mejores prácticas internacionales
Sujetos o unidades de análisis	BCBS, OCDE, FMI, BID y Banxico
Técnica	Recolección y revisión bibliográfica y análisis de contenido
Instrumento	Documentos consultados
Alcance	Desarrollo de categorías conceptuales
Limitaciones	Fuentes de información
Procedimiento	Recopilación de documentos oficiales, comparación, interpretación, discusión de resultados, elaboración de reporte final

Fuente: Elaboración propia con base en Galeano (2012).

Por ello, y conforme la clasificación de Olliver y Thompson (2017), se utiliza un enfoque cualitativo, no experimental, que pretende describir los principios de supervisión bancaria, el gobierno corporativo para bancos, supervisión basada en riesgos y las implicaciones para bancos y sistemas bancario propuestos por los organismos mencionados anteriormente, por medio de la técnica de recolección, revisión de bibliografías y análisis de contenido, y con un nivel de

profundidad de carácter descriptivo. Para el análisis de la información se utiliza el software Atlas.ti versión 7, para extraer, analizar e inter-vincular segmentos de datos cualitativos desde los instrumentos mencionados anteriormente, creando con ello, una red semántica con las categorías de las descripciones mencionadas anteriormente.

3.1.3. Estudio de caso: Ataque a SPEI Banxico en 2018. Esta sección busca apoyar y facilitar el entendimiento sobre la situación actual en materia de riesgos cibernéticos a los que se exponen los bancos e instituciones financieras que utilizan plataformas electrónicas. Por tal motivo, en el presente apartado se utiliza el estudio cualitativo de caso, no experimental, que, de acuerdo con la clasificación de Galeano (2012), el tipo o clase de estudio que se aborda es un estudio de caso intrínseco, aquel que se construye a partir del interés de un caso en específico, por ello, se examina el caso particular de *Ataque a Sistema de Pagos Electrónicos Interbancarios (SPEI) 2018*, con la finalidad de proporcionar mayor conocimiento sobre la problemática de ciberataque presentado en el SPEI que conecta con instituciones financieras y el Banco de México. La Tabla 3 muestra el diseño descrito anteriormente.

Así mismo, es necesario señalar que el caso de estudio se enfoca en una investigación de carácter tranversal. A su vez, se realiza el estudio a un nivel de profundidad de tipo descriptivo, con la finalidad de desarrollar categorias conceptuales, que abarcan: los sucesos y funciones operativas del SPEI; los factores de riesgo operacional; factores organizacionales; y su relacion con el marco normativo de las ITFs. De esta manera, la técnica que se utiliza se centra en la recopilación de informes oficiales del ataque al SPEI e informes trimestrales emitidos por el Banco de México, dichos informes contemplaron el periodo de enero a junio correspondientes al periodo en el que se registraros los ataques, y una entrevista semiestructurada al Director General de

Desarrollo Regulatorio de la CNBV, el Lic. Luis Leyva Martínez, llevada a cabo el día 4 de octubre del 2018, a las 9:00 horas y por vía telefónica, misma que se encuentra en el Apéndice A.

Tabla 3

Diseño del método para el estudio de caso: Ataque a SPEI Banxico 2018.

Elementos del método	Método de investigación empleado
Enfoque	Mixto: Cualitativo
Tipo de Investigación	No experimental
Temporalidad	Transversal
Nivel de Profundidad	Descriptivo
Diseño del Método	Análisis del caso de estudio. Ataque a SPEI de Banxico 2018
Sujetos o unidades de análisis	Sucesos operativos del SPEI Abril-Mayo, Factores de riesgo operacional, Factores organizacionales, Marco normativo
Técnica	Triangulación de informes oficiales, informes trimestrales emitidos por Banxico y entrevista semiestructurada
Instrumento	Documentos consultados
Alcance	Desarrollo de categorías conceptuales
Limitaciones	Fuentes de información
Procedimiento	Solicitud de entrevistas, realización de entrevistas, captura de información, análisis de resultados, interpretación, discusión de resultados, elaboración de reporte final

Fuente: Elaboración propia con base en Galeano (2012).

Para el análisis de la información se utiliza el software Atlas.ti versión 7, para extraer, analizar e inter-vincular segmentos de datos cualitativos desde los documentos mencionados anteriormente, creando con ello, una red semántica con las categorías de las descripciones mencionadas anteriormente.

3.1.4. Estrategia integral de riesgos operacionales *Fintech*. En este último apartado, se presenta una propuesta para la implementación y desarrollo de un sistema de gestión e integral de

riesgos operacionales, para su aplicación a empresas *Fintech*. Para el desarrollo de la propuesta, se muestran las relaciones entre los principios Gobierno corporativo, supervisión basada en riesgos y un modelo de gestión de riesgo operacional.

Por lo que, el análisis de la investigación se basa en: la asignación de autoridades y responsabilidades basadas en las mejores prácticas de gobierno corporativo; la estructuración de políticas y procedimientos para la identificación, medición, mitigación y monitoreo de los procesos para una supervisión basada en riesgos; y por último, se consideran los procesos para la elaboración de políticas y procedimientos de administración de riesgos operacionales, el establecimiento de medidas de mitigación de riesgos, y procedimientos documentados de recuperación y reestructuración de operaciones, como un requisitos para la gestión de riesgos operacionales.

4. Resultados

4.1. Marco Normativo Internacional: *Sandboxes* Regulatorios

Las innovaciones en tecnología financiera son planteadas como nuevas oportunidades para los consumidores de este tipo de servicios y para el mercado financiero en general. Estos reflejan mayores oportunidades de inclusión financiera o menores costos de transacción. No obstante, resulta que es esencial el papel de las autoridades para evaluar las implicaciones de las innovaciones en tecnología financiera, para determinar si el marco regulatorio debe modificarse o adecuarse para incorporarse a los nuevos avances.

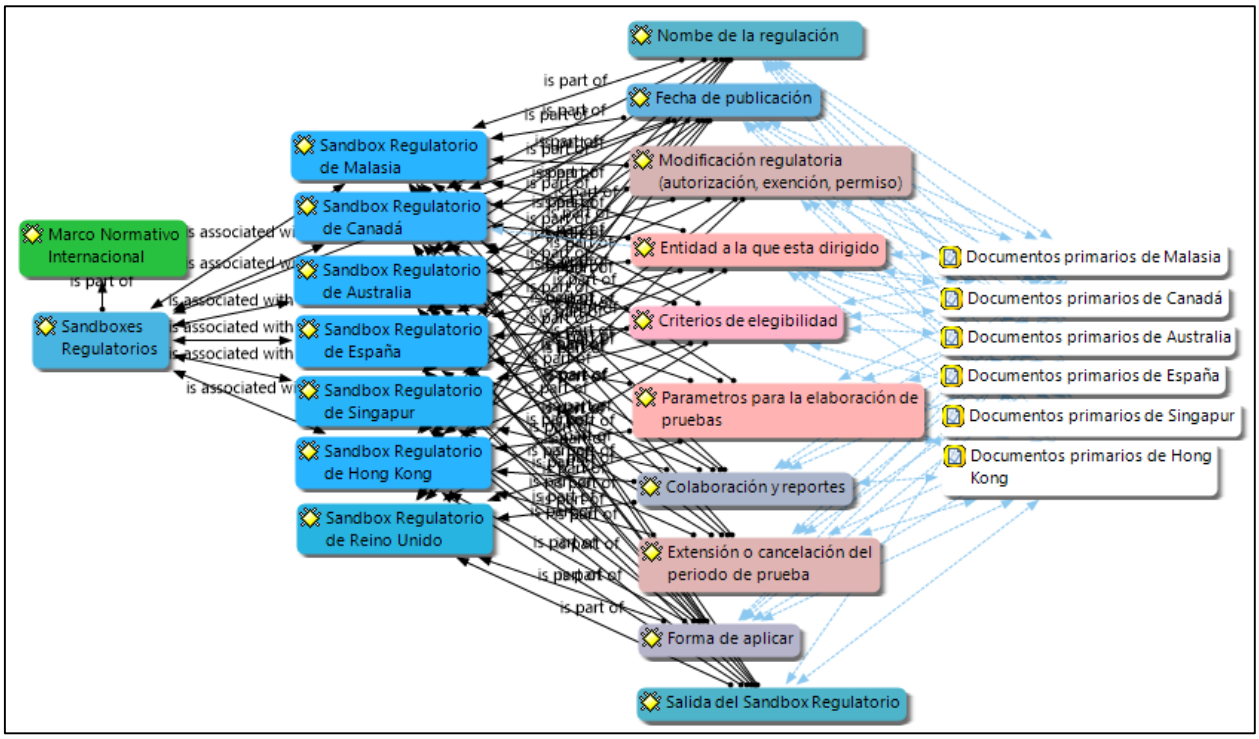

Figura 16. Red semántica del análisis del marco normativo internacional. Fuente: Elaboración propia.

Con base en la idea anterior, a continuación se presentan las iniciativas más valoradas en cuanto a los *Sandbox* regulatorios propuestos por organismos reguladores o gubernamentales que han

hecho su declaración formal, destacando a países como Malasia, Canadá, Australia, España, Singapur, Hong Kong y el Reino Unido. Así mismo, la Figura 16 muestra la red semántica del análisis realizado en el software Atlas.ti. En el Apéndice B, se muestran tablas del análisis del contenido de los organizamos que representan a los países mencionados anteriormente.

4.1.1. Descripción general por país de los *Sandbox* regulatorios.

Malasia: Bank Negara Malaysia (BNM). El Banco Central de Malasia, (BNM) por sus siglas en inglés, busca proporcionar un entorno regulatorio que sea propicio para el despliegue del sector *Fintech*, el cual debe incluir la revisión y la adopción de los requisitos o procedimientos regulatorios que pudiesen impedir las innovaciones o hacerlas inviables. Como parte del proceso, BNM presenta un *Financial Technology Regulatory Sandbox Framework*, el 18 de octubre del 2016, el cual permitie que la innovación *Fintech* se puedan implementar y probar en un entorno real, dentro de parámetros y plazos específicos (BNM, 2016).

Canadá: Canadian Securities Administrators (CSA). El *CSA Regulatory Sandbox* de Canadá, se creó el 23 de febrero del 2017 como una iniciativa de *Canadian Securities Administrators* (CSA), para apoyar a las entidades de Tecnología Financiera (*Fintech*) que buscan ofrecer productos, servicios y aplicaciones innovadores en Canadá, y el cual permite que las entidades puedan inscribirse y obtener apoyo para exentar los requisitos de la Ley de Valores de Canadá, siempre y cuando éstas, tengan la intención de probar sus productos, servicios y aplicaciones en todo el mercado canadiense y por tiempo limitado (CSA, 2017).

Australia: Australian Securities and Investment Commission (ASIC). La Comisión australiana de Valores e Inversiones (ASIC) por sus siglas en inglés, se creó para fomentar y facilitar la innovación de los mercados de servicios financieros y de crédito, siempre y cuando, sea

posible que éstos produzcan resultados beneficiosos para los inversores y los consumidores de servicios financieros. Tras la búsqueda para facilitar el desarrollo de productos y servicios innovadores, ASIC estableció un centro de innovación para apoyar a las nuevas empresas de tecnología financiera *Fintech*. Para ello, crea el *Regulatory Guide* (RG) 257 "*Testing Fintech products and services without holding an Australian Financial Services (ASF)* o *credit license*", el cual, permite que los productos o servicios de empresas *Fintech* se prueben sin autorización. El *Regulatory Guide* 257, se publicó en agosto de 2017, basado en la legislación y los reglamentos en la fecha de su emisión, Así mismo, la versión anterior "*Superseded Regulatory Guide* 257", fue publicada en diciembre de 2016 y actualizada en febrero de 2017 (ASIC, 2017).

España: Asociación Española Fintech e Insurtech. La Asociación española *Fintech* e *Insurtech* establece la necesidad de adoptar medidas para el desarrollo de entidades *Fintech*, puesto que éstas han traído beneficios para el conjunto de la economía española, mismos que definen la necesidad de crear un marco regulatorio apropiado, por medio de la reducción de los problemas de información asimétrica, y el aumento de la competencia en el sector financiero. Por tal motivo, valoran la necesidad de diferenciar a aquellas entidades cuyas actividades se encuentran sujetas a una autorización previa, respecto de aquellas que únicamente pueden prestar servicios adicionales al ámbito financiero. Por ello, en febrero del 2017 se emite el *Libro Blanco de la Regulación Fintech en España*, en el que se establecen propuestas regulatorias independientes (Asociación Española Fintech e Insurtech, 2016).

Singapur: Monetary Authority of Singapore (MAS). La Autoridad Monetaria de Singapur (MAS) por sus siglas en inglés, es la encargada de fomentar y experimentar el sector *Fintech*, con la finalidad de probar innovaciones prometedoras en el mercado, las cuales, puedan tener la oportunidad de una adopción más amplia, tanto en Singapur como en el extranjero. Para lograr

este objetivo, se define que las instituciones financieras *Fintech* o cualquier empresa interesada, puede solicitar ingresar a un espacio de seguridad regulatoria *Sandbox*, por tanto, el 16 de noviembre del 2016, se crea *FinTech Regulatory Sandbox Guidelines*, en el cual, se permite experimentar servicios financieros innovadores en un entorno de prueba, pero dentro de un espacio y duración definidos (MAS, 2016).

Hong Kong: Hong Kong Monetary Authority (HKMA), Securities and Futures Commission (SFC) y Insurance Authority. La Autoridad Monetaria de Hong Kong (HKMA) por sus siglas en inglés, la Comisión de Valores y Futuros (SFC) por sus siglas en inglés y la Autoridad de Seguros (IA) por sus siglas en inglés, lanzaron en Hong Kong un programa *Fintech Supervisory Sandbox (FSS)*, un programa *Regulatory Sandbox SFC* y un programa *Insurtech Sandbox* respectivos. Estas iniciativas tienen como finalidad, la realización de pruebas piloto de productos *Fintech* para aquellas empresas que tienen la intención de realizar una prueba, y solicitar el acceso al *Sandbox* considerado como el más relevante, y, donde el regulador, junto con otros reguladores, actúan como el punto de contacto principal, contribuyendo a que la entidad *Fintech*, pueda acceder al *Sandbox* de forma concurrente (HKMA, 2016; IA, 2017 y SFC, 2017).

Reino Unido: Financial Conduct Authority (FCA). El Reino Unido es el pionero en el desarrollo de incentivos regulatorios en el desarrollo de entidades *Fintech*. Es a través de la *Financial Conduct Authority* (FCA) que se lanza la iniciativa *Project Innovate*, el 16 de junio del 2017, con la finalidad de fomentar la innovación y el interés de los consumidores y promover su competencia. Dentro del *Project Innovate* se desarrolla la iniciativa de *Regulatory Sandbox* por el cual, la FCA recibe información sobre las necesidades de los distintos participantes y supervisa las pruebas utilizando un entorno regulatorio personalizado para cada prueba, incluidas las garantías para los consumidores (FCA, 2017).

4.1.2. Análisis de categorías por país. Se observa que, generalmente, las instituciones financieras analizadas en la presente investigación (Figura 17), tienen la libertad de lanzar al mercado nuevos productos y servicios financieros, ya sea que, estás cuenten con una autorización correspondiente o bien, puedan inscribir sus productos ante las autoridades correspondientes. No obstante, en el caso de los productos y servicios que utilizan innovaciones en tecnología financiera, la legislación actual generalmente no contempla normativa específica para ese tipo de innovaciones, lo que deja en una línea de indefinición, si se trata o no, de actividades que deben ser reguladas y, en caso de ser reguladas, el enfoque bajo el cual debe definirse o modificarse la regulación y supervisión de estas innovaciones.

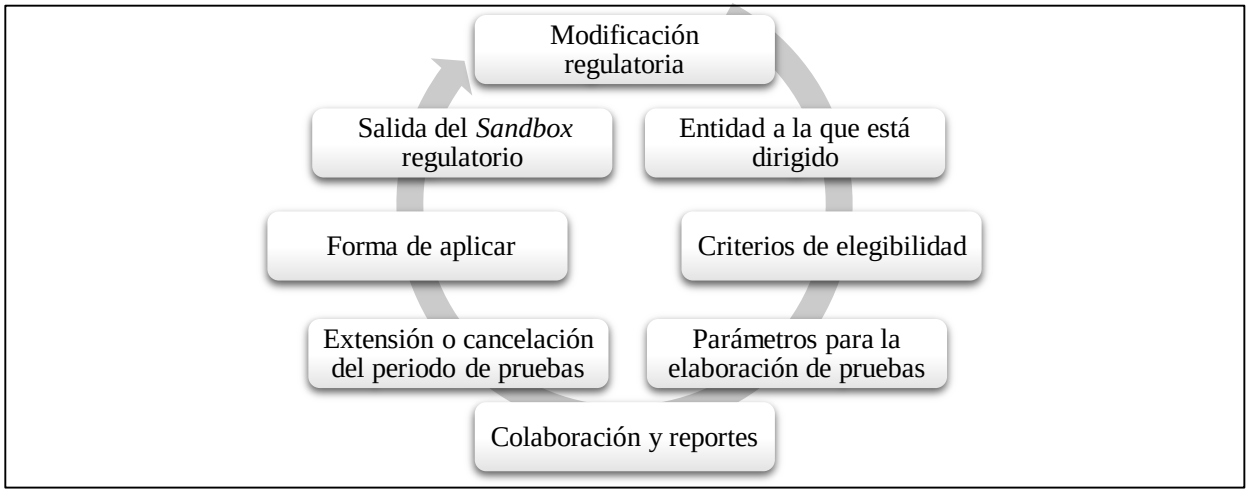

Figura 17. Elementos básicos de un *Sandbox* regulatorio. Fuente: Elaboración propia.

En este sentido, algunas autoridades financieras, como las mencionadas anteriormente, implementan esquemas bajo el enfoque de experimentación regulatoria, es decir, *Sandbox* regulatorios, con la intención de que, las instituciones de tecnología financiera (*Fintech*) tengan la oportunidad de desarrollar productos o servicios que implican beneficios para los consumidores o que contribuyan al crecimiento del mercado. En este contexto, y aun cuando existen diferencias

entre los diferentes *Sandbox* regulatorios, de manera general, se puede afirmar que todos cuentan con elementos básicos: modificación regulatoria, entidad a la que está dirigido, criterios de elegibilidad, parámetros para la elaboración de pruebas, colaboración y reportes, extensión o cancelación del periodo de pruebas, forma de aplicar y salida del *Sandbox* regulatorio, tal como se muestra en la Figura 17. A continuación se presenta una comparación de los elementos básicos de los países sujetos al análisis.

Modificación regulatoria: (autorización, exención, permiso). En Malasia, el BNM adopta un enfoque de director informal, para proporcionar orientación y asesoramiento a las entidades *Fintech* sobre las modificaciones o requerimientos legales y regulatorios vigentes que se puedan realizar. La modalidad del *Sandbox* regulatorio de Canadá, de forma similar, se basa en la realización de cambios en su marco regulatorio, según es necesario, y en virtud de los avances de nuevas innovaciones tecnológicas, no obstante, en Canadá las empresas autorizadas para operar en el *Sandbox* deben permanecer sujetas a todos los requisitos regulatorios que puedan aplicarse.

En el caso de Australia, una empresa necesita tener una licencia o autorización AFS antes de que pueda lanzar al mercado un nuevo producto o servicio financiero. Sin embargo, en algunas situaciones, es posible probar estos productos o servicios sin una autorización. Hay tres casos en los que no se requiere una autorización, y puede ser por medio de una exención de autorización *Fintech*, o solicitar otro tipo de exención de autorización ya prevista en la ley para probar el producto, o solicitar una cancelación individual de ASIC que representa una excepción individual. De forma similar, en el Reino Unido, las entidades deben ser autorizadas o registradas por la FCA, a menos que se apliquen ciertas exenciones, para ello, la FCA cuenta con un proceso de autorización que se ajusta a las empresas que son aprobadas en el *Sandbox* regulatorio.

En Hong Kong, las modalidades emitidas por la IA, SFC y HKMA, son propuestas similares a la de Australia y el Reino Unido, puesto que, la IA, SFC y HKMA son las encargadas de determinar los requisitos legales y regulatorios específicos que se adaptan dependiendo del tipo de actividad que realicen. Similarmente, en Singapur, el MAS es la institución encargada de determinar los requisitos legales y regulatorios específicos que se flexibilizan dependiendo del producto financiero a probar, el tipo de solicitante y el tipo de innovación.

En el caso de España, su propuesta se basa en la modalidad de no sujeción, en la que el *Sandbox* regulatorio permite que las entidades *Fintech* e *Insurtech* que realicen actividades no expresamente reguladas hasta la fecha, comiencen a probar sus productos en un espacio de pruebas seguro o controlado, permitiendo así lanzar este tipo de productos y servicios innovadores al mercado con el respaldo de los reguladores. En el Apéndice B, Tabla B1, se muestran las categorías de análisis y su descripción detallada por país.

Entidad a la que está dirigido. En Malasia, el *Sandbox* regulatorio es creado para que se aplique a: entidades financieras establecidas por cuenta propia o en colaboración con una empresa *Fintech,* o una empresa *Fintech* que tenga la intención de solicitar o solicite la aprobación del BNM para participar en el *Sandbox*; una empresa *Fintech* que pretenda continuar operando, es decir, una empresa autorizada o registrada; y, una empresa que ya ha sido autorizada o registrada de acuerdo a la legislación vigente de Malasia.

Por su parte, en Canadá, el CSA *Regulatory Sandbox* se dirige a modelos de negocios que son verdaderamente innovadores desde la perspectiva del mercado canadiense, en donde los solicitantes pueden ir desde empresas de nueva creación, hasta empresas ya establecidas. De forma similar, en Singapur, el *Sandbox* regulatorio se dirige a las empresas que buscan aplicar la tecnología de una manera innovadora, para brindar servicios financieros que puedan o estén

regulados por el MAS. Así mismo, en Hong Kong, la IA, SFC y HKMA dirigen su iniciativa *Sandbox* regulatorio al desarrollo y aplicación de la tecnología en la industria, asociándose a la actividad correspondiente de dichos organismos.

En el caso de España, se valora la necesidad de diferenciar aquellas entidades cuyas actividades se encuentran sujetas a una autorización previa, respecto de aquellas que únicamente pueden prestar servicios adicionales al ámbito financiero. Para ello, se plantean propuestas regulatorias independientes, destacando el: asesoramiento y gestión patrimonial; finanzas personales, financiación alternativa, *crowdlending, equity crowdfunding, crowdfunding/lending,* servicios transaccionales/divisas, medios de pagos, infraestructura financiera, criptocurrencies y *blockchain, insurtech,* identificación *online* de clientes y *big data.*

Por su parte, el *Sandbox* regulatorio de Australia, se propone para: el titular de una autorización o licencia ASF existente; productos o servicios que no requieren autorización; y, entidades que, sean de representantes autorizados o sean parte de la estructura corporativa de una empresa que tenga una licencia ASF. Con algunas similitudes, en el Reino Unido su *Sandbox* regulatorio se dirige a entidades autorizadas, a entidades no autorizadas que requieren autorización para operar con negocios de tecnología. En el Apéndice B, Tabla B2, se muestran las categorías de análisis y su descripción detallada por país.

Criterios de elegibilidad. En Malasia el BNM toma en cuenta los beneficios potenciales del producto, servicio o solución propuesto, tales como: la eficacia, la seguridad, la accesibilidad y la calidad de los servicios financieros; la mejora de la eficacia y la eficiencia de la gestión de riesgos potenciales y sus respectivas medidas de mitigación; y, abrir nuevas oportunidades de financiamiento o inversiones en la economía de Malasia. En el caso de Canadá, las empresas que deseen postularse deben estar preparadas para proporcionar pruebas en el *Sandbox* regulatorio, un

plan de negocios y una discusión de los beneficios potenciales para los inversores, que incluya la forma de minimizar los riesgos de los inversores.

No obstante, en Singapur, los solicitantes que desean entrar al *Sandbox* regulatorio, deben ayudar a fomentar más la experiencia del sector *Fintech* dentro de un espacio y duración bien definidos; administrar mejor los riesgos; crear nuevas oportunidades; o mejorar la vida de las personas. Así mismo, el solicitante debe entender claramente el objetivo y los principios del *Sandbox,* y debe enfatizar que el *Sandbox* no puede usarse como un medio para eludir los requisitos legales y reglamentarios. Adicionalmente, el producto debe de ser diferente a los que actualmente existen, de lo contrario, el solicitante debe demostrar que se está aplicando una tecnología diferente, o la misma tecnología se aplica de manera diferente. Así mismo, el solicitante debe demostrar que ha cumplido con sus procedimientos debidamente.

Para el caso del Reino Unido, las solicitantes tienen que cumplir con una serie de requisitos, los cuales determinan la necesidad de que las entidades solicitantes deban ofrecer innovaciones destinadas al mercado del Reino Unido, innovaciones nuevas y únicas. Además, la innovación debe ofrecer una buena perspectiva de los beneficios identificables para los consumidores, y debe de existir una verdadera necesidad de probar la innovación en el *Sandbox* propuesto por la FCA. En el Apéndice B, Tabla B3, se muestran las categorías de análisis y su descripción detallada por país.

Parámetros para la elaboración de pruebas. En Malasia, el solicitante, debe realizar una evaluación adecuada para demostrar la utilidad y funcionalidad del producto, servicio o solución e identificar los riesgos asociados. Así mismo, los solicitantes deben demostrar que tienen los recursos necesarios para respaldar las pruebas en el *Sandbox*. Esto incluye, los recursos necesarios y la experiencia para mitigar y controlar los riesgos y pérdidas potenciales que surgen de la oferta

del producto, servicio o solución, además de que deben tener un plan de negocios realista para implementar el producto, servicio o solución a una escala comercial en Malasia después de salir del *Sandbox*.

En el caso de Canadá, las empresas solicitantes deben presentar su modelo de negocios al personal de su regulador local de valores. La tarea del personal es analizar el modelo de negocio, para ello, deben realizar preguntas y trabajar con la empresa para identificar los requisitos regulatorios para los cuales se necesita un registro y/o exención libre. Así mismo, el personal y la empresa también pueden negociar sobre la elegibilidad de la empresa para participar en el *Sandbox* regulatorio de la CSA, incluidos los límites y las condiciones que podrían imponerse. Posteriormente, la empresa debe presentar una solicitud a su regulador local de valores para registrarse y liberar los requisitos regulatorios, de tal forma que si se presentó de forma adecuada ante el regulador local de valores, la solicitud se puede hacer bajo el régimen de pasaportes australianos, lo que le da a la empresa acceso a los mercados de capital en múltiples jurisdicciones.

En Australia, ASIC determina que se deben evaluar las solicitudes de AFS y las autorizaciones de crédito, como parte de su función como regulador de las industrias de servicios financieros y de crédito. Además, se define que los intermediarios deben cumplir con una serie de obligaciones generales, como requisitos para hacer todo lo necesario para garantizar que los servicios cubiertos se presten de manera eficiente, honesta y justa, y por medio de; el cumplimiento de las leyes y condiciones pertinentes para sus autorizaciones; tener soluciones adecuadas de resolución de conflictos y compensación para clientes minoristas; y tomar medidas para garantizar que sus representantes estén adecuadamente capacitados, sean competentes y cumplan con la ley.

En España, sólo se menciona que las entidades *Fintech* o *Insurtech* beneficiarias pueden comenzar su actividad empresarial bajo la modalidad de exención para el caso de actividades

reguladas o bien bajo la modalidad de no sujeción para el caso de actividades no expresamente reguladas. En el caso de Singapur, no se definen parámetros previamente, no obstante se menciona que dado que el *Sandbox* funciona en el entorno de prueba, debe tener un espacio y una duración bien definidos para el lanzamiento del servicio financiero propuesto, dentro del cual, se pueden contener las consecuencias de posibles fallas.

En Hong Kong, la IA, dentro de sus parámetros, establece que debe haber un alcance claramente definido en el *Sandbox*, que incluya tiempo y duración, o fecha de lanzamiento oficial esperada de la iniciativa al mercado, el tamaño y tipo de negocio de seguros, y usuarios específicos, la tecnología involucrada, los resultados esperados y los criterios de éxito de la prueba; así mismo, debe contar con los controles de gestión de riesgos y la protección del cliente, recursos y preparación de la aseguradora y una estrategia de salida del *Sandbox*.

Por su parte, la SFC en Hong Kong, impuso sus propios parámetros que incluyen; la limitación de los tipos de clientes a los que la empresa puede atender o la exposición máxima de cada cliente, a fin de limitar el alcance y los límites del negocio de la empresa en actividades reguladas. En algunos casos, las condiciones de la licencia pueden requerir que la empresa establezca esquemas de compensación apropiados para los inversores, o que se someta a auditorías periódicas de supervisión por parte de la SFC. Además, se espera que las empresas calificadas cuenten con medidas adecuadas de protección al inversor para abordar los riesgos o inquietudes reales o potenciales identificados cuando operan en el *Sandbox*.

Así mismo, la HKMA, en Hong Kong, establece que la administración de un banco autorizado para usar FSS, debe garantizar limites en la implementación de definiciones claras sobre el alcance y las fases (si las hay) de pruebas piloto, los acuerdos de tiempo y terminación; medidas para proteger los intereses de los clientes; controles de compensación para mitigar riesgos asociados

con un cumplimiento incompleto de los requisitos de supervisión; la preparación de los sistemas y procesos involucrados en la prueba y monitoreo cercano de la prueba; por último, se establece que la FSS no debe utilizarse como un medio para eludir los requisitos de supervisión aplicables.

En el caso del Reino Unido, el solicitante debe de contar con un plan de pruebas bien desarrollado con objetivos, parámetros y criterios de éxito claros, deben además, contar con pruebas realizadas hasta la fecha, contar con recursos para probar en el *Sandbox* y contar con protecciones para asegurar a los consumidores y proporcionar compensaciones adecuadas, si es necesario. En el Apéndice B, Tabla B4, se muestran las categorías de análisis y su descripción detallada por país.

Colaboración y reportes. En el caso de Malasia, se precisaron requerimientos de aplicación, donde estable que el solicitante debe presentar al BNM una carta de solicitud firmada por el Director Ejecutivo (CEO) del solicitante u oficial debidamente autorizado por el CEO. El solicitante también debe incluir los resultados clave que la prueba pretende lograr, y los indicadores apropiados para medir dichos resultados. Posteriormente, se especifica que el BNM debe informar al solicitante de su elegibilidad para participar en el *Sandbox*. A partir de entonces, se establece que el BNM involucraría a los participantes en parámetros de prueba, como el alcance y la duración de la prueba, las flexibilidades regulatorias solicitadas y la frecuencia de los informes; medidas específicas para determinar el éxito o el fracaso de la prueba al final del período de prueba; una estrategia de salida si la prueba falla o se suspende; y un plan de transición para la implementación del producto, servicio o solución a escala comercial, luego de realizar pruebas exitosas y salir del *Sandbox*.

Para el caso de Canadá, las empresas que tengan la intención de operar en el CSA *Regulatory Sandbox,* deben estar preparadas para proporcionar al personal de la CSA la información sobre sus

operaciones, para fines de monitoreo y recopilación de datos, y a su vez, éstas deben estar sujetas a revisiones de cumplimiento y vigilancia por la CSA. No obstante, en el caso de en Australia, se define que dentro de los 2 meses posteriores al final de la exención, la entidad debe enviar a la ASIC un breve reporte con los detalles de la prueba, que incluye información sobre los clientes, sobre la naturaleza de las quejas, aspectos o retos a los que se enfrentaron, requisitos regulatorios identificados como barreras e información financiera.

En España, sólo se menciona que AEFI es la principal asociación representativa del sector *Fintech* e *Insurtech* en España, la cual tiene como objetivo, colaborar y promocionar la interacción entre las principales entidades del mercado en España. De forma similar, en Singapur, los participantes deben reportar al MAS sobre los avances de la prueba, de acuerdo al calendario previamente acordado entre ellos y colaborar mutuamente en cuestiones relevantes. En el caso del Reino Unido, una vez que se solicita el acceso al *Sandbox* regulatorio, la FCA trabaja de manera abierta y transparente con el solicitante, para garantizar que en todo momento permanezca listo, dispuesto y organizado para cumplir con los estándares del *Sandbox*.

En Hong Kong, la IA establece un equipo de facilitación de *Insurtech* para mejorar la comunicación con las empresas involucradas en el desarrollo y la aplicación de *Insurtech* en Hong Kong, así como para promover a Hong Kong como un centro de *Insurtech* en Asia. El objetivo del equipo, es facilitar la comprensión de la comunidad de *Insurtech* sobre el régimen regulatorio actual, así como, actuar como una plataforma para intercambiar ideas de iniciativas innovadoras de *Insurtech* y brindar asesoramiento sobre temas relacionados con *Insurtech*, según corresponda. Por su parte, la SFC en Hong Kong, las empresas calificadas pueden ser puestas bajo un monitoreo y supervisión estrecha por parte de la SFC cuando operan en el *Sandbox*. En tales casos, el SFC

puede participar en un diálogo más intenso con las empresas, y puede resaltar las áreas de cumplimiento en las que pueden mejorar sus controles internos y la gestión de riesgos.

Por otro lado, la HKMA, en Hong Kong, crea una sala de chat que busca proporcionar comentarios de supervisión a los bancos y empresas tecnológicas en una etapa temprana, cuando se están contemplando nuevas aplicaciones tecnológicas, lo que reduce el trabajo abortivo y acelera el despliegue de nuevas aplicaciones tecnológicas. Las empresas pueden acceder a la sala de chat a través de correos electrónicos, videoconferencias o reuniones cara a cara con el HKMA. En el Apéndice B, Tabla B5, se muestran las categorías de análisis y su descripción detallada por país.

Salida del Sandbox regulatorio. En Malasia, al finalizar la prueba, los participantes deben presentar un informe final que contenga: resultados clave, indicadores de rendimiento clave frente a las medidas acordadas para el éxito o fracaso de la prueba y los resultados de la prueba; una cuenta completa de todos los informes de incidentes y resolución de quejas de los clientes; y, en el caso de una prueba fallida, las lecciones aprendidas de la prueba. En el caso de Canadá, una vez completados los periodos de prueba, se precisa, que el personal de la CSA debe revisar la solicitud de forma libre, para determinar los límites y las condiciones que se aplicarán a la empresa en el CSA *Regulatory Sandbox*, caso por caso, una vez que haya finalizado el periodo de prueba.

Para el caso de Australia, una vez transcurridos los 12 meses de exención, la empresa no podrá ofrecer el producto innovador hasta que cumpla con todos los requisitos legales y obtener la licencia ASF o establecer un acuerdo con una empresa que tenga licencia ASF. No obstante, en España, se evalúan los resultados de las pruebas, y la autoridad supervisora, tras consultar con el promotor, se decidirá sobre la caducidad de la licencia *Sandbox*. En el caso de *Singapur*, al salir del *Sandbox* regulatorio, la entidad puede lanzar el producto al mercado solo si cumple con las

condiciones previamente establecidas, es decir, MAS y la entidad, deben estar de acuerdo en que la prueba cumplió con los resultados esperados y que la entidad puede cumplir con todos los requerimientos legales y regulatorios.

En Hong Kong, en el caso de la IA, el solicitante debe presentar al IA una estrategia de salida para la ejecución piloto si tiene que terminarse sin éxito, puesto que el *Sandbox* no es un medio para eludir los requisitos de supervisión aplicables y relacionados. El caso de la SFC, en Hong Kong, una vez que una empresa calificada ha demostrado que su tecnología es confiable y adecuada para su propósito, y que sus procedimientos de control interno han abordado adecuadamente los riesgos identificados, la empresa puede solicitar al SFC la eliminación o variación de algunas o todas las condiciones de licencia impuestas, por lo que puede llevar a cabo actividades reguladas y estar sujeto a la supervisión de la SFC en las mismas condiciones de las entidades con licencia que operan fuera del *Sandbox*.

Por último, en el Reino Unido, una vez que el solicitante haya sido autorizado por la FCA, debe cumplir con estándares mínimos en todo momento, cumplir con las normas y principios relevantes para su negocio y enviar informes periódicos. En el Apéndice B, Tabla B6, se muestran las categorías de análisis y su descripción detallada por país.

Extensión o cancelación del periodo de prueba. En Malasia, al finalizar el período de prueba, la aprobación para participar en el *Sandbox* y cualquier flexibilidad regulatoria otorgada a los participantes expirará automáticamente, a menos que el participante haya obtenido una aprobación previa por escrito del BNM para una extensión del período de prueba. Sin embargo, se debe de considerar que el período de prueba inicial no debe exceder los 12 meses a partir de la fecha de inicio de la prueba. Para extender el período de prueba, los participantes deben enviar una solicitud por escrito al BNM a más tardar 30 días calendario antes de que finalice el período de prueba.

Por su parte, en Australia, ASIC puede otorgar una exención individual para extender el periodo de prueba la extensión es de 12 meses. No obstante, en el caso de España, se establece que de no cumplirse los resultados esperados, se realizará la concesión de una prórroga definida o indefinida, para el caso de que las actividades probadas aún no se encuentren reguladas tras esta fase, o la obtención de una licencia ordinaria cuando las entidades *Fintech* o *Insurtech* hayan alcanzado la capacidad necesaria para cumplir con los requisitos habituales.

De manera similar, en Singapur y el Reino Unido, se establece que si existieran razones excepcionales por las cuales el servicio financiero propuesto no se pueda implementar en Singapur, el solicitante debe estar preparado para continuar contribuyendo de otra manera,ya que, los escenarios de prueba, y los resultados esperados de la prueba en el *Sandbox,* deben estar claramente definidos. En el caso de Hong Kong, la SFC sólo considera que si una empresa calificada que opera en el *Sandbox* no está en forma y no es adecuada para mantener la licencia, su licencia puede ser anulada. En el Apéndice B, Tabla B7, se muestran las categorías de análisis y su descripción detallada por país.

Forma de aplicar. En Malasia, el BNM detalla formatos especiales e información específica para las entidades solicitantes. No obstante, en Canadá, para presentar una solicitud para aplicar en el *Regulatory Sandbox,* la entidad solicitante debe comunicarse con el regulador de valores en la jurisdicción donde se encuentra su oficina central. Para ello, se asigna a un personal dedicado, quien debe estar disponible para entidades *Fintech* que buscan asistencia para navegar el entorno regulatorio de valores.

En el caso de Australia, no se necesita aplicar para obtener este beneficio, es decir, se define que si la empresa cumple con los requisitos de elegibilidad y sigue las condiciones previstas, tiene la exención por 12 meses. No obstante, el único requisito es que debe notificar a la ASIC antes de

usar la exención de licencia y enviar determinada información, para que posteriormente ASIC notifique por escrito la fecha en que inicia su exención de licencia. Así mismo, la guía destaca claramente que el uso de la exención de la licencia no significa que la empresa haya obtenido la licencia o autorización ASF. Similarmente al caso de Australia, en el Reino Unido no es necesario aplicar para obtener este beneficio. Si la empresa cumple con los requisitos de elegibilidad y sigue las condiciones previstas por la FCA.

En el caso de España, el supervisor competente debe analizar el proyecto presentado y los documentos que se acompañen y resolverá sobre la concesión o no de la licencia. Además, la autoridad supervisora tiene la facultad de conceder licencias condicionadas al cumplimiento de determinados requisitos o, incluso, firmar protocolos individuales cuando considere necesario que ambas partes, supervisor y solicitante, manifiesten por escrito los distintos compromisos asumidos para la concesión de la licencia.

Para el caso de Singapur, de forma similar al caso de Malasia, existen formatos especiales e información específica que debe enviarse por correo electrónico a un oficial de revisión del MAS. Por ello, se crean tres etapas, la primera es la etapa de aplicación, posteriormente, la etapa de evaluación, y por último, la etapa de experimentación.

En Hong Hong, la IA cuenta con un grupo de trabajo *Future Task Force* (FTF) enfocado a promover la aplicación *Fintech* en la industria de seguros, misma que brinda orientación para la aplicación de un *Sandbox* regulatorio. Por su parte, la SFC crea un portal en línea de asesoramiento y seguimiento en línea. Por otra parte, el HKMA recomienda que los bancos y sus empresas tecnológicas asociadas que intenten acceder al FSS, se pongan en contacto con el HKMA antes de tiempo. En el Apéndice B, Tabla B7, se muestran las categorías de análisis y su descripción detallada por país.

4.2. Mejores Prácticas Internacionales: Regulación y Supervisión Bancaria

El Comité de Supervisión Bancaria de Basilea (BCBS) señala que un sistema eficaz de supervisión bancaria se sitúa en elementos externos o condiciones previas que repercuten en la eficacia de la supervisión en la práctica, estos elementos externos incluyen, entre otros, a políticas macroeconómicas sólidas y sostenibles, una infraestructura pública bien desarrollada y una disciplina de mercado eficaz. Así mismo, en la práctica diaria, los supervisores también son responsables de reaccionar a tiempo para mitigar los efectos que dichas deficiencias pueden tener para la eficacia de la regulación y la supervisión de las entidades (Guerrero, Focke, y Mejía, 2011).

Por otra parte, el fortalecimiento del marco normativo basado en el cumplimiento de los estándares internacionales de regulación y supervisión, históricamente ha incluido aspectos como: la protección legal a los supervisores; la autorización de los establecimientos bancarios y su supervisión permanente; un adecuado esquema de gobierno corporativo y gestión integral de riesgos; normas de adecuación de capital; transparencia y protección al usuario de servicios financieros; y reglas que facilitan el acceso al financiamiento. Así mismo, el Comité señala que la mayoría de los países de América Latina han ido fortaleciendo su regulación y su supervisión. En este sentido, sostiene que los países han reforzado sus normas de capacidad de capital, que incluye no sólo el riesgo crediticio, sino también el riesgo de mercado, de tasa de interés y operacional. De igual forma, se han adoptado normas relacionadas con la administración de riesgos integrales, de crédito, de liquidez, de mercado, operativo, legal, de reputación, etc., y principalmente se han orientado hacia procesos de supervisión enfocada en riesgos.

En efecto, el enfoque moderno de supervisión bancaria pone énfasis al menos a tres aspectos mencionados anteriormente: la supervisión consolidada de los conglomerados financieros, los esquemas de supervisión transfronteriza (ambos considerados ya entre los principios de

supervisión bancaria de Basilea y la OCDE), y el enfoque de supervisión basada en riesgos. Con base en lo anterior, los siguientes apartados, muestran las categorías que se analizan y los hallazgos encontrados. La Figura 18 muestra la red semántica del análisis realizado en el software Atlas.ti.

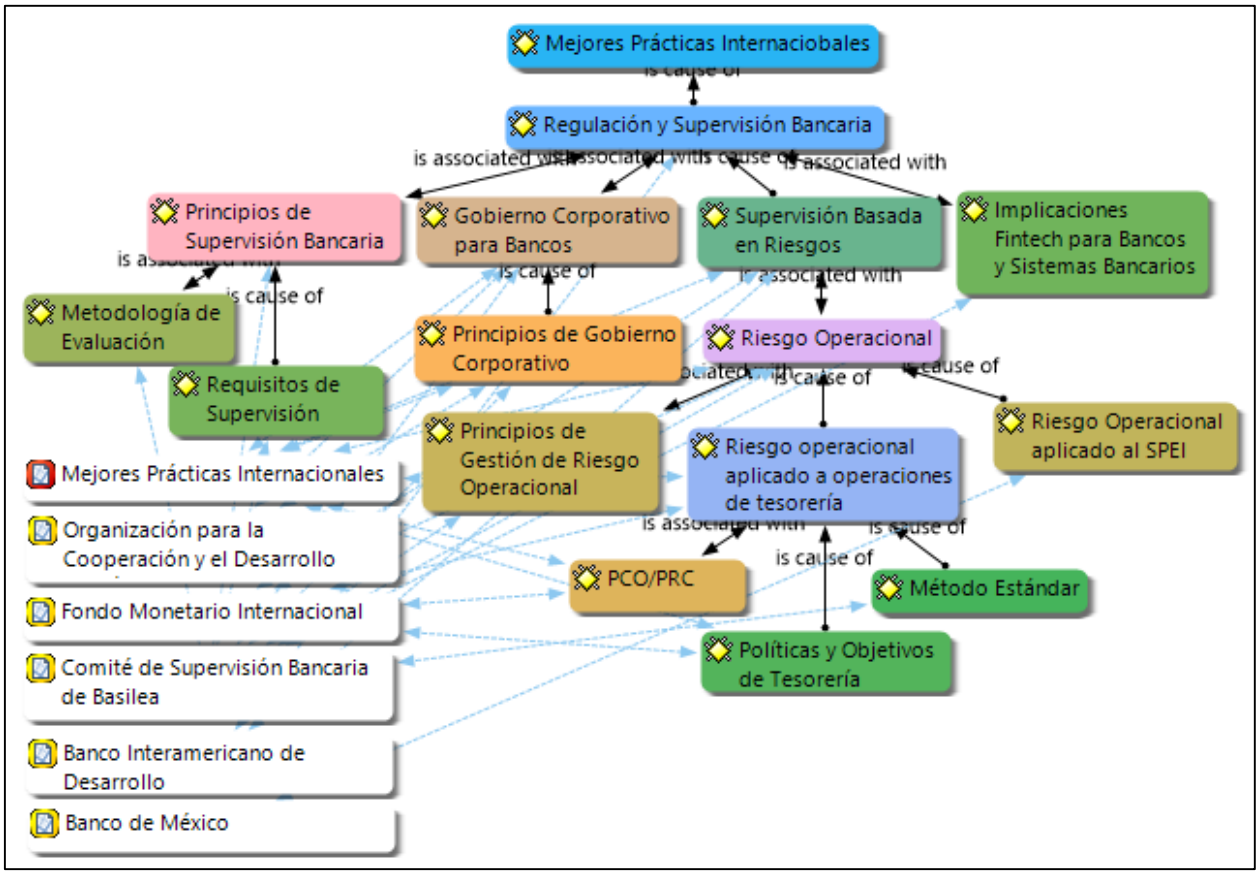

Figura 18. Red semántica de mejores prácticas internacionales. Fuente: Elaboración propia.

4.2.1. Principios de supervisión bancaria. Los Principios Básicos para una supervisión bancaria eficaz emitidos por la BCBS representan normas mínimas obligatorias para la correcta regulación y supervisión de bancos y sistemas bancarios. En los países, dichos principios sirven como referencia para evaluar la calidad de sus sistemas de supervisión e identificar las medidas necesarias para alcanzar niveles de calidad semejantes a las prácticas de supervisión. Los principios básicos también los son utilizados por el Fondo Monetario Internacional (FMI) y el Banco Mundial en su programa de evaluación del sector financiero (PESF), con la finalidad de

comprobar la eficacia de los sistemas y prácticas de supervisión bancaria en los distintos países (Basilea, 2011).

Los Principios Básicos ofrecen un estándar integral para el establecimiento de la regulación, supervisión, buen gobierno y gestión de riesgos del sector bancario, y ante la importancia de implementar normas consistentes y de forma efectiva. Dichos principios básicos constan de 29 reglamentos necesarios para la eficacia del sistema financiero. Los principios se agruparon en dos grandes categorías.

La primera (Principios 1 a 13) se centran en las facultades, atribuciones y funciones de los supervisores, tales como: las atribuciones, objetivos y facultades para las autoridades que participan en la supervisión de bancos y grupos bancarios; independencia operativa, rendición de cuentas en el desempeño de sus funciones, recursos adecuados y protección legal de los supervisores; la cooperación y colaboración con las autoridades locales y supervisores extranjeros; las actividades que pueden desarrollar las entidades autorizadas para operar con bancos y sujetas a supervisión; los criterios para la concesión de licencias y el cambio de titularidad de participaciones significativas; las adquisiciones sustanciales; un enfoque supervisor para el desarrollo y mantenimiento de una evaluación prospectiva del perfil de riesgo de bancos individuales y grupos bancarios; técnicas y herramientas de supervisión e informes de supervisión; facultades correctivas y sancionadoras del supervisor; supervisión consolidada para todo el grupo bancario y en base a un adecuado seguimiento; y, relaciones entre el supervisor de origen y el de desarrollo de grupos bancarios transfronterizos.

Mientras que la segunda (Principios 14 a 29) se desarrollan las regulaciones y requisitos prudenciales que deben cumplir los bancos, tales como: gobierno corporativo de políticas y procesos solidos; procesos de gestión integral de riesgos; suficiencia de capital; adecuados

procesos de gestión del riesgo de crédito; activos dudosos, provisiones y reservas; concentración de riesgos y límites de exposición a grandes riesgos; transacciones con partes vinculadas para reducir el riesgo de conflictos de intereses; riesgo país y riesgo de transferencia; adecuados procesos de gestión del riesgo de mercado; riesgo de tasa de interés en la cartera de inversión; adecuados procesos de gestión de riesgo de liquidez; adecuados procesos de gestión del riesgo operacional; control de auditoria internos; información financiera y auditoria externos; divulgación y transparencia; y, utilización abusiva de servicios financieros.

Estos principios son creados para promover la seguridad y solidez del sistema financiero mundial. No obstante, es importante que el enfoque regulatorio se base en el tipo de riesgos que crean las actividades de instituciones financieras no bancarias, que tome en cuenta que los aspectos de regulación son necesarios para proteger la estabilidad y solidez del sistema financiero, pero ajustados acorde al tipo y tamaño de las operaciones de las instituciones , y que, ya sean bancos o instituciones no bancarias, la regulación debe medir los riesgos derivados de esta línea de negocios contra los costos de supervisión, y de esa manera impulsar la inclusión financiera en los países.

Requisitos de supervisión bancaria. El Comité de Basilea señala que los supervisores deben ser capaces de asegurar las condiciones externas que puedan afectar negativamente al conjunto de bancos o sistemas bancarios, ya que un sistema de supervisión bancaria fuerte, es aquel en el que se pueden desarrollar, implementar, vigilar y hacer cumplir políticas de supervisión en circunstancias económicas y financieras normales o de tensión. Para ello, se crean elementos básicos o prerrequisitos que afectan directamente a la eficiencia de la supervisión en la práctica, ya que no suelen ser parte del dominio directo o único de los supervisores bancarios (Basilea, 2011).

Los elementos básicos antes mencionados incluyen: políticas macroeconómicas sólidas y sostenibles; un marco bien concebido para la formulación de políticas de estabilidad financiera; una infraestructura pública bien desarrollada; un marco claro para la gestión, recuperación y resolución de crisis; un adecuado nivel de protección sistémica (o red de seguridad pública); y una disciplina de mercado eficaz. Para ello, los supervisores deben trabajar junto con los gobiernos y autoridades competentes para solucionar problemas que no sean de su competencia directa o única, así como también, deben adoptar medidas que impidan las consecuencias de dichos problemas para la eficiencia de la regulación y supervisión de los bancos.

Metodología de evaluación. La metodología se crea para aplicarse en varios contextos, por una parte, se puede aplicar por medio de una autoevaluación realizada por los propios supervisores bancarios, las evaluaciones del FMI y el Banco Mundial sobre la calidad de sistemas de supervisión, por exámenes realizados por terceros en el sector privado, como empresas de consultoría, o revisiones por pares. No obstante, sea cual sea el contexto, debe de considerar los beneficios que trae consigo dicha evaluación en el cumplimiento de los principios básicos (Basilea, 2011).

Además, señala que es mejor que una parte externa debidamente calificada sea la encargada de la evaluación en el cumplimiento de dichos principios, misma que debe de estar conformada por dos individuos con diversas perspectivas para que exista un control dual. Así mismo, se sugiere que para una evaluación justa en el proceso de supervisión bancaria, no debe ser revisada sin la cooperación auténtica de todas las autoridades pertinentes, además se plantea que la evaluación por personas inexpertas podría inducir a errores, por ello, la evaluación debe de ser aplicada de forma integral.

4.2.2. Gobierno corporativo. El Comité de Supervisión Bancaria de Basilea (BCBS) destaca que un gobierno corporativo es esencial para el correcto funcionamiento del sector bancario y de la economía en su conjunto, puesto que los bancos desempeñan un papel crucial en la economía, mediante la intermediación de capital entre ahorradores y depositantes, para actividades que fomentan el desarrollo empresarial y crecimiento económico. Además, la seguridad y robustez de los bancos son clave para la estabilidad financiera, por lo que su forma de operar es fundamental para una economía sólida (Basilea, 2015).

Del mismo modo, el BCBS sostiene que un gobierno corporativo debe tener como finalidad proteger el interés de las partes que puedan resultar afectadas, conformes con el interés público y de forma sostenible. Un gobierno corporativo puede determinar la asignación de autoridades y responsabilidades al Consejo de Administración y Alta Dirección en la práctica de las actividades y negocios del banco, entre ellos: fijan la estrategia y los objetivos del banco; seleccionan y supervisan al personal; dirigen las actividades bancarias cotidianas; protegen los intereses de los depositantes; alinean la cultura, actividades y el comportamiento de las entidades; y establecen funciones de control.

Por tanto, el Comité de Basilea basa sus directrices en los principios de gobierno corporativo publicados por la Organización para la Cooperación y el Desarrollo Económicos (OCDE). Los principios de la OCDE, que son ampliamente aceptados y establecidos, han intentado contribuir con los gobiernos en sus esfuerzos por evaluar y mejorar sus marcos de gobierno corporativo y han orientado a los participantes y reguladores de los mercados financieros.

La OCDE, declara que los supervisores se interesan por el gobierno corporativo por ser un componente esencial para el funcionamiento seguro y estable de cualquier banco, puesto que, de no aplicarse correctamente, podría deteriorar su perfil de riesgo. Los bancos bien gobernados han

contribuido a mantener un proceso de supervisión eficaz y eficiente, al resultar menos necesaria la intervención supervisora. Los gobiernos corporativos sólidos han permitido a los supervisores, depositar más confianza en los procesos internos del banco (OCDE, 2004).

En el mismo orden de ideas, el Comité de Basilea y sus atribuciones, evidencian el fortalecimiento tanto de las prácticas generales de gobierno de los bancos, como de los procesos de vigilancia por parte de los supervisores, razón por la que publicarón *Los principios para mejorar el gobierno corporativo* (Basilea III) (Basilea, 2015). Además, sostienen que los bancos, en general, comprenden los elementos más importantes del gobierno corporativo, como su vigilancia eficaz por parte del Consejo, la gestión rigurosa del riesgo, controles internos estrictos, el cumplimiento y otras áreas relacionadas. Para evaluar el progreso realizado por las autoridades nacionales y el sector bancario en el área de gobierno del riesgo, el Consejo de Estabilidad Financiera (FSB) encuentra que las instituciones financieras y las autoridades nacionales emprenden medidas para mejorar el gobierno enfocado al riesgo.

Principios de gobierno corporativo. Para lograr el objetivo de promover un gobierno corporativo sólido en las instituciones financieras, el Comité de Basilea (2015) plantea 14 principios generales diseñados para reforzar los principios básicos de gobierno corporativo que pueden ayudar a identificar, evitar o minimizar problemas. Dichos principios se enuncian a continuación:

- Principio 1. El consejo de administración tiene una responsabilidad con todo el banco, la cual incluye la aprobación y supervisión de la implementación de objetivos estratégicos del banco, el gobierno y los valores corporativos.
- Principio 2. Los miembros del Consejo de administración deben estar en constante capacitación para el buen desempeño de su puesto; deben contar con un claro entendimiento

de su rol que desempeñan dentro del gobierno corporativo y ser capaces de practicar un juicio sólido y objetivo sobre los asuntos del banco.

- Principio 3. El Consejo debe definir prácticas de gobierno corporativo apropiadas para su trabajo, y contar con medios necesarios que le permitan garantizar que éstas son seguidas y revisadas periódicamente para la mejora continua.
- Principio 4. En una estructura de grupo, el consejo de administración de la empresa tiene la responsabilidad de adecuar el gobierno corporativo en todo el grupo, y asegurarse de que existan políticas y mecanismos adecuados a la estructura, negocio y riesgo del grupo y sus entidades.
- Principio 5. Bajo la dirección del consejo de administración, la alta dirección debe asegurarse de que las actividades del banco sean consistentes con la estrategia del negocio, la tolerancia al riesgo y las políticas aprobadas por el consejo.
- Principio 6. Los bancos deben contar con un sistema de control interno efectivo y una función de administración de riesgos con suficiente autoridad, carácter, independencia, recursos y acceso al consejo.
- Principio 8. Una administración de riesgos efectiva requiere de una comunicación interna robusta dentro del banco acerca de riesgo, a través de la organización y por medio de reportes al consejo de administración y a la alta dirección.
- Principio 9. El consejo de administración y la alta dirección deben utilizar de manera efectiva el trabajo realizado por la función de auditoría interna, auditoría externa y la función de control interno.

- Principio 10. El consejo de administración debe supervisar activamente el diseño y operación del sistema de compensaciones, así como monitorear y revisar dicho sistema con el fin de asegurarse que éste opera según lo planteado.
- Principio 11. La compensación a empleados debe estar alineada de manera efectiva con los riesgos prudentes a tomar: las compensaciones deben ser ajustadas para todo tipo de riesgos, el resultado en las compensaciones debe ser simétrico con el resultado en los riesgos, los programas de compensación deben ser sensibles al horizonte temporal de los riesgos y la mezcla de dinero en efectivo, acciones y otra forma de compensación, deberá ser consistente con la alineación al riesgo.
- Principio 12. El consejo y la alta dirección deben saber y entender la estructura operacional del banco y los riesgos que ésta plantea.
- Principio 13. Cuando un banco opera a través de entidades con un propósito especial, o estructuras relacionadas o en jurisdicciones que impiden la transparencia o que no cumplan con estándares bancarios internacionales, el consejo de administración y la alta dirección deben entender el propósito, estructura y riesgos de estas operaciones y buscar mitigar los riesgos identificados.
- Principio 14. El gobierno del banco debe ser lo suficientemente transparente para sus accionistas, depositantes, otras partes interesadas relevantes y participantes del mercado.

No obstante, no existe un único modelo de buen gobierno corporativo, los principios de gobierno corporativo de la OCDE en colaboración con el G20, actualizados en el 2015, se apoyan en los elementos comunes a los diferentes estilos existentes. Estos se basan en un trabajo exhaustivo que recoge las nuevas tendencias en los sectores empresarial y financiero, incluyendo las enseñanzas aprendidas de la crisis financiera, el aumento de las actividades empresariales

transfronterizas, los cambios en el funcionamiento de los mercados de valores y las consecuencias de una cadena de inversión cada vez más larga y compleja (OCDE, 2016). Los 6 Principios de gobierno corporativo de la OCDE y el G20 tratan sobre:

- Principio 1. La consolidación de una base sólida para un marco eficaz de Gobierno Corporativo, el cual debe promover transparencia y equidad de los mercados, y la asignación eficiente de los recursos.
- Principio 2. El marco del gobierno corporativo debe proteger y facilitar el ejercicio de los derechos de los accionistas y garantizar el trato equitativo a todos ellos, incluidos los minoritarios y los extranjeros.
- Principio 3. El marco del gobierno corporativo debe proporcionar incentivos sólidos a lo largo de toda la cadena de inversión y facilitar que los mercados de valores funcionen de forma que contribuya al buen gobierno corporativo.
- Principio 4. El marco de gobierno corporativo debe reconocer los derechos de los actores interesados que disponga el ordenamiento jurídico o se estipulen de mutuo acuerdo, así mismo, debe fomentar la cooperación activa entre éstos y las sociedades.
- Principio 5. El marco del gobierno corporativo debe garantizar la comunicación oportuna y precisa de todas las cuestiones relevantes y relativas a la empresa.
- Principio 6. El marco para el gobierno corporativo debe garantizar la orientación estratégica de la empresa, el control efectivo de la dirección por parte del Consejo y la rendición de cuentas ante la empresa y los accionistas.

4.2.3. Supervisión basada en riesgos. Las mejores prácticas de supervisión a nivel internacional han tenido un enfoque de supervisión basada en riesgos (SBR). Este enfoque permite que el supervisor evalué y de seguimiento a los diversos riesgos, financieros y no financieros,

puesto que son inherentes y relevantes para las entidades supervisadas. Además, la SBR constituye un enfoque que incorpora elementos cuantitativos, como elementos cualitativos propios de cada entidad (Guerrero, Focke, y Pereira, 2011).

Así mismo, la SBR posibilita la realización de una evaluación integral por entidad, por grupo y en el sistema financiero en su conjunto, con el propósito de mitigar o evitar los riesgos sistemáticos. La SBR tiene entre sus tareas, verificar que las instituciones financieras apliquen modelos de administración del riesgo con una estructura formal, ordenada y lógica para desarrollar un enfoque de gestión de riesgos conocido como "IMMM" (Identificación, Medición, Mitigación o Control y Monitoreo); los modelos de IMMM de gestión de riesgos deben ser adecuados al tamaño y a la complejidad de la entidad financiera. No obstante, la SBR presenta carencias importantes, como la implementación de un gobierno corporativo y el cumplimiento de políticas orientadas a una disciplina de mercado.

Riesgo operacional. El Comité de Supervisión Bancaria de Basilea (Basilea, 2004) reconoce que el método preciso para la gestión de riesgos operativos que cada banco elija, depende de factores que consideran su tamaño y sofisticación, así como la naturaleza y complejidad de sus actividades. Así mismo, señala que para la realización de una adecuada gestión del riesgo operativo se requieren muchos elementos fundamentales, como estrategias claramente definidas y el seguimiento de las mismas por parte del Consejo de Administración y de la Alta Gerencia, una sólida cultura de gestión del riesgo operativo y de control interno, herramientas eficaces para la transmisión interna de información y planes de contingencia. Por tanto, el Comité subraya, que los principios aquí mencionados ofrecen a todos los bancos las pautas para desarrollar unas buenas prácticas.

***Principios de gestión de riesgos operativos*.** El Comité de Basilea (2011) estructura una serie de principios que derivan, en primera instancia: en el desarrollo de un marco adecuado para la gestión de riesgos, estos incluyeron los principios del 1 al 3; la gestión de riesgo operativo por medio de la identificación, evaluación seguimiento y control, destacando los principios del 4 al 7; y, la función de supervisión, ubicados en los principios del 8 al 10.

Dentro del desarrollo de un marco adecuado para la gestión de riesgos operativos, destaca la función de Consejo de Administración, quien debe ser responsable de conocer los principales aspectos de los riesgos operativos para el banco, y la revisión periódica del marco que utiliza el banco para la gestión de riesgos, y debe asegurar que dicho marco este sujeto a un proceso de auditoría interna eficaz e integral por parte del personal capacitado y competente. Así mismo, la alta gerencia debe ser responsable de poner en práctica dicho marco, aprobado por el consejo de administración.

En la identificación, evaluación, seguimiento y control de la gestión de riesgos operativos, los bancos deben identificar el riesgo operativo inherente a todos sus procesos, actividades, procedimientos y sistemas relevantes; así mismo, deben vigilar periódicamente los perfiles de riesgo y exposiciones relevantes a pérdidas; deben además, contar con políticas de procesos y procedimientos para controlar y cubrir los riesgos operativos más relevantes, así como, contar con planes de contingencia y continuidad de actividades.

Dentro de las funciones de la supervisión de un banco, se destaca, que estos deben exigir a los bancos el mantenimiento de un marco eficaz de identificación, evaluación, seguimiento y control de sus riesgos operativos más relevantes; además deben realizar una evaluación periódica de las políticas y procedimientos con las que cuenten los bancos; y, los bancos deben proporcionar información suficiente como medio de divulgación.

Riesgo operacional aplicado a operaciones de tesorería. Storkey (2011) señala que los tesoreros de un gobierno corporativo han comenzado a comprender la gestión del riesgo operacional y la importancia que cubre para sus tesorerías, la Figura 19 muestra los riesgos percibidos.

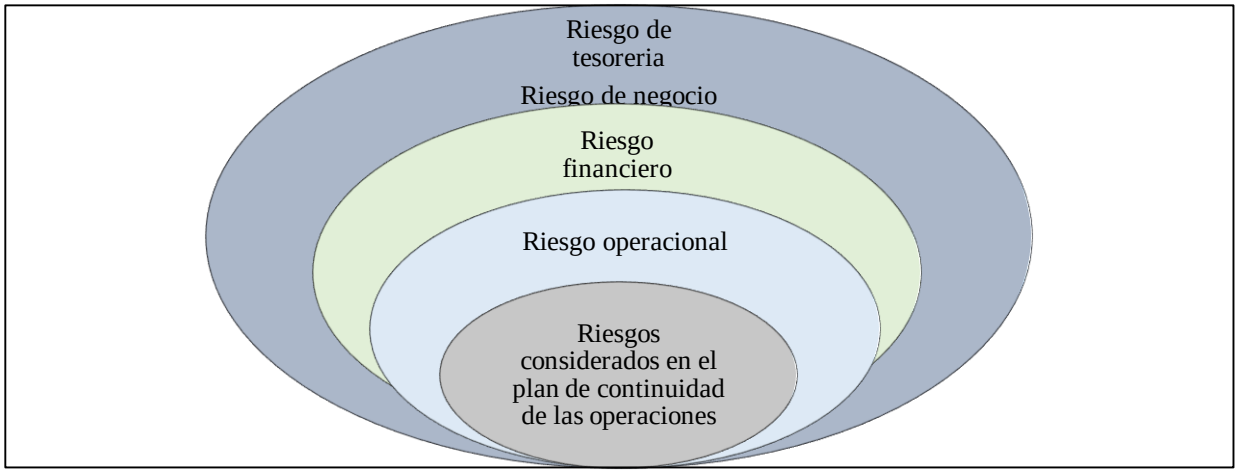

Figura 19. Riesgos de tesorería percibidos. Fuente: Elaboración propia con base en Storkey (2011).

Así mismo, señala que los riesgos operacionales que afectan a la tesorería destacan por: fallas de infraestructura y tecnología relacionadas con sistemas informáticos, energía, telecomunicaciones, datos y registros físicos; incidentes de imposibilidad de acceso a las instalaciones, ya sea por inaccesibilidad o daño de las instalaciones; dependencia de otros proveedores de servicios clave, como el banco central o bancos comerciales, proveedores de telecomunicaciones, servicios de Internet y otras operaciones de tercer término, o fallas de recursos debidas a incidentes como las pandemias; errores o fallas humanas debidas a falta de recursos, conocimientos, capacitación, políticas, procedimientos, delegaciones, códigos de conducta y deficiencias en la gestión; y la incumplimiento de obligaciones reglamentarias, jurídicas o contractuales, laborales o de otro tipo, incluidos los objetivos de la gerencia y la obligación de

declaración de información. Así mismo, señala que los planes de continuidad de las operaciones deben ser una parte integrante del marco de gestión del riesgo operacional de tesorería.

Bajo el mismo orden de ideas, Magnusson, Prasad, & Storkey (2010) señalan que la formulación de un marco de gestión de riesgos operacionales, puede ser un proceso que implique una inversión de tiempo y esfuerzo, no sólo para determinar y comprender los riesgos, sino también, para formular técnicas de mitigación en un entorno de cambio constante. No obstante, subrayan que el marco puede desarrollarse y aplicarse de manera escalonada, a medida que mejoren las técnicas y el personal de tesorería comprenda mejor los riesgos y las técnicas de mitigación. Para que el marco tenga éxito, es sumamente importante desarrollar una cultura de consciencia del riesgo en todos los aspectos de tesorería y cerciorarse de que todo el personal participe en la formulación y la aplicación del marco.

En la primera etapa de desarrollo del marco, se detalla que la alta gerencia debe comprender y transmitir al personal la importancia asignada a la gestión del riesgo operacional y la necesidad de que el personal participe y coopere constantemente. Así mismo, cada gerente de departamento tiene que responsabilizarse de la gestión del riesgo operativo en el ámbito que le corresponda. El responsable impulsa y guía el proceso en toda la tesorería, coordina la declaración de datos al tesorero y a la alta gerencia, y formula las políticas y los procedimientos de la gestión de riesgos operacionales adecuados y el entorno de control. Además, la gestión del riesgo operacional debe ser una responsabilidad que todo el personal de tesorería debe compartir y comprender. Los altos funcionarios deben encargarse de detectar y monitorear los riesgos en sus respectivas unidades y de garantizar que las actividades de control funcionen de la manera prevista y conforme a las prioridades fijadas por el tesorero.

Riesgo operacional aplicado al SPEI. El Banco de México publica los reglamentos aplicables al Sistema de Pagos Electrónicos Interbancarios (DOF, 2017a), dentro de los cuales destacan requisitos aplicables para la gestión del riesgo operacional. En primera instancia, el interesado debe contar con políticas y procedimientos documentados que incluyen; una metodología para la administración del riesgo operacional relacionada con la operación con el SPEI que tenga en consideración la identificación, evaluación, monitoreo y mitigación de los riesgos identificados, así como los roles y responsabilidades definidos para su ejecución, revisión y actualización; una metodología para el análisis de impactos al negocio; procedimientos de contratación y capacitación del personal para asegurar que aquel relacionado con la operación con el SPEI, cuente con las habilidades, competencias y conocimientos requeridos para el puesto que desempeña; y, manuales de procedimientos y de operación que describan las actividades requeridas para realizar su operación con el SPEI y el personal responsable de la ejecución de dichas actividades de forma que se asegure que exista una segregación de funciones en los procesos críticos que se realicen para la operación del SPEI y una definición precisa de responsabilidades.

Así mismo, el interesado debe establecer medidas de mitigación de los riesgos, tales como: contar con un listado de los riesgos operacionales identificados, que indique la clasificación del riesgo y el resultado de su evaluación, así como los controles asociados para la operación con el SPEI, incluyendo los tecnológicos y aquellos asociados a proveedores externos; contar con un análisis de capacidad sobre los recursos tecnológicos, humanos y materiales dispuestos para la operación con el SPEI para asegurar que cuente con los recursos suficientes para manejar volúmenes altos de operación y cumplir con sus objetivos de nivel de servicio; y, contar con políticas y lineamientos para la gestión de privilegios de acceso físico a los sitios operativos desde

donde se realiza la operación con el SPEI y a los centros de datos que alojan a la Infraestructura Tecnológica dispuesta para operar con el SPEI.

Además, establece procedimientos que deben seguir para la recuperación y restauración de la operación con el SPEI que incluyan: una política de continuidad, así como estrategias y procedimientos que deberá seguir; acciones que debe seguir para la atención de incidentes que causen una afectación en la operación normal con el SPEI que contemple las fases de identificación, diagnóstico, atención, recuperación, restauración y documentación e indique los roles y responsabilidades correspondientes; actividades que debe realizar para dar respuesta a emergencias ante la ocurrencia de algún incidente que afecte la operación normal con el SPEI; las acciones que deberá seguir para el restablecimiento de la operación normal; y, un plan de pruebas al que deberá dar seguimiento para evaluar las estrategias y procedimientos de continuidad implementados relacionados con la operación con el SPEI indicando los lineamientos, tipo de pruebas a realizar y periodicidad de las mismas

4.2.4. Implicaciones para bancos y sistemas bancarios. Muchos de los hallazgos y observaciones del Comité de Basilea se basan en escenarios que enmarcaron las nuevas tecnologías y modelos de negocios financieros innovadores (Tabla 4). No obstante, la naturaleza y el alcance de los riesgos bancarios puede cambiar significativamente con el tiempo en la creciente adopción de entidades *Fintech*, en forma de nuevas tecnologías que pueden afectar los modelos de negocios bancarios. Si bien, estos desarrollos pueden generar riesgos nuevos y adicionales, también pueden abrir nuevas oportunidades para los consumidores y los bancos (Basilea, 2018).

Tabla 4

Lista de riesgos y oportunidades que emanan de las tecnologías financieras y la innovación.

	Riesgos	Oportunidades
Impacto en el sector de consumo	• Privacidad de datos. • Seguridad de datos. • Discontinuidad de los servicios bancarios. • Prácticas de marketing inapropiadas.	• Inclusión financiera. • Servicios bancarios mejores y más personalizados. • Menores costos de transacción y servicios bancarios más rápidos.
Impacto en los bancos y sistemas bancarios	• Riesgos estratégicos y de rentabilidad. • Riesgo cibernético. • Aumento de la interconexión entre partes financieras. • Alto riesgo operacional - sistémico • Alto riesgo operacional – idiosincrásico. • Riesgo de gestión de terceros / proveedores. • Riesgo de cumplimiento que incluye la falta de protección de los consumidores y la regulación de la protección de datos. • Lavado de dinero - riesgo de financiamiento al terrorismo • Riesgo de liquidez y volatilidad de las fuentes de financiación bancaria.	• Uso innovador de los datos para fines de marketing y gestión de riesgos. • Mejores procesos bancarios y más eficientes. • Posible impacto positivo en la estabilidad financiera debido al aumento de la competencia • *Regtech.*

Fuente. Elaboración propia con base en Basilea (2018).

Por esa razón, el Comité de Basilea señala que los supervisores bancarios deben permanecer enfocados en garantizar la seguridad y solidez del sistema bancario, deben estar atentos a las oportunidades para mejorar tanto la seguridad como la solidez y la estabilidad financiera, al mismo tiempo que monitorean las prácticas actuales que pueden obstaculizar indebidamente o no las innovaciones beneficiosas en la industria financiera.

Así mismo, sostiene que las innovaciones *Fintech* tienen beneficios potenciales para todos los usuarios de servicios financieros. Estos incluyen; expandir el acceso a los servicios financieros (inclusión financiera), llegar a los consumidores mal atendidos, reducir los costos de transacción, brindar mayor transparencia con productos más simples y revelaciones de costos claras, brindar mayor conveniencia y eficiencia, y permitir controles más estrictos sobre el gasto y sus presupuestos. En conjunto, esto puede resultar en una mejor experiencia para el cliente al proporcionar una mejor comprensión de los productos y términos. Algunas oportunidades importantes a considerar incluyen:

- Inclusión financiera. La financiación digital ha mejorado el acceso a los servicios financieros por parte de los grupos que carecen de servicios, puesto que la tecnología puede llegar a los lugares más remotos. Por lo tanto, los servicios financieros pueden proporcionarse a más personas con mayor rapidez, responsabilidad y eficiencia.
- Servicios bancarios mejores y más personalizados. Las entidades de *Fintech* podrían ayudar a la industria bancaria a mejorar sus ofertas tradicionales.
- Costos de transacción más bajos y servicios bancarios más rápidos. Las innovaciones de las entidades *Fintec*h pueden acelerar las transferencias y los pagos y reducir sus costos.
- Procesos bancarios mejorados y más eficientes. La innovación puede permitir la realización de operaciones en un entorno más seguro, gracias al uso de tecnologías criptográficas o biométricas y sistemas más interoperables que disminuyen las posibilidades de fracaso.
- Posible impacto positivo en la estabilidad financiera debido al aumento de la competencia. La entrada de nuevas entidades que compiten con los bancos tradicionales podría eventualmente fragmentar el mercado de servicios bancarios y reducir el riesgo sistémico asociado con entidades de tamaño sistémico, como también lo analiza el FSB.

- *Regtech*. *Fintech* podría utilizarse para mejorar los procesos de cumplimiento en las instituciones financieras.

4.3. Estudio de Caso del Ataque a SPEI Banxico en el 2018

Los ataques cibernéticos representan movimientos económicos, sociales o políticas, y se llevan a cabo principalmente a través de Internet. Los ataques son dirigidos al público en general, a organizaciones privadas o países. El Banco Mundial (BM, 2016) señala que la falta de fronteras del acceso no autorizado y la complejidad y diversidad de las amenazas que tienen como fin el acceso ilegal a la información, han escalado. Y, aunque la mayoría de las instituciones gubernamentales y grandes corporaciones han desarrollado herramientas individuales para mantener la seguridad de la información, los objetivos de los ataques se han ampliado e incluyen, además de las instituciones de gobierno: infraestructura crítica, industrias y empresas específicas, lo que requiere contramedidas más fuertes. Los siguientes apartados, muestran el análisis descriptivo realizado del ataque al SPEI de Banxico en el 2018, así como la Figura 20 presenta la red semántica del análisis realizado en el software Atlas.ti.

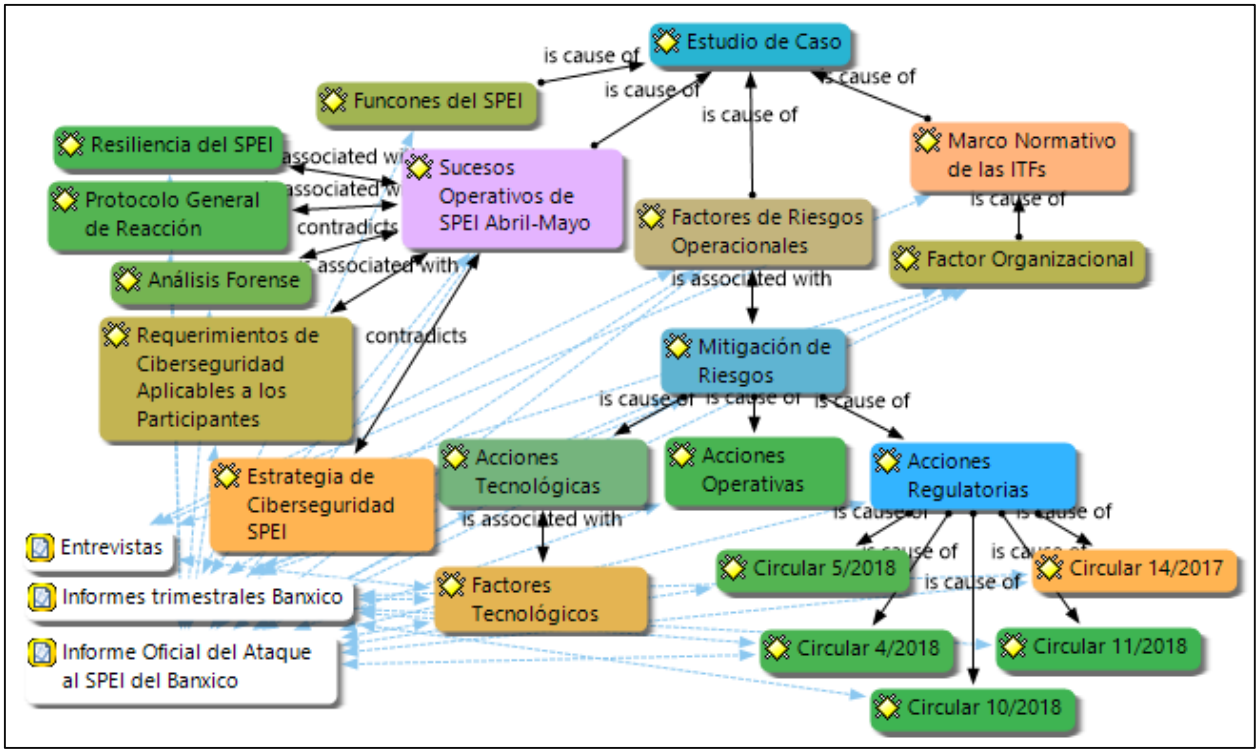

Figura 20. Red semántica del estudio de caso. Fuente: Elaboración propia.

4.3.1. Funcionalidad del SPEI. El Sistema de Pagos Electrónicos Interbancarios (SPEI) es la infraestructura de pagos del Banco de México, creado para permitir a las instituciones financieras participantes, enviar y recibir transferencias de fondos en moneda nacional entre sí. Este sistema se puede describir como un camino central en la que se concentran los participantes, en el que se cargan y abonan las cuentas de los participantes con Banxico, con el fin de liquidar las operaciones que realizan entre sí, ya sea que hayan sido enviadas por cuenta propia o por cuenta de sus clientes. Así mismo, el sistema opera las 24 horas del día, los 365 días al año lo que permite que las instituciones financieras que participan en él, puedan brindar a usuarios finales servicios de transferencia electrónica en tiempo real (Banxico, 2018a).

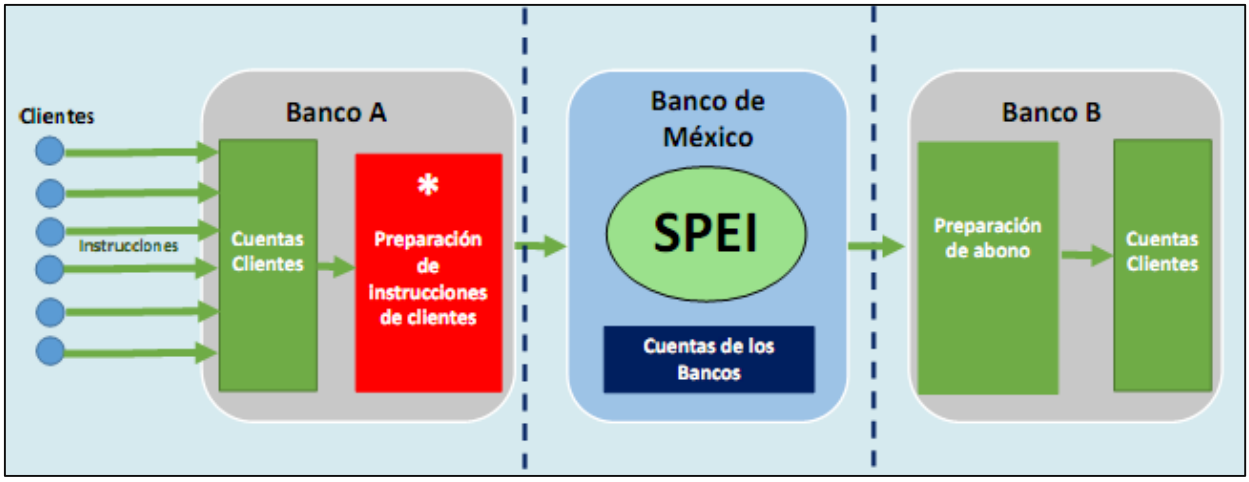

Figura 21. Funcionamiento del SPEI. Fuente Banxico (2018a, p. 50).

Así mismo, para realizar una transferencia de fondos a través del SPEI (Figura 21), es necesario, en primera instancia, que el cliente final incluya -desde su banca electrónica o aplicación móvil- a su institución participante los pagos que desea realizar, para que el participante pueda validar los elementos de seguridad de la institución y guardar la evidencia, y proceder con la preparación de instrucciones de sus clientes, incluyendo elementos de seguridad adicionales, en los que únicamente ellos tienen el control, para posteriormente enviarlos al SPEI de Banxico Posteriormente Banxico, verifica las firmas electrónicas de los participantes, y procede a su procesamiento y posterior liquidación al participante receptor del pago, y por último, se les informa a los participantes de la liquidación, y el participante receptor del pago, acredita los fondos en la cuenta de su cliente y envía al Banxico la información para generar un Comprobante Electrónico de Pago (CEP) (Banxico, 2018a).

4.3.2. Sucesos operativos del SPEI en el periodo entre abril y mayo del 2018. El 17 de abril un participante del Sistema de Pagos Interbancarios (SPEI) registra un ataque cibernético. Es a partir de esta fecha que se identifican cuatro eventos adicionales. Dichos ataques se presentaron en los aplicativos que utilizan los participantes afectados para preparar órdenes de transferencia de

fondos y conectarse al SPEI, los cuales se encontraban enfocados en diversos elementos que componen dichos aplicativos y en la infraestructura de cómputo y telecomunicaciones de los participantes. A pesar de lo anterior, Banxico y el sistema central del SPEI no fue objeto de ataques, por lo que el SPEI, de forma segura, continuó procesando normalmente órdenes de transferencias electrónicas entre los participantes, y sólo en algunos casos, con mayores tiempos de procesamiento, la Figura 22 muestra un diagrama de flujo de envío y recepción de transferencia de fondos a través del SPEI (Banxico, 2018b).

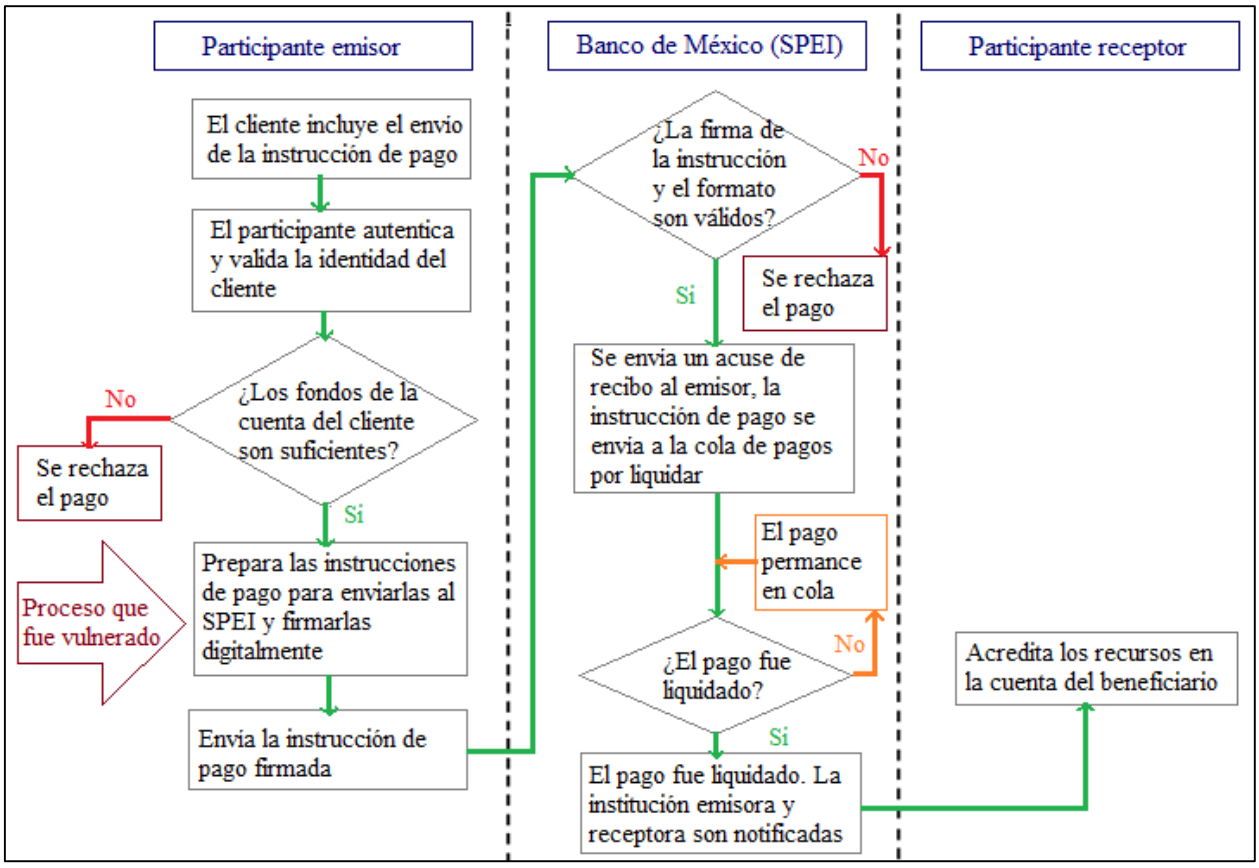

Figura 22. Diagrama de flujo de una transferencia de fondos a través de SPEI. Fuente: Banxico (2018b, p. 6).

El ataque consistió en la elaboración o implementación de órdenes de transferencia falsas en los sistemas de los participantes donde se procesan las instrucciones de pago de los participantes afectados. Los atacantes quebrantan la infraestructura tecnológica de los participantes y generan en sus sistemas órdenes de transferencias ilegales, con cargo a las cuentas de los participantes, en alguna etapa del proceso previa a su conexión al SPEI.

Las órdenes de transferencias siempre incluyen el número de la cuenta emisora y de la receptora. En el caso de las que se generaron de forma ilegal, los números de las cuentas emisoras fueron inventaron, por lo que no correspondían a cuentas de clientes, mientras que las cuentas receptoras eran reales. La introducción de estas órdenes de transferencia fue realizada en una etapa del proceso ejecutada en los sistemas de los participantes que no contaban con controles para asegurar que dichas órdenes fuesen ilegales.

Los sistemas de los participantes atacados, firmaron y enviaron al SPEI las órdenes de transferencias ilegales, validadas como si fueran legales. El SPEI, al recibir las órdenes de transferencias, revisa que estén firmadas por los participantes, las procesa y abona el monto respectivo en la cuenta que le lleva al participante receptor. El participante receptor, una vez que recibe del SPEI la confirmación de la liquidación, realiza el correspondiente abono en la cuenta que este le lleva a su cliente receptor (en este caso, la cuenta especificada en la orden de transferencia de pago ilegal). Y, finalmente, los recursos ilegales son retirados mediante disposiciones de efectivo.

Posteriormente, los participantes afectados se percatan de las instrucciones de pago ilegales por dos vías, la primera de ellas, mediante alertas internas producto de sus procesos de validación de operaciones; y, posteriormente, por medio de alertas por parte de otros participantes receptores de operaciones sospechosas.

Debido a estos mecanismos de alerta, algunas de las transacciones identificadas fueron detenidas por los participantes receptores, con lo que se evitó la disposición indebida de parte de los recursos de procedencia fraudulenta. Los recursos de los clientes no estuvieron en riesgo, puesto que los atacantes buscaron vulnerar las conexiones de las instituciones con el SPEI, lo cual involucro únicamente recursos de la institución afectada. No obstante, la afectación a los clientes fue la retención de los pagos para aquellas transacciones en las que participa alguna institución afectada o que opera bajo el esquema alterno para enviar órdenes de pago a través del SPEI.

Con forme a los sucesos anteriormente descritos, Banxico realiza una serie de medidas para contener posibles daños procedentes de esos ataques sobre los participantes que fueron afectados, así como en el sistema de pagos en general. Dichas medidas contemplan, en primer lugar, la migración a una plataforma de operación contingente, a los participantes afectados y con un mayor perfil de riesgo; la implementación de alertas en el SPEI central para detectar anomalías en los mensajes de pago y la implementación de controles adicionales en los aplicativos que proveen los servicios de conexión al SPEI a los participantes; y, por último, la emisión de regulaciones para proporcionar medidas de control (Banxico, 2018d).

Protocolo General de Reacción. En cada caso de evento relacionado con ciberseguridad, se aplica un protocolo que implica la desconexión de la institución atacada y el inicio de operación a través de esquemas de contingencia. Para estos fines, Banxico cuenta con un esquema de conexión paralelo de operación alterna para hacer transacciones en el SPEI (COAS), este es un procedimiento semiautomático, que permite a los participantes operar desde una plataforma distinta y por lo tanto, más segura.

Una vez identificados los casos de ataques a alguna institución, se identifican elementos de riesgo que pueden resultar comunes a otros participantes. Y, con base en esta información, se emite

un comunicado avisando a aquellos participantes en los que se identificó un mayor riesgo que tendrían que conectarse al SPEI a través del COAS desde sus instalaciones en una fecha futura. La operación a través del esquema de contingencia reduce los riesgos al tratarse de una infraestructura distinta a la que se ha visto afectada.

Resiliencia del SPEI. Pese a los ataques, el SPEI se continúa brindando servicios de manera segura y procesando grandes cantidades de pagos, así mismo, sigue procesando órdenes de transferencia electrónicas entre los participantes de forma segura, y en algunos casos con retrasos en los tiempos de servicio. De igual forma, los participantes que fueron afectados, recuperaron el nivel de operación en el SPEI una vez que se establecieron sus procesos de contingencia.

Análisis forense. El análisis forense declara que el objetivo del ataque fue generar transferencias electrónicas de fondos hacia cuentas bancarias específicas, con el fin de sustraer ilegalmente recursos monetarios. De esta manera, se destaca, que no se trata de un ataque al sistema central del SPEI operado por Banxico, ni a alguna infraestructura del mismo, sino que fue un ataque en el que se comprometieron elementos de los sistemas de las instituciones financieras vulneradas, además de que estuvo dirigido particularmente a vulnerar los sistemas para generar y enviar órdenes de transferencias de fondos.

Para ello, los atacantes se aprovecharon de las funcionalidades y el procesamiento libre del SPEI, de tal manera que la transmisión automatizada de las órdenes ilegales de transferencias se pudiera llevar a cabo antes de que pudieran detectarlas a tiempo las instituciones financieras de donde estas se originaron. En consecuencia, el ataque no tuvo como propósito volver inoperante al SPEI o penetrar las defensas de Banxico.

El análisis forense concluye que la forma de operar requiere contar, por parte de los atacantes, de un conocimiento profundo de la infraestructura tecnológica y de los procesos de las

instituciones vulneradas, así como del acceso a ellas. Así mismo, señala que se utilizaron técnicas comunes como robo de credenciales, escalamiento de privilegios, movimientos laterales entre servidores, inserción de archivos o ejecución de instrucciones y borrado de bitácoras.

Requerimientos de Ciberseguridad Aplicables a los Participantes. Entre los requerimientos que destacan, se encuentran aquellos relacionados con la seguridad de los aplicativos de la conexión SPEI y con el esquema de operación alterna COAS, tales como:

- Contar con procedimientos para evaluar los protocolos de comunicación utilizados en la infraestructura tecnológica;
- Contar con procedimientos que permitan administrar las vulnerabilidades de seguridad informática;
- Contar con procedimientos para detectar y gestionar incidentes de seguridad informática en la infraestructura tecnológica;
- Contar con procedimientos que aseguren que los componentes que brindan seguridad a sus sistemas informáticos se encuentren vigentes;
- Requerimientos relacionados con la seguridad de los aplicativos de conexión al SPEI y con el esquema de operación alterna COAS:
  - Contar con procedimientos que permitan vigilar, auditar y rastrear todas las operaciones realizadas por los sistemas informáticos;
  - Contar con procedimientos de contratación y capacitación del personal para asegurar que aquel relacionado con la operación con el SPEI, cuente con las habilidades, competencias y conocimientos requeridos para el puesto que desempeña; y

- Acreditar que pueden continuar con su operación ante la activación del "Procedimiento de Operación Alterno SPEI" (POA-SPEI), así como operar mediante el procedimiento de contingencia denominado "Cliente de Operación Alterno SPEI" (COA-SPEI).

Es importante mencionar que el Banco de México, a partir de entonces, intensifica sus procesos de supervisión en esta materia.

Estrategia de Ciberseguridad del SPEI. El Banco de México adopta varias medidas para fortalecer la ciberseguridad de los sistemas de pagos, en particular del SPEI. Estas medidas contemplan tareas y acciones implementadas, tanto al interior de Banxico, como las que son requeridas a los Participantes del SPEI (Banxico, 2018c). Las medidas de acción al interior del Banco de México contemplan las revisiones periódicas de códigos y su funcionalidad; esquemas de desarrollo seguro de software; actualizaciones periódicas de la infraestructura conforme a mejores prácticas internacionales; pruebas de penetración; auditorías internas y externas; protocolos de desconexión ante eventos de ciberseguridad. Mientras que en lo que se refiere a continuidad de operaciones, las medidas necesarias se refieren a la obligación de contar con una versión del SPEI que sea ejecutada en un sistema operativo diferente a aquel en el que opera cotidianamente, además de contar con esquemas de operación de alta disponibilidad, así como, contar con un cliente de operación alterno (COAS).

En tanto que las medidas y acciones establecidas por Banxico para los participantes, se establece la emisión de regulaciones en temas de ciberseguridad y continuidad operativa y la supervisión continúa del cumplimiento de las mencionadas regulaciones. Así mismo, en referencia a continuidad de operaciones, las medidas establecidas se enfocan a contar con; planes de recuperación de desastres; contar con centros de cómputo alternos y enlaces de telecomunicaciones; y por último, certificaciones para su operación en COAS.

4.3.3. Factores de Riesgos Operacionales. El Consejo de Estabilidad del Sistema Financiero acuerda una serie de principios, con la finalidad de incorporar las mejores prácticas y recomendaciones internacionales. Al respecto, el Banco de México emite disposiciones para fortalecer los procesos que realizan las instituciones financieras y establecer requerimientos a los participantes del SPEI en materia de seguridad de la información (Banxico, 2018b).

Mitigación de riesgos. Con el propósito de continuar propiciando el buen funcionamiento del SPEI, el Banco de México considera necesario reforzar las medidas adoptadas para mitigar riesgos los riesgos operacionales que pudieran estar relacionados con el manejo de recursos provenientes de transferencias de fondos derivados de las cuentas de clientes que implicaban mayores riesgos, como las que se muestran a continuación (Banxico, 2017a).

Acciones operativas. Se solicita a los participantes cuyos aplicativos e infraestructura de cómputo para conectarse al SPEI resultaron afectados, tomar medidas para renovar los elementos de seguridad de sus operadores, para autenticarse en los sistemas de pagos operados por Banxico, al tiempo que el Instituto Central aplica y fortalece el esquema de soporte a todos los participantes del sistema, además, Banxico refuerza el monitoreo de su infraestructura y sistemas para detectar cualquier comportamiento anómalo (Banxico, 2018b).

Acciones tecnológicas. Se destaca a los participantes en los que se detectaron los incidentes, mismos que debían operar por vías alternas y mantener su capacidad para enviar órdenes de transferencia a la infraestructura del SPEI; se establecen alertas en el SPEI para detectar algunas anomalías en los mensajes; se mantuvo un soporte técnico reforzado las 24 horas del día para los participantes; se exige a los proveedores de servicios de conexión al SPEI que incorporarán controles adicionales en sus aplicativos; por último, se solicita a los participantes hacer un análisis profundo de sus infraestructuras para detectar algún software durmiente (Banxico, 2018b).

Al respecto, el Banco de México sostiene que, el uso creciente de tecnologías digitales, así como el grado elevado de interconexión entre instituciones financieras han propiciado que el sistema financiero se haya convertido en un sector particularmente vulnerable a este tipo de ataques. Además, sostiene que los costos potenciales de los ataques cibernéticos son aquellos que derivan de afectar la estabilidad financiera, puesto que un ataque cibernético que logra afectar el desempeño de las infraestructuras financieras pude comprometer el buen funcionamiento de los sistemas de pagos o propagarse a través de todo el sistema financiero. Tomando en cuenta que el sistema de pagos permite la liquidación eficiente de un gran número de transacciones en la economía, ataques cibernéticos que afecten su funcionamiento podrían tener un impacto importante en la actividad económica, por tal motivo, es indispensable establecer las acciones tecnológicas mencionadas anteriormente (Banxico, 2018d).

Acciones regulatorias. El Banco de México emite disposiciones presentadas en la Circular 4/2018 y Circular 5/2018, las cuales otorgan a las instituciones de crédito y demás entidades que prestan el servicio de transferencias de fondos, espacio para que éstas puedan implementar medidas de control adicionales y encaminadas a fortalecer sus sistemas de detección de transferencias irregulares, así como, verificar la integridad de sus operaciones y evitar posibles afectaciones a dichas instituciones, al resto de los participantes y al sistema en su conjunto (DOF, 2018b; DOF, 2018c).

Circular 4/2018. Se establece un plazo fijo de un día para la entrega en efectivo o cheque de caja de recursos provenientes de transferencias de fondos por montos iguales o superiores a 50 mil pesos. Adicionalmente, se impone para todas las entidades que participaron en sistemas de transferencias de fondos ejecutadas el mismo día en que se generó su instrucción, la obligación de que los recursos de una transferencia de fondos enviada por otra entidad mediante dichos sistemas

o de un traspaso entre cuentas abiertas en la misma entidad fuesen entregados, en efectivo o cheque de caja, por montos iguales o superiores a $50,000 únicamente al día hábil siguiente, a aquel en que se haya recibido la transferencia o traspaso respectivo (DOF, 2018b).

Esta obligación, es únicamente aplicable para el retiro de los recursos de transferencias de fondos que el cliente solicitó en efectivo o cheque de caja, por lo que no afecto la disposición, en ese mismo día, de la totalidad o parte de esos recursos que el cliente puede hacer por otros medios.

Circular 5/2018. Esta disposición establece que para que los participantes en el SPEI pudieran obtener autorizaciones temporales, que el Instituto Central otorga después de analizar caso por caso, con el fin de que, durante la vigencia de dichas autorizaciones, puedan acreditar en las cuentas de los beneficiarios los recursos de las transferencias de fondos que recibieran por montos iguales o superiores a $50,000.00, hasta que se realizaran validaciones específicas sobre su legitimidad. La vigencia de las autorizaciones fue por periodos determinados por el Banco de México, los cuales no podían ser superiores a los seis meses, durante los cuales, los participantes autorizados tenian que desarrollar sistemas para que pudieran llevar a cabo las validaciones indicadas, de manera automatizada, en los periodos establecidos en la regulación (DOF, 2018c).

En ningún caso, los periodos de tiempo solicitados para llevar a cabo las validaciones referidas podían extender del mismo día de operación del SPEI en que el participante recibiera una transferencia de fondos. Así mismo, los participantes que obtuvieron la autorización debían comunicarlo a su clientela.

Circular 10/2018 y Circular 11/2018. En adición a las disposiciones mencionadas en el párrafo anterior, las Circulares 10/2018 y 11/2018 establecen requerimientos para robustecer los elementos de seguridad en la prestación de servicios de transferencias de fondos a aquellos clientes que ofrecen el intercambio o compraventa de activos virtuales. (DOF, 2018d; DOF, 2017b).

Entre estos requisitos se incluyen, en primera instancia, la identificación las cuentas pertenecientes a este tipo de clientes para poder implementar validaciones adicionales, previo a la acreditación de recursos provenientes de transferencias a través del SPEI; el abono de los recursos que recibieron al día hábil siguiente al de su recepción, y en el tiempo en el que no se contaban con la autorización del Banco de México para llevar a cabo en plazos distintos las validaciones; abstenerse de poner a disposición de este tipo de clientes los recursos que recibían el mismo día de su recepción, en aquellos casos en que el Banco de México emitió avisos ante posibles ataques; las cuentas que los participantes del SPEI llevaron a este tipo de empresas debían ser cuentas de depósito de dinero a la vista, abiertas únicamente en aquellas instituciones financieras facultadas para ofrecerlas; y abstenerse de proveer cuentas a estas empresas con la finalidad de que estas fueran, a su vez, asignadas a clientes para la transferencia de recursos destinados a la compra de activos virtuales.

Asimismo, en las Circulares 10/2018 y 11/2018 se establecen los requisitos sobre políticas y procedimientos adicionales que debían de seguir los participantes del SPEI, que incluyeron requisitos como; seguir los protocolos de acción establecidos por el Banco de México para hacer frente a posibles ataques; contar con protocolos y procedimientos que documenten las acciones a tomar en caso que se materialicen riesgos de ciberseguridad que pudieran afectar la operación del participante en el SPEI; el establecimiento e implementación de pruebas de confianza e integridad a su personal y a terceros que tengan acceso a información y sistemas relevantes en su operación con el SPEI; y la designación a un oficial de seguridad de la información responsable de las políticas de riesgos de ciberseguridad y la implementación de medidas correctivas ante la materialización de estos riesgos que pudiese afectar la operación del participante con el SPEI (DOF, 2018d; DOF, 2017b).

Circular 14/2017. Todas las instituciones financieras participantes en el SPEI debían cumplir con las obligaciones de administración de riesgos operacionales establecidas en la presente circular, las cuales incluyen una metodología para la administración del riesgo operacional relacionada con la operación con el SPEI, la cual debe de considerar la identificación, evaluación, monitoreo y mitigación de los riesgos identificados, así como los roles y responsabilidades definidos para su ejecución; una metodología para el análisis de impactos al negocio; procedimientos de contratación y capacitación del personal para asegurar que aquel relacionado con la operación con el SPEI, cuentera con las habilidades, competencias y conocimientos requeridos para el puesto a desempeñar; y manuales de procedimientos y de operación que describan las actividades requeridas para realizar su operación con el SPEI y el personal responsable de la ejecución de dichas actividades (DOF, 2017a).

4.3.4. Marco Normativo de las ITFs. En la entrevista el Director de Desarrollo Regulatorio, el Lic. Luis Leyva Martínez, señala que el ataque al SPEI del Banco de México, implica riesgos que se deben atender desde la regulación del Banco de México, que si bien, en este momento se está fortaleciendo, es decir, en este momento está en consulta pública o si no es que ya la publicaron. Señala además, que lo que se realiza por el Banco de México es fortalecer justo ese nodo, el tema de las conexiones al SPEI, es decir, qué características deben tener los proveedores que se conectan al SPEI, qué elementos de seguridad debe de contemplar, la forma de mitigar y contener los riesgos cibernéticos, etc., en otras palabras, esas medidas serían aplicable directamente a las Instituciones de Tecnología Financiera. No obstante, en este momento se está trabajando en dosificando la regulación poco a poco, ya que no es un ejercicio que se tiene que ir calibrando con mucho cuidado.

Factores Organizacionales. En la entrevista con el Lic. Luis Leyva Martínez, señala que cuando se empieza a conocer a las entidades *Fintech,* se puede observar que los recursos con los que cuenta son pocos. Además, en su experiencia ha ido detectando que algunas tienen buenos estándares de seguridad, algunas han contratado proveedores para robustecer su marco de administración de riesgos tecnológico, algunas otras tienen ya una separación de sus áreas, las más grandes han establecido estándares con base en líneas de defensa, han implementado mecanismos de identificación del usuario, es decir, la propia industria ha ido avanzando poco a poco.

Así mismo, sostiene que normalmente las entidades *Fintech* son muy ligeras en cuanta costos, porque están basados ampliamente en tecnología, ellos experimentan pérdidas durante varios años hasta llegar el punto de equilibrio, les cuesta trabajo, y en la experiencia del Lic. Luis Leyva no ha visto a alguna que llegue al equilibrio antes de los 3, 4 años; de manera que son entidades que si bien son ligeritas en cuanto a costos, son entidades que traen modelos nuevos y demás, y en lo que se ubican en el mercado, en lo que adquieren una posición en el mercado se tardan un poco de tiempo, y además, ahora tienes que agregar el costo regulatorio que implica tener que cumplir con la Ley.

Así mismo, cuando a la Comisión le tocó entrar en el proceso del diseño de la regulación, es decir, cuando se estaba diseñando la Ley, lo que se trataba de hacer no era necesariamente generar regulaciones que fuesen prohibitivas o cosas que les generaran cosos exorbitantes, pero si lo se trataba de hacer es que una vez de que deban entrar en el terreno regulatorio, una vez de que se vuelven entidad financieras, porque en realidad eso son, a quien se tiene que tutelar es al público inversionista, y en ese sentido es que la atención está puesta ahí, y en este sentido de que se deben establecer requisitos regulatorios que lo que buscan es proteger a los inversionistas a través de mecanismos de transparencia, a través de mecanismos de buenos procesos, a través de buenos

sistemas de control interno, de administración de riesgos, que generen entidades que no sean autorizadas un día, y al día siguiente ya estén en problemas, es por eso que se debe tener mucho cuidado de que las entidades que van a entrar, sean entidades que ya estén en el terreno de revisar actividades que son reguladas, que están tomando recursos del público, y como tal, amerita tener un grado de seriedad en cuanto a institucionalización.

Menciona además, que la Ley en este momento les concede a las *Fintech* un plazo transitorio para acudir a la Comisión y obtener la autorización, de manera que en este momento, no existe un plazo de estar supervisando, más bien se está formando las prácticas de supervisión, se está elaborando toda la infraestructura para recibirlas, esto tiene que ver con preparar la supervisión, los procesos de autorización, además de seguir emitiendo la regulación secundaria necesaria para que cuando entren en vigor al solicitar su autorización y empiecen a operar, ya operen con un marco legal completo, la Ley *Fintech* sólo establece un marco general, pero ha dado muchas facultades para incluir dentro de las Disposiciones de Carácter General aspectos ya más técnicos.

4.4. Propuesta de Estrategia Integral de Riesgos Operacionales para entidades *Fintech*

A continuación se propone una estrategia integral de riesgos operacionales para su aplicación a entidades *Fintech* de México. Con la intención de que la mencionada estrategia cuente con el compromiso y deber por parte de las autoridades de la entidad *Fintech*. La estrategia que se propone busca englobar las actividades para la implementación y mejora continua del proceso de gestión de riesgos operacionales. El marco normativo de mejores prácticas internacionales ha recomendado que las entidades que realizan actividades bancarias, desarrollen, implementen y mejoren continuamente un marco de trabajo o estructura de apoyo, y cuyas intenciones son integrar el proceso de gestión de riesgos en el gobierno corporativo de la entidad, planificación y estrategia,

procesos de información, políticas, valores y cultura. Con base a lo anterior, se describe la estrategia integral que se propone (Figura 23).

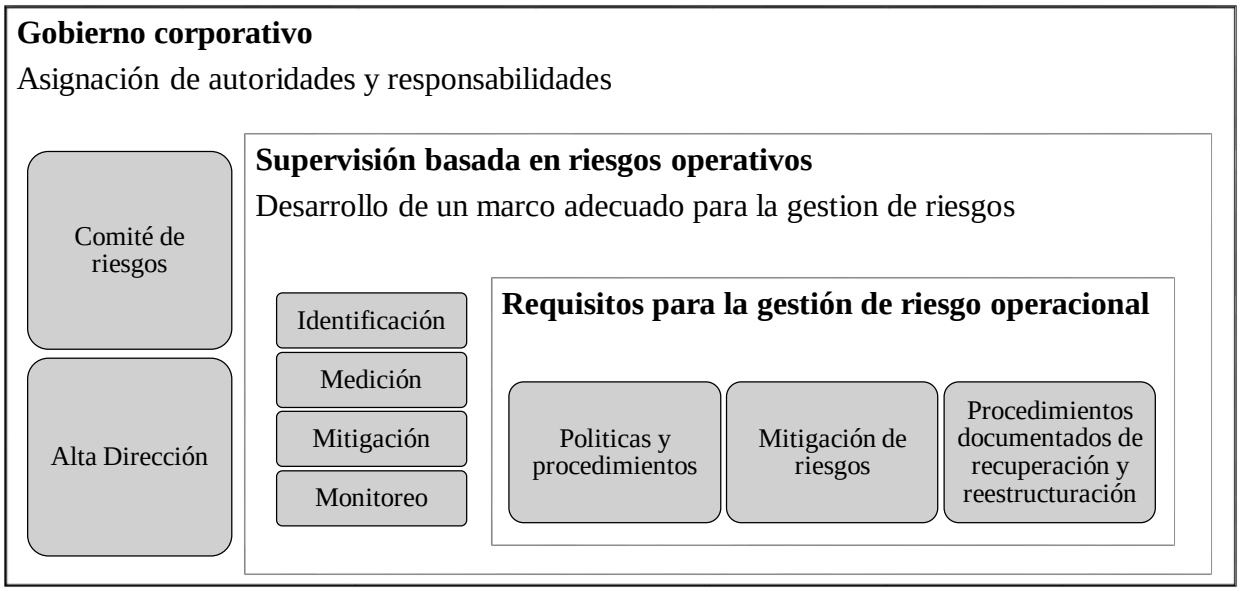

Figura 23. Propuesta de estrategia integral de riesgos operacionaes en entidades Fintech. Fuente: Elaboración propia.

4.4.1. Gobierno corporativo en entidades *Fintech*. Se propone la creación de un Gobierno Corporativo, basado en los principios de Basilea III, que tome en cuenta la asignación de autoridades y responsabilidades a un Comité de Riesgos y a la Alta Dirección, quienes lleven a cabo procesos de supervisión en la entidad *Fintech*. Así mismo, se propone que su aplicación sea acorde al tamaño, complejidad, estructura, relevancia económica, perfil de riesgo operacional y modelo de negocio de la entidad *Fintech*, ya sea, en la figura de una *institución de financiamiento colectivo* o *instituciones de fondo de pago electrónico*, mismas que establece la Ley ITF, y, que tenga la finalidad salvaguardar el interés de las partes que pueden resultar afectadas y de forma sostenible. La Figura 24, presenta los elementos a considerar por un Gobierno Corporativo enfocado a las entidades *Fintech*.

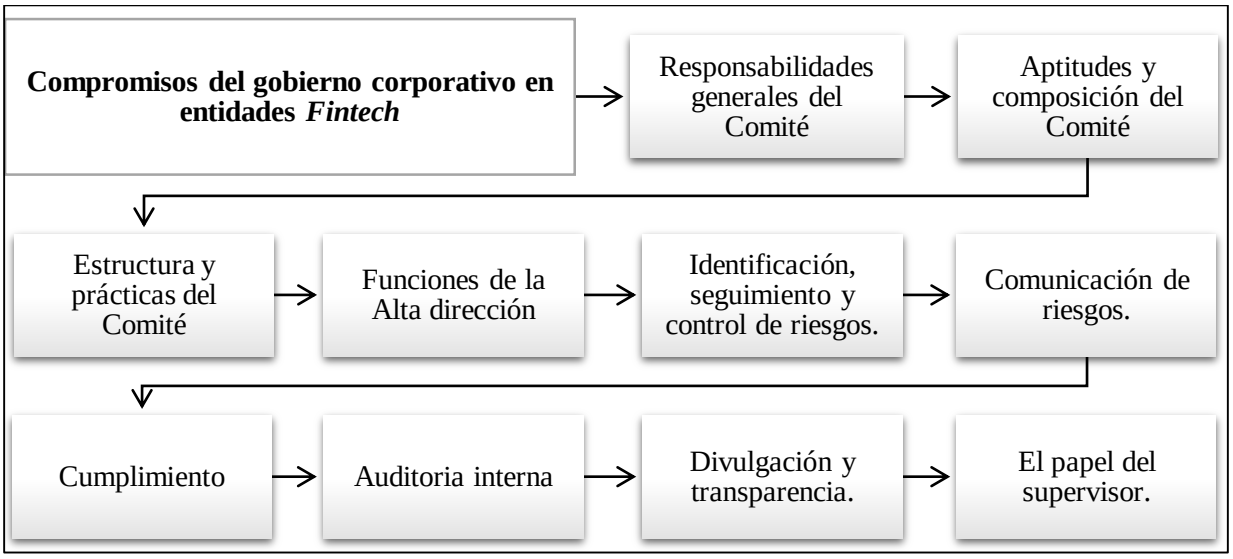

Figura 24. Implementación de un gobierno corporativo en entidades *Fintech*. Fuente: Elaboración propia.

- Responsabilidades generales del comité. La responsabilidad por parte del comité con toda la entidad *Fintech*, incluyendo la implementación de objetivos estratégicos de la entidad.
- Aptitudes y composición del comité. Los miembros del comité de riesgos deben estar en constante capacitación para el buen desempeño de su puesto.
- Estructura y prácticas del comité. El comité debe definir prácticas de gobierno corporativo apropiadas para su trabajo, y contar con medios necesarios que garanticen que éstas son seguidas y revisadas periódicamente para la mejora continua.
- Funciones de del comité de riesgos. El comité debe ser el responsable de adecuar el gobierno corporativo en todo el grupo, y asegurarse de que existan políticas y mecanismos adecuados a la estructura.
- Identificación, seguimiento y control de riesgos. El comité debe asegurarse de que las actividades de la entidad sean consistentes con la estrategia del negocio, la tolerancia al riesgo y las políticas aprobadas por el la alta dirección.

- Comunicación de riesgos. Las entidades deben contar con un sistema de control interno efectivo y una función de gestión de riesgos con suficiente autoridad, carácter, independencia, recursos y acceso al consejo.
- Cumplimiento. Una comunicación interna y robusta por parte del comité de riesgos y de la alta dirección dentro de la entidad *Fintech*, por medio de reportes.
- Auditoria interna. El comité de riesgos y la alta dirección deben utilizar de manera efectiva el trabajo realizado por la función de auditoría interna, auditoría externa y la función de control interno.
- Divulgación y transparencia. El comité de riesgos y la alta dirección deben saber y entender la estructura operacional de la entidad *Fintech* y los riesgos que ésta plantea.
- El papel del supervisor. El comité y la alta dirección deben entender el propósito, estructura y riesgos de estas operaciones y buscar mitigar los riesgos identificados.

4.4.2. Supervisión basada en riesgos operacionales en entidades *Fintech*. En el desarrollo de un marco adecuado para la gestión de riesgo operacionales en entidades *Fintech*, se proponen las buenas prácticas de Basilea, en colaboración con el FMI y el Banco Mundial, que consideren: los principales aspectos de los riesgos operacionales en las entidades *Fintech* y la categorización del riesgo; el aseguramiento de proceso de auditoría interna de forma eficaz e integral; y la puesta en práctica del marco para la gestión de riesgos operativos. La Figura 25, muestra el planteamiento descrito anteriormente.

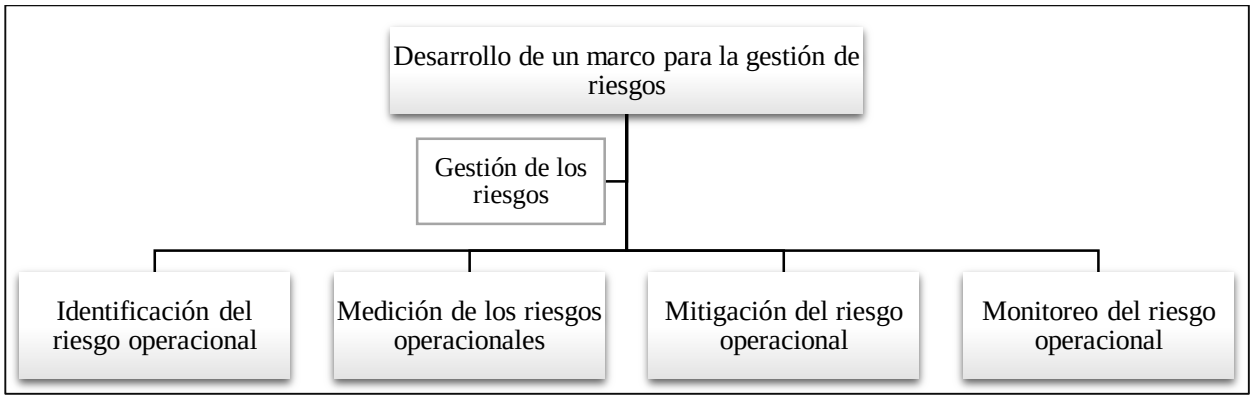

Figura 25. Marco para la evaluación de riesgos operativos. Fuente: Elaboración propia.

Identificación. Se propone que las entidades *Fintech* identifiquen y evalúen el riesgo operativo inherente a todos sus productos, actividades, procesos y sistemas relevantes. Además, de comprobar que antes de lanzar o presentar nuevos productos, actividades, procesos o sistemas, se evalúe adecuadamente su riesgo operativo.

Medición. La evaluación periódica de los perfiles de riesgo operativo y las exposiciones centrales a pérdidas por parte de las entidades *Fintech*, sin descartar que la alta gerencia y el comité de riesgos deben recibir información pertinente de forma periódica acerca de la gestión del riesgo operativo.

Mitigación. Contar con políticas, procesos y procedimientos para controlar y cubrir los riesgos operativos más relevantes por parte de las entidades *Fintech*, y verificar periódicamente sus estrategias de control y reducción de riesgos, y ajustar su perfil de riesgo operativo según corresponda.

Monitoreo. Contar con planes de contingencia y de continuidad de las operaciones que desarrolle la entidad *Fintech*, con la finalidad de asegurar su capacidad operativa continua y la reducción de pérdidas en caso de una interrupción grave de la operación.

4.4.3. Requisitos para la gestión del riesgo operacional para entidades *Fintech*. Con la finalidad de robustecer la seguridad del sistema de operación de las entidades *Fintech* de forma integral, se propone que las entidades *Fintech*, basados en los requerimientos emitidos por el Banco de México a los participantes del SPEI, implementen requisitos para la gestión del riesgo operacional, descritos en la Figura 26, con la intención de permitir la generación de condiciones que sea apropiadas para un ambiente de competencia y control adecuado de riesgos operacionales, y que brinden certeza y confianza a los participantes y usuarios.

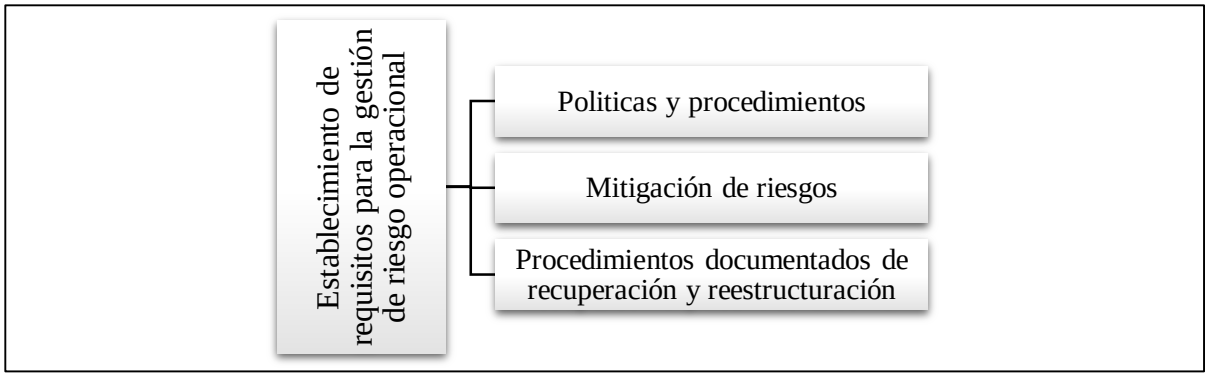

Figura 26. Requisitos para la gestión de riesgos operacionales. Fuente: Elaboración propia.

Políticas y procedimientos.

1. Contar con una metodología para la administración del riesgo operacional relacionada con la operación del sistema o infraestructura de operación de la entidad *Fintech*, que considere la identificación, evaluación, monitoreo y mitigación de los riesgos identificados, así como los roles y responsabilidades definidos para su ejecución, revisión y actualización, tal como se describió anteriormente;
2. Procesos críticos de operación relacionados con el sistema de operación de la entidad *Fintech*;

3. Procedimientos de contratación y capacitación del personal para asegurar que aquel relacionado con el sistema de operación de la entidad *Fintech* cuente con las habilidades, competencias y conocimientos requeridos para el puesto que desempeña; y
4. Manuales de procedimientos y de operación que describan las actividades requeridas para realizar la operación del sistema en la entidad *Fintech*, y el personal responsable de la ejecución de dichas actividades, así como, la definición precisa de responsabilidades.

Mitigación de riesgos.

1. Contar con un listado de los riesgos operacionales identificados, que indique la clasificación del riesgo y el resultado de su evaluación, así como los controles asociados para la operación en el sistema de la entidad *Fintech*, incluyendo los tecnológicos y aquellos asociados a proveedores externos;
2. Contar con un análisis de capacidades sobre los recursos tecnológicos, humanos y materiales que están disponibles para la infraestructura de operación de la entidad *Fintech*, con la finalidad de asegurar que se cuenta con los recursos suficientes para manejar volúmenes altos de operación y cumplir con objetivos de nivel de servicio; y
3. Contar con políticas y lineamientos para la gestión de privilegios de acceso físico a los sitios operativos.

Procedimientos documentados de recuperación y reestructuración.

1. Contar con política de continuidad, así como estrategias y procedimientos que deberá seguir para que, ante la materialización de los escenarios de contingencia identificados en el análisis de riesgos, pueda continuar con la operación en un nivel mínimo aceptable;
2. Las acciones que deberá seguir para la atención de incidentes que causen una afectación en la operación normal, con infraestructura que contemple las fases de identificación,

diagnóstico, atención, recuperación, restauración y documentación e indique los roles y responsabilidades correspondientes;

3. Las actividades que deberá realizar para dar respuesta a emergencias ante la ocurrencia de algún incidente que afecte la operación normal con el sistema de operación de la entidad *Fintech* en el que se considere la activación de las estrategias y procedimientos de continuidad implementados y se indiquen los roles y responsabilidades.
4. Las acciones que deberá seguir para el restablecimiento de la operación normal, una vez que se active alguna estrategia o se ejecute algún procedimiento de continuidad.
5. Un plan de pruebas al que deberá dar seguimiento para evaluar las estrategias y procedimientos de continuidad implementados relacionados con la operación con el sistema de operación de la entidad *Fintech*.

Conclusiones

El objetivo del presente trabajo fue proponer una estrategia integral de gestión de riesgos operacionales para las Instituciones de Tecnología Financieras de México (ITF), que considerara aspectos tecnológicos, humanos, organizacionales y normativos; con la finalidad de disminuir el impacto financiero que puedan sufrir dichas instituciones y sus clientes, ante amenazas a sus sistemas operativos. Para ello, se buscó aprobar o rechazar la preposición central, misma que se sustenta en que el impacto financiero de los riesgos a los que son susceptibles las ITFs, se pueden mitigar mediante una estrategia integral de administración de riesgos operacionales, considerando los aspectos tecnológicos, humanos, organizacionales y normativos de estas instituciones.

En el mismo orden de ideas, la investigación se justifica puesto que en un periodo corto de tiempo, México ha incrementado su participación en el sector financiero, precisamente para avanzar en el desarrollo de la innovación *Fintech* y situarse como uno de los potenciales a nivel mundial. Esta cifra supone un crecimiento en número de empresas de nueva creación en el sector, con un crecimiento anualizado del 40% para mediados del 2018. De igual forma, se estima que el valor total de las transacciones en el sector para finales del 2018 será de $36,439 millones de dólares, con una trayectoria de crecimiento de más del 17.3% anual para llegar a $69,000 millones de dólares en el 2022. No obstante, analistas señalan que es necesario observar el fenómeno del desarrollo *Fintech* en México, con el fin de identificar todas sus implicaciones, ya que, se requiere de una estrecha colaboración regulatoria y de gestión interna, y la gestión de riesgos operacionales vinculados a la prestación de servicios por parte de terceros y la protección frente a ciberataques, que pueden derivar del futuro incremento en el volumen de las actividades *Fintech*.

Con base a lo descrito anteriormente, en el primer objetivo particular se buscó describir los factores tecnológicos, humanos y organizacionales que rigen las normativas institucionales

Fintech a nivel internacional, en este caso, *Sandbox* regulatorios, por ello, la investigación involucró la búsqueda de las definición de las empresas que pueden participar, sus criterios de elegibilidad para ser aceptado en estos esquemas, sus parámetros para realizar la prueba, la definición de la colaboración e información a reportar a las autoridades, etc. En cada país, la elaboración y descripción de estos parámetros implicó evaluaciones de las innovaciones en tecnología financiera independientes en cada país, para posteriormente determinar si el marco regulatorio debía modificarse o adaptarse para incorporarse esta nueva realidad, de tal forma que se pudiera fomentar y facilitar la innovación sin deteriorar la protección al público usuario de los servicios financieros y de la estabilidad financiera de estos mercados. Por lo tanto, el alcance de este objetivo, pone hincapié en la importancia de fijar marcos regulatorios, en este caso para entidades *Fintech*, enfocados análisis de situación interna de un país.

El segundo objetivo particular fue, describir los mecanismos empleados en las mejores prácticas de regulación y supervisión bancaria. El alcance de este objetivo, implicó la búsqueda exhaustiva de aquellos organizamos enfocados a evaluar y proponer recomendaciones sobre supervisión y regulación a las entidades que realizan actividades bancarias. Por ello, el análisis realizado permitió detectar la importancia de desarrollar, implementar y mejorar continuamente el marco de trabajo o estructura de apoyo de las entidades que se enfocan a mejorar su marco de trabajo, además de destacar la importancia de integrar un proceso e gestión de riesgos y el gobierno corporativo en la entidad, enfocado en la planificación estratégica, procesos de información, políticas, valores y cultura.

El tercer objetivo particular fue, contextualizar el caso real de una institución financiera con impactos financieros derivados de amenazas en sus sistemas operativos. El estudio de caso fue el Ataque al SPEI del Banco de México. No obstante, el alcance del objetivo implicó la realización

y concentración de una entrevista, la búsqueda de informes y comunicados emitidos por el Banco de México para construir los eventos que propiciaron los ataques al SPEI, así como los mecanismos de mitigación y regulación que el Banco de México implemento. Así mismo, el análisis permitió destacar la importancia de tomar medidas necesarias en materia tecnológica, operativa y regulatoria por parte de aquellas instituciones que utilizan medios electrónicos para realizar actividades que implican el manejo de recursos provenientes de clientes inversores, puesto que, la complejidad y diversidad de las amenazas que tienen como fin el acceso ilegal a la información, ha escalado.

Por último, el cuarto objetivo particular, fue elaborar una estrategia integral de administración de riesgos para empresas *Fintech* en México. La estrategia que se propuso, buscó englobar las actividades para la implementación y mejora continua del proceso de gestión de riesgos operacionales en entidades *Fintech*, basándose en las buenas prácticas de supervisión de Basilea, la implementación de requisitos de supervisión basados en los requerimientos emitidos por el Banco de México a los participantes del SPEI, y la implementación de un gobierno corporativo basado en los principios de Basilea. Es importante destacar la el papel que juega la gestión de riesgos, puesto que representa hacer un esfuerzo anticipado para reducir pérdidas en el futuro, y que implica la realización de un proceso de identificación, análisis, cuantificación de vías adecuadas para emprender acciones preventivas y correctivas.

Es esencial, por lo tanto, que los las entidades *Fintech*, desarrollen estrategias, programas y planes para mitigar posibles vulnerabilidades. Estos deben ser coherentes con los criterios de reducción del riesgo, con la participación de entidades regulares, una planificación financiera, y gobiernos locales, el sector empresarial y la sociedad.

Por último, se recomienda a futuras investigaciones, la realización de estudios de indicadores financieros y operativos de las entidades *Fintech* que operan en México, puesto que, en la presente investigación, una de las principales limitaciones fue la falta de información de este tipo, ya que, en el actual periodo, las entidades *Fintech* se encuentran en un proceso transitorio de supervisión por parte de la CNBV, el cual implicará tiempo en cuanto a recopilación de información y estructuración de bases de datos con información financiera y operativa.

Referencias

Afful-Broni, A. (2012). Relationship between Motivation and Job Performance at the University of Mines and Technology, Tarkwa, Ghana: Leadership Lessons. *World Publishing Co., 3*(3), 309-314.

Alt, R., & Puschmann, T. (2012). The rise of customer-oriented banking - electronic markets are paving the way for change in the financial industry. *Electronic Markets, 22*(4), 203-215.

Arias, A. (2004). Acumulación de capacidades tecnológicas: el caso de la empresa curtidora ALFA. *Inestigación Económica, 63*(249), 101-123.

Asociación Española Fintech e Insurtech. (02 de 2017). *El libro Blanco de la regulación Fintech en España.* Obtenido de http://asociacionfintech.es

Australian Securities & Investments Commission, ASIC. (2017). *RG 257 Testing fintech products and services without holding an AFS or credit licence.* Obtenido de https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-257-testing-fintech-products-and-services-without-holding-an-afs-or-credit-licence/

Avendaño, O. (2018). Los retos de la banca digital en México. *IUS Revista del Instituto de Ciencias Jurídicas de Puebla, 12*(41), 87-108.

Ayón, M., y Pérez, C. (2017). *Prevención de lavado de dinero: Gestión de riesgos latentes.* Obtenido de https://assets.kpmg.com/content/dam/kpmg/pa/pdf/delineandoestrategias/DE-prevencion-lavado-dinero.pdf

Banco de México, Banxico. (2005). Definiciones básicas de Riesgo. Obtenido de http://www.banxico.org.mx/sistema-financiero/d/%7B691D5348-6C29-424E-4A6F-C1E6F6F47A00%7D.pdf

Banco de México, Banxico (2018a). *Informe Trimestral Enero - Marzo 2018*. Obtenido de http://www.banxico.org.mx/publicaciones-y-prensa/informes-trimestrales/%7B7E9CAB5E-DA3C-B3A8-7DB3-F517D6C69960%7D.pdf

Banco de México, Banxico (2018b). *Información sobre los ataques a los Participantes del SPEI*. Obtenido de http://www.banxico.org.mx/spei/d/%7BFFC53F5A-CA04-3098-EBF6-B0F17E533183%7D.pdf

Banco de México, Banxico (2018c). *Estrategia de Ciberseguridad del SPEI*. Obtenido de http://www.banxico.org.mx/spei/d/%7BD8F9F341-00E7-459A-D35D-5F487FA05AA1%7D.pdf

Banco de México, Banxico. (2018d). *Informe Trimestral Abril-Junio 2018*. Obtenido de http://www.banxico.org.mx/publicaciones-y-prensa/informes-trimestrales/%7B247C655C-1793-909F-7173-C82C3AB0F5F1%7D.pdf

Banco Mundial, BM. (2016). *Panorama general de inclusión financiera*. Obtenido de http://www.bancomundial.org/es/topic/financialinclusion/overview#1

Bank Negara Malaysia, BNM. (2016). *Financial technology regulatory sandbox framework.* Kuala Lumpur, Malasia: BNM/RH/PD 030-1.

Bancomer, BBVA. (2018). *Cómo facilitan el trabajo a las pymes el 'fintech', el 'bitcoin' y el 'crowdlending'*. Ciudad de México: Centro de innovación BBVA.

Barberis, J., Arner, D., & Buckley, R. (2016). The Evolution of Fintech: A New Post-Crisis Paradigm. *Georgetown Journal of International Law, 47*, pp. 1271-1273.

Basel Committe on Banking Supervision, Basilea (2018). *Implications of fintech developments for banks and bank supervisors.* Obtenido de https://www.bis.org/bcbs/publ/d431.pdf

Bell, M. (1984). *Learning and the Accumulation of Industrial Technological Capacity in Developing Countries.* Palgrave Macmillan, London: Technological capability in the Third World.

Bell, M., & Pavitt, K. (1995). The Development of Technological Capabilities. *Trade, technology and international competitiveness, 22*(4831), 69-101.

Benavides, G. (2007). *GARCH Processes and Value at Risk: An Empirical Analysis for Mexican Interest Rate Futures.* Chile: Panorama Socioeconómico.

Benton, K., Myers, R., & Martello, A. (2016). *Perspectives of Fintech: A conversation with Governor Lael Brainald*. Philadelphia, E.U.: Consumer Compliance Outlook.

Berndsen, R. (20 de 06 de 2016). *If Blockchain is the Answer, What is the Question?* Obtenido de Conferencia en la Dutch Blockchain Conference, De Nederlandsche Bank: https://www.dnb.nl/ binaries/Speech%20Ron%20Berndsen_tcm46-342846.pdf?2017111320

Canadian Securities Administrators, CSA (2017). *CSA Regulatory Sandbox*. Obtenido de https://www.securities-administrators.ca/industry_resources.aspx?id=1588&terms=sandbox

Cañas, L. (2009). *Gestión de riesgos de negocio. Desarrollo e implementación de sistemas de gestión de riesgos.* El Salvador: Departamento de Investigación Económica y Financiera del Banco.

Carrillo, M. R. (2007). La proteccion de los consumidores en las transacciones electronicas de pago. *Telematique, 6*(3), 33-49.

Casares, I., y Lizarzaburu, E. R. (2016). *Introducción a la Gestión Integal de Riesgos Empresariales, Enfoque: ISO 31000.* Lima, Perú: Platinum Editorial.

Chiavenato, I. (2007). *Administración de Recursos Humanos* (8va ed.). México: Mc Graw Hill.

Child, J. (1984). New technology and developments in management organization. *Omega, 12*(3), 211-223.

Chishti, S., & Barberis, J. (2016). The Fintech Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries. *Financial Analysts Journal*, *73*(2), 136-137.

Cohen, W., & Levinthal, D. (2000). Absorptive capacity: A new perspective on learning and innovation. *Strategic Learning in a Knowledge economy*(35), pp. 39-67.

Comisión Nacional Bancaria y de Valores, CNBV (2005). *Disposiciones de carácter general aplicables a las instituciones de crédito.* Obtenido de https://www.cnbv.gob.mx/Prensa/Presentaciones%20Seminario%20Corresponsales/i.%20Circular%20%C3%9Anica%20de%20Bancos.pdf

Comité de Supervisión Bancaria de Basilea, Basilea (2011). *Principios Básicos para una supervisión bancaria eficaz.* Obtenido de https://www.bis.org/publ/bcbs213_es.pdf

Comité de Supervisión Bancaria de Basilea, Basilea. (2004). *Buenas prácticas para la gestión y supervisión del riesgo operativo.* Suiza: Banco de Pagos Internacionales.

Comité de Supervisión Bancaria de Basilea, Basilea. (2015). *Principios de gobierno corporativo para bancos.* Obtenido de https://www.bis.org/bcbs/publ/d328_es.pdfPrincipios de gobierno corporativo para bancos

Consejo Nacional de Inclusión Financiera, CONAIF (2016). *Política Nacional de Inclusión Financiera.* Obtenido de https://www.gob.mx/cms/uploads/attachment/file/110408/PNIF_ver_1jul2016CONAIF_vfinal.pdf

Cuesta, C., Ruesta, M., Tuesta, D., y Urbiola, P. (16 de 07 de 2015). *Economía Digital: la transformación digital de la banca, BBVA*. Obtenido de www.bbvaresearch.com

Dapp, T. (2014). *Fintech – The digital (r)evolution in the financial sector*. Obtenido de https://www.deutschebank.nl/nl/docs/FintechThe_digital_revolution_in_the_financial_sector.pdf

De Olso, M. (2005). *Guía para la recogida e interpretación de datos sobre la Innovación.* Luxembourg, España: OECD.

Deal, T. A., y Kennedy, A. (1985). *Cultura Corporativa.* Bogotá, Colombia: Editorial Legis.

Deloitte. (2017). *A tale of 44 cities: Connecting Global FinTech: Interim Hub Review 2017.* United Kingdom: Global Fintech Hubs.

Diario Oficial de la Federación, DOF. (2017a). *Circular 14/2017, Reglas del Sistema de Pafos Electrónicos Interbancarios.* México: Banco de México. Obtenido de https://dof.gob.mx/nota_detalle.php?codigo=5488888&fecha=04/07/2017

Diario Oficial de la Federación, DOF. (2017b). *Circular 11/2018 Reforma a las reglas del sistema de pagos electrónicos interbancarios SPEI: En materia de mitigación de riesgos.* México: Banco de México. Obtenido de http://www.banxico.org.mx/marco-normativo/normativa-emitida-por-el-banco-de-mexico/circular-14-2017/%7B33EFD864-87F6-89BF-9F19-35E4D80E4CF4%7D.pdf

Diario Oficial de la Federación, DOF. (2018a). *Disposiciones de caracter general aplicables a las Instituciones de Tecnológia Financiera.* México: CNBV. Obtenido de https://dof.gob.mx/nota_detalle.php?codigo=5537450&fecha=10/09/2018

Diario Oficial de la Federación, DOF. (2018b). *Circular 4/2018 Disposiciones generales aplicables al servicio de transferencias de fondos y los sistemas de pagos administrados*

por el banco de México. México: Banco de México. Obtenido de http://www.dof.gob.mx/normasOficiales.php

Diario Oficial de la Federación, DOF. (2018c). *Circular 5/2018 Reforma a las reglas del sistema de pagos electrónicos interbancarios SPEI en materia de tiempos de acreditación de transferencias recibidas por los participantes.* México: Banco de México. Obtenido de http://www.banxico.org.mx/marco-normativo/normativa-emitida-por-el-banco-de-mexico/circular-14-2017/%7BFD8C941A-5DCE-51D6-02B7-99803E33F27E%7D.pdf

Diario Oficial de la Federación, DOF (2018d). *Circular 10/2018 Reforma a las disposiciones generales aplicables a los participantes del sistema de pagos electrónico interbancarios SPEI en materia de mitigación de riesgos.* México: Banco de México. Obtenido de http://www.dof.gob.mx/nota_detalle.php?codigo=5533263&fecha=27/07/2018

Dutrénit, G. (2000). *Learning and Knowledge Management in the Firm: From Knowledge Accumulation to Strategic Capabilities.* México: Edward Elgar Publishing.

Fernández, R. (1994). La Corporación Virtual y el factor humano. *Capital Humano, 6*(69), 25-29.

Financial Conduct Authority, FCA. (2017). *Regulatory sandbox.* Obtenido de https://www.fca.org.uk/firms/regulatory-sandbox

Financial Inclusion Innovation Laboratory, Fiinlab (2017). *Panorama Fintech en México.* México: Endeavor.

Financial Stability Board, FSB (2017). *Financial Stability Implications from FinTech: Supervisory and Regulatory Issues that Merit Authorities' Attention.* Obtenido de http://www.fsb.org/wp-content/uploads/R270617.pdf

Finnovista. (06 de 07 de 2017). *El ecosistema Fintech de México crece un 50% en menos de un año y releva a Brasil como Líder Fintech en América Latina*. Obtenido de https://www.finnovista.com/actualizacion-fintech-radar-mexico/

Finnovista. (01 de 07 de 2018). *México supera la barrera de las 300 startups Fintech y refuerza su posición como segundo ecosistema Fintech más importante en América Latina*. Obtenido de https://www.finnovista.com/actualizacion-finnovista-fintech-radar-mexico-agosto-2018/

Fintech México. (17 de 01 de 2018). *El crecimiento esperado se debe al efecto positivo que la Ley Fintech*. Obtenido de https://www.fintechmexico.org/es/noticias/

Foncillas, B. (2017). El sector financiero ante el reto digital. *Revista de economía* (898), pp. 23-34.

Freeman, C. (1989). *Technology policy and economic performance: Lessons from Japan.* Great Britain: Pinter Publishers.

Furche, P., Madeira, C., Marcel, M., y Medel, C. A. (2017). Fintech y la banca central en la encrucijada. *Revista de Políticas Públicas,* (148), pp. 39-79.

Gai, K. (2016). Cuestiones de seguridad y privacidad: una encuesta sobre FinTech. *Smart Computing and Communication*, *27*(17), pp. 236-247.

Galeano, M. U. (2012). *Estrategias de investigación social cualitati; El giro en la mirada.* Medellín, Colombia: La Carretra.

García, R. (2018). *Decálogo para la implementacion de un Sandbox en España.* Obtenido de https://asociacionfintech.es/wp-content/uploads/2018/03/Decalogo_Sandbox.pdf

García, S. (2017). *Nuevos servicios transaccionales: el cliente en primer plano.* Madrid, España*:* Departamento de Investigación IEB.

Gareth, J. (2008). *Teoría organizacional: Diseño y cambio en las organnizaciones* (5ta ed.). México: Pearson Educación.

Gitman, L. J. (2007). *Principios de Administración Financiera* (11va ed.). México: Pearson Educación.

Gitman, L., & Joehnk, M. (2009). *Fundamentos de inversiones* (10va ed.). México: Pearson Educación. doi:ISBN: 978-970-26-1514-9

Guerrero, R. M., Focke, K. S., & Mejía, A. C. (2011). *Supervisión con base en riesgos: Precisión del marco conceptual.* Washington: Banco Interamericano de Desarrollo.

Guibert, S. (2016). La revolución Fintech, pagos móviles y desafíos para la banca. *Diario La Ley*, (8825), p.1.

Hall, R. (1996). *Organizaciones, estructuras, procesos y resultados.* México: Prentice Hall.

Hernández, J. (2017). Capacidades tecnológicas y organizacionales de las empresas mexicanas participantes en la cadena de valor de la industria aeronáutica. *Economía: teoría y práctica* (47), pp. 65-98.

Hernández, J. S., y Vera-Cruz, A. (2003). Aprendizaje y acumulación de capacidades tecnológicas en la industria maquiladora de exportación: El caso de Thomson-Multimedia de México. *Espacios, 24*, p. 2.

Hernandez, R., Fernández, C., & Baptista, P. (2006). *Metodología de la Investigación* (4a ed.). México: McGraw Gil Interamericana.

Herrera, D. (2016). *Alternative Finance (Crowdfunding) Regulation in Latin America and the Caribbean: A Balancing Act.* Caribbean: Inter-American Development Bank.

Hickson, D. (1966). A convergence in organization theory. *Administrative Science Quarterly, 11*(2), 224-237.

Hidalgo, A., León, G., y Pavón, J. (2013). *La gestión de la innovación y la tecnología en las organizaciones.* Madrid: Pirámide.

Hodge, B. J., Anthony, W. P., y Gales, L. M. (1998). *Teoría de la Organización. Un enfoque estratégico. Prentice Hall.* Madrid, España: Prentice Hall.

Holgado, A. M., y Harizmendi, J. (2017). *Los riesgos financieros de las fintech* (Tesis de maestria). Universidad Pontifica ICAI, Madrid, España..

Hong Kong Monetary Authority, HKMA. (2017). *Fintech Supervisory Sandbox (FSS)*. Obtenido de https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech-supervisory-sandbox.shtml#1

Igual, D. (2016). *Fintech: Lo que la tecnología hace por las Finanzas.* Balcelona: Profit Editorial. S.L.

Insurance Authority, IA. (2017). *Insurtech Corner*. Obtenido de https://www.ia.org.hk/en/aboutus/insurtech_corner.html

Jacobson, A. (2015). *Mexico's 3 greatest financial inclusion challenges, as defined by 20 experts*. Obtenido de https://medium.com/village-capital/mexico-s-3-greatest-financial-inclusion-challenges-as-defined-by-20-experts-cb37952ff0fc

Joyanes, L. (2015). *Sistemas de información en la empresa.* Colombia: Editorial Uoc.

Julapa, J. (2017). Fintech Lending: Financial Inclusión, Risk Pricing, and Alternative Information. *Federal Reserve Bank of Philadelphia*, *17*(17), 1-48.

Katz, J. (2007). *Cambios estructurales y ciclos de destrucción y creación de capacidades productivas y tecnológicas en América Latina.* Chile: The Macmillan Press Ltd.

Kim, L. (1999). *Learning and innovation in economic development.* Great Britain: Edward Elgar Publishing.

Kim, L., & Dahlman, G. (1992). Technology policy for industrialization: An integrative framework and Korea's experience. *Research Policy, 21*(5), 437-452.

Kiviat, T. I. (2015). Más allá de Bitcoin: problemas para regular las transacciones de blockchain. *Duke Law Journal*, (13), pp. 569-582.

Kopp, E., Kaffenberger, L., & Wilson, C. (2017). *Cyber Risk, Market Failures, and Financial Stability*. International Monetary Fund.

Lall, S. (1992). Technological Capabilities and Industrialization. *World Development, 20*(2), 65-186.

Lara, A. (2008). *Medición y control de riesgos financieros* (3a ed.). México: Limusa.

Lawrence, P. R., & Lorsch, J. W. (1967). *Organization and Environment.* Boston: Harvard University.

Levine, R., Lin, C., & Wang, Z. (2017). *Acquiring Banking Networks.* doi: 10.3386 / w23469

Ley de Instituciones de Tecnologia Financiera. (ITF, 2018). *Ley para regular las de Instituciones de Tecnologia Financiera.* Ciudad de México: Diario Oficial de la Federación. Obtenido de http://www.diputados.gob.mx/LeyesBiblio/ref/lritf/LRITF_orig_09mar18.pdf

Lizarzaburu, E. R., Barriga, G., Noriega, L., Lopéz, L., y Mejía, P. (2017). Gestión de Riesgos Empresariales: Marco de revisión ISO 31000. *Espacios, 38*(59), 8.

Lozano, G., y Moreno, P. (2016). *Megatendencias del mercado y FinTech en México.* España: Camara Española de Comercio.

Luthans, F. (2002). *Organizational behavior.* Nueva York: McGraw-Hill Higher Education.

Magnusson, T., Prasad, A., & Storkey, I. (2010). *Guidance for Operational Risk Management in Government Debt Management.* Washington, DC: Debt management performance assessment (DeMPA). Obtenido de

http://documents.worldbank.org/curated/en/419301468153852761/Guidance-for-operational-risk-management-in-government-debt-management

Malinova, K., & Park, A. (2016). M*arket Design with Blockchain Technology* (Tesis de maestría). Universidad McMaster, Toronto.

Martinez, C., Medina, S., y Colmenares, G. (s.f.). *Clasificación Del Riesgo Financiero Basado en Modelos De Calificación Difusos Caso: La Banca Venezolana entre 1996 y 2004* (Tesis doctoral). Universidad de Los Andes, Venezuela.

Maslow, A. H. (1953). A theory of human motivation. *Psycological Review, 50*(4), 370-396.

Mertens, D. (2014). *Research and evaluation in Education and Psychology: Integrating diversity with quantitative, qualitative, and mixed methods* (4a ed.). Singapure: Sage publications.

Mintzberg, H. (1995). *La estructuración de las organizaciones.* Barcelona: Ariel.

Monetary Authority of Singapore, MAS. (2016). *Fintech Regulatory Sandbox Guidelines.* Obtenido de http://www.mas.gov.sg/~/media/Smart%20Financial%20Centre/Sandbox/FinTech%20Regulatory%20Sandbox%20Guidelines.pdf

Morales, A., Morales, J. A., y Alcocer, F. R. (2014). *Administración Financiera.* Mexico: Grupo editorial patria.

Ngwenya-Scoburgh, L. (2009). *Organizational Learning: an exploration of the influence of capabilities and factors* (Tesis doctoral). Capella University, Minneapolis, E.U.

Noya, E. (2016). ¿Es el "fintech" el mayor desafío que afronta la banca? *Harvard Deusto business review, 254,* pp. 22-29.

Olivencia, M. (2007). *Derecho Patrimonial y Tecnología.* Madrid: Marcial Pons.

Olliver, J. O., y Thompson, P. I. (2017). *Guía para elborar trabajos de investigación en Ciencias Económico - Administrativas.* México: Textos Universitarios.

Ontiveros, E., Martín, Á., Navarro, M. Á., y Rodríguez, E. (2012). Las TIC y el sector financiero del futuro. Barcelona: Ariel SA.

Organización para la Cooperación y el Desarrollo Económico, OCDE. (2004). *Principios de Gobierno Corporativo de la OCDE.* Paris, Francia: OECD Principles of Corporate Governance.

Organización para la Cooperación y el Desarrollo Económico. (OCDE, 2016). *Principios de Gobierno Corporativo de la OCDE y del G20.* Paris, Francia: OCDE. Obtenido de http://dx.doi.org/10.1787/9789264259171-es

Padilla, A., y Águila, A. (2003). La evolución de las formas organizativas. De la estructura simple a la organización en red y virtual. *Investigaciones Europeas, 9*(3), 69-94.

Prieto, A. (2005). *Conceptos de Informática e Introducción a la Informática.* Madrid: McGraw-Hill.

Real Academia Española, RAE. (2017). *Definición de la palabra "Riesgo"*. Obtenido de http://dle.rae.es/?id=WT8tAMI

Reimann, B. C. (1973). On the dimensions of bureaucratic structure: an empirical reappraisal. *Administrative Science Quarterly, 18*(4), 462 - 476.

Robbins, S. P. (2004). *Comportamiento organizacional* (10a ed.). México D.F.: Prentice Hall.

Romero, B., y Alvarado, A. (2014). *El factor humano en las organizaciones y su relación con la promoción de la competitividad y la productividad.* Sucre, Bolivia: Ecorfan-Bolivia.

Rojas, L. (2016). La revolución de las empresas FinTech y el futuro de la Banca: Disrupción tecnológica en el sector financiero. *Corporación Andina de Fomento*, (24), pp. 11-38.

Sánchez, M. (2016). Fintech: panorama actual y tendencias regulatorias. *Revista de Derecho del Mercado de Valores,* (19), p. 1.

Sanicola, L. (12 de 02 de 2017). *"¿Qué es FinTech?"* . Obtenido de https://www.huffingtonpost.com/entry/what-is-fintech_us_58a20d80e4b0cd37efcfebaa

Schatán, C. (2017). Perspectivas de las tecnologías de la información en México. *Revista de Comercio Exterior,* (9), pp. 1-9.

Schein, E. (1992). *Organizational culture and leadership.* San Francisco, E.U.: Jossey-Bass.

Schueffel, P. (2017). Domar a la bestia: una definición científica de Fintech. *Revista de gestión de la innovación*, (6), pp. 32-54.

Scott, W. R. (1981). *Organizations: Rational, Natural, and Open Systems.* Upper Saddle River, NJ: Prentice Hall.

Securities and Futures Commission, SFC. (2017). Circular to announce the SFC Regulatory Sandbox. Obtenido de https://www.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=17EC63

Seibold, S., & Samman, G. (2016). *Consensus - Immutable Agreetment for the Internet of Value. KPMG.* Obtenido de https://activos.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmgblockchain-consenso-mechanism.pdf .

Silva, A., y Ramos, M. C. (2017). *La evolución del sector fintech, modelos de negocio, regulación y retos.* México: Fundación de Estudios Financieros, FUNDEF A.C.

Sirvent, C. (2008). *Sistemas Jurídicos Contemporáneos.* México: Porrúa.

Smets, J. (2016). Fintech and Central Banks. *In Speech at the Colloquium of the Belgian Financial Forum in cooperation with SUERF, Fintech and the Future of Retail Banking, Brussels*. Chicago: European Money and Finance Forum Eggsplore.

Soler, J. A., Staking, K. B., Ayuso, A., Beato, P., Botín, E., Escrig, M., y Falero, B. (1999). *Gestión de Riesgos Financieros: Un enfoque práctico para países latinoamericanos.* Washington, D.C.: Banco Interamericano de Desarrollo (BID).

Storkey, I. (2011). *Gestión del riesgo operacional y planificación de la continuidad de las operaciones para tesorerías estatales modernas.* Forndo Monetario Internacional.

Storkey, I. (2011). *Gestión del riesgo operacional y planificación de la continuidad de las operaciones para tesorerías estatales modernas.* . Obtenido de https://www. imf. org/external/spanish/pubs/ft/tnm/2011/tnm1105s. pdf.

Tapia, G. N. (2014). Tecnologías emergentes y factores financieros elementales a considerar. *Revista de investigación en modelos financieros, 1*, pp. 305-339.

Tarziján, J. (2007). *Fundamentos de estrategia empresaria.* Chile: Universidad Católica de Chile.

Teddlie, C., & Tshakkori, A. (2003). *Major Issues and Controversies in the Use 01 Mixed Methods in the Social and Behavioral Studies.* Thousand Oaks, Sage: Handbook of Mixed Methods in Social & Behavioral Research.

Uría, F. (2017). *La regulación del sector financiero ante el resto del fintech.* Madrid: Departamento de Investigación del IEB.

Van Horne, J. C., y Wachowicz, J. M. (2010). *Fundamentos de Administración Financiera* (13va ed.). México: Pearson Educación.

Vroom, V. H. (1964). *Work and motivation,.* Nueva York: John Wiley.

William, J. (2016). *Fintech: The Beginner's guide to financial technology.* Fairfield, Ohio: CreateSpace Independent Publishing Platform.

World Economic Forum, WEF (2015). *The Future of FinTech: A Paradigm Shift in Small Business Finance.* Obtenido de https://www.weforum.org/reports/future-fintech-paradigm-shift-small-business-finance

Yáñez, Á. (2018). FinTech en la industria financiera: Nuevos espacios de desarrollo y convergencia regulatoria. *Dirección de estudios SBIF, 18*(1), 1-18.

APÉNDICES

Apéndice A

Entrevista Semiestructurada

Inicio

Fecha: 04 / 10 / 2018 **Hora:** 9:00 am

Lugar y/o medio específico: Vía telefónica

Entrevistado:

- Persona entrevistada: Luis Leyva Martínez
- Empresa/Institución: CNBV
- Función: Director General de Desarrollo Regulatorio en la CNBV
- Correo electrónico: lleyva@cnbv.gob.mx
- Experiencia el puesto de trabajo (Años): 4 años

Introducción

Buen día, como parte de mi tesis en el posgrado de Ciencias Económico-Administrativas de la Universidad Autónoma de Querétaro estoy realizando una investigación acerca de los impactos financieros a las que son susceptibles las Instituciones de Tecnología Financiera con la finalidad de proponer una estrategia integral de riesgos operacionales. La información brindada en esta entrevista es de carácter confidencial, solo será utilizada para los propósitos de la investigación, así mismo, la entrevista tiene como propósito cumplir con un tiempo estimado de 20min. Agradezco su colaboración.

Preguntas

1. *¿Podría explicarme sobre el proceso para el diseño de la ley de Instituciones de Tecnología Financiera y cuáles fueron sus principales retos?* Respuesta. La Ley Fintech fue el

resultado del trabajo de más de dos años de investigación y desarrollo por parte de la CNBV, la Secretaría de Hacienda y el Banco de México. En los años previo, antes de que se tuviera una definición legal para un proyecto, normalmente comenzamos con pláticas con nuestros pares regulatorios, con entidades que supervisan y regulan entidades financieras en otros países, se tuvo un acercamiento con el Reino Unido, el Banco Mundial, así mismo, tuvimos la ayuda del Banco Interamericano de Desarrollo, de forma que tuvimos muchas personas acompañándonos en este proceso. Normalmente como nosotros trabajamos, la CNBV y particularmente el área que yo dirijo que es el área de Dirección de Desarrollo Regulatorio hacemos ejercicios, más bien, análisis de Derecho Comparado, revisamos experiencias a nivel internacional, se revisa qué es lo que se está realizando allá fuera, es decir, que han hecho otros países, y también se revisa qué es lo que están haciendo en México. Particularmente, el problema con Fintech es que no había demasiado afuera, puesto que al ser un fenómeno nuevo en comparación a la vejes que tiene, por ejemplo, el Sistema Financiero de México, Fintech es muy nuevo en términos de entender crowfunding, en términos de entender los pagos a través de las instituciones como las que regula la Ley Fintech, y en este sentido, no había demasiados estándares, es decir, no hay puntos de referencia, a diferencia de, por ejemplo, si se quiere regular el estándar de capital de un banco, si se quiere regular algo así podemos encontrar los estándares que emite el comité de Basilea, si se quiere regular un aspecto que tenga que ver con el mercado de valores, en este sentido están los principios y documentos que emite la Organización Internacional de Comisiones de Valores, es decir, existen ciertos estándares ya acordados a nivel global, pero en el caso de Fintech no hay nada, lo que hay, las regulaciones más avanzadas, por ejemplo, del Reino Unido, la de España que son los pioneros en regular el crowfunding, todavía son muy resientes, por lo que aún no pasamos un ciclo como para ver qué tan buenas regulaciones son, es decir, fue uno de los primeros problemas que tuvimos, y

en realidad estamos en la orillita del desarrollo, no hay mucho hacia donde voltear, y si volteamos hacia fuera (internacionalmente), y hacia dentro (internacionalmente) fue necesario tener muchas pláticas, muchas reuniones con el gremio de las plataformas de crowfunding, de algunas empresas que se dedican a ofrecer servicios con monederos electrónicos para entender sus modelos de negocio, para entender el grado de sofisticación e institucionalización que tenían, los controles internos, el mercado que estaban atendiendo, es decir, queríamos conocer primero qué es lo que estábamos regulando, entonces, esas dos grandes vertientes constituyeron grandes retos. Digamos, primero, no había estándares internacionales, es decir, no hay algo probado, y dos, que al ser un sector relativamente nuevo en México como tal, implicó introducirnos para conocer los modelos, y cuando uno ya empieza a conocer los modelos con cuidado hay muchas diferencias al interior del propio gremio puesto que no todos son iguales, por tal motivo regular esto suena complicado, porque además, yo le agrego una tercer vertiente, y tiene que ver con que regular tecnología es una de las cosas más complicadas que existen, porque la tecnología por definición se mueve mucho más rápido que la regulación y eso implica que el diseño de una ley donde están quedando cosas en piedra, tenía que ser flexible, tenía que darnos a nosotros como entidad financiera la posibilidad de regular a través de las Disposiciones de Carácter General no sólo lo que ya está hoy en día, sino lo que puede llegar a pasar en 20 años, requirió un diseño técnico muy distinto del que se observa en las leyes tradicionales, por ejemplo, la Ley de Mercados de Valores, la Ley de Instituciones de Crédito, la Ley de Fondos de Inversión, aquí las facultades que tenemos son mucho más amplias, de modo que se pueda tener más oportunidad de atender no sólo el ahora, sino también el mañana, además que plantemos la Ley basada en una serie de principios rectores de todo el accionar de la autoridad, de manera que estos principios fuesen inmutables, pero que a la vez permitieran tener un bracero para el mañana, respecto por ejemplo, de cuidar la inclusión, cuidar la competencia, ser

neutrales tecnológicamente hablando, es decir, estos principios están diseñados para que nos acompañen en la interpretación de la Ley en el tiempo.

2. Para la elaboración de la regulación secundaria de la Ley Fintech, ¿Su equipo de trabajo contempló analizar las regulaciones, acuerdos y/o propuestas de otros países a nivel internacional? De ser así, ¿Cuáles fueron y por qué? ¿Qué factores de análisis tomaron en cuenta? Respuesta. Tomamos lo que encontramos, dentro de lo poco que encontramos hay países como el Reino Unido que sin duda fue el más avanzado, esta Australia, y como están muy relacionados respecto de su marco normativo, entonces están muy parecidos, también Singapur, sigue el mismo camino, y conforme se va uno alejando y empieza a mirar digamos a Asia, o a Estados Unidos, hay cambios, no sólo por el cambio del marco por el tipo de estructura legal del país, sino también, por la realidad del sistema financiero, son cuestiones distintas, entonces lo que se tomo era lo que nos parecía sensato y razonable, por ejemplo, el Reino Unido fue el pionero en establecer un sandbox regulatorio, este sandbox en el Reino Unido nos da la oportunidad de generar un espacio de mayor libertad regulatoria para proyectos que el día de hoy pueden empezar a trabajar a nivel de un piloto y cristalizarse en un periodo después, pero bajo el cobijo de una regulación que los va encaminado, esa estructura en México no la teníamos, puesto que es más particular de regímenes como el Reino Unido, donde regulan con base en principios, con base en guías que no es tan prescriptiva, y de más -va en esa línea- pero es una buena idea porque hemos tenido cosas de este lado, en México, en donde llega de repente un banco con alguna idea, con algún nuevo producto, y no lo puede desarrollar porque la regulación no se lo permite, el mismo problema que hay allá lo tenemos aquí, en este sentido lo que tratamos de hacer, adecuar esas buenas practicas, esas buenas ideas, que vimos en algunas otras latitudes, a la estructura de México, entonces lo que tratamos de hacer fue separar bien esas cuestiones y creamos un sandbox, es decir,

necesitamos un sandbox para entidades financieras para cuando quieren venir y traer, por ejemplo, un nuevo procedimiento de autenticación de clientes basado en la lectura del iris -ha pero mi regulación sólo habla de la huella digital- en este caso lo que se hace es irse por el lado del sandbox, lo empezamos a pilotear, y en el tiempo, vamos viendo que tan consistentes son los resultados que tienes como entidad financiera, te generamos una autorización acotada por un plazo perentorio, y al final, a mí Comisión, me dio tiempo de mover la regulación de tal forma que no te cuartea a ti banco de hacer este desarrollo y a la vez de que yo, Comisión, aprendí, nos fuimos juntos de la mano, y al final del camino tienes una regulación que recógela experiencia del sandbox, el otro sandbox te dice, qué pasa si yo no soy banco, yo soy una entidad fintech, soy una entidad que quiero hacer algo, pero para eso que quiero hacer requiero convertirme en banco, o requiero convertirme en una operadora de Fondos de Inversión, en este sentido yo Comisión te recomiendo que te vayas al otro sandbox y presentas tu modelo novedoso, este debe tener un impacto, un beneficio, que tiene que probar que es tecnológicamente la novedad, y se meten por ese camino, al final, bajo ese sandbox, dentro del proceso se les realiza una regulación a doc, durante el periodo transitorio que les dura la autorización y al final de ese periodo tendían que adoptar una de las figuras reguladas, ya sea un banco, una casa de bolsa, un fondo de inversión, lo que más se asemeje a lo que ellos están piloteando, por eso, lo que se hico fue hacer las adecuaciones para el caso mexicano. Y como ejemplo el ejemplo anterior tengo muchos, cosas que vimos en otros países y las pasábamos por la realidad mexicana -y decíamos- no, es que esto en México no va a funcionar, no, es que esto en México lo tenemos que hacer de otra manera, te pongo otro ejemplo, en crowfunding de capitales, en Estados Unidos, tienen un proceso muy similar al que nosotros seguimos para autorizar emisoras de valores en México, es decir, llenan un prospecto que requiere de la autorización de la autoridad estadounidense, y para ello hay todo un marco muy completo en

torno a eso, en México no adoptamos esa figura porque significaba en automático matar al sector, y no podíamos aplicar las reglas de mercado de valores al crowfunding de capital, entonces lo que hicimos fue tomar algunos ejemplos con respecto a qué información les piden, y eso lo meteré yo Comisión en un proyecto de regulación secundaria, tomando algunos de los elementos y algunas ideas, pero claramente como base, no era algo que se pudiera extrapolar o algo que pudiésemos adoptar directamente aquí en México, la realidad es distinta, entonces digamos que fue caso por caso, ejemplo por ejemplo, y cuestiones muy técnicas, topes de financiamiento, límites de cuanto puede financiarse un inversionista en crowfunding, vivimos la experiencia internacional, vimos donde estaban los límites, vimos que tipos de aspectos regulaban, y cuando lo veíamos bajo el bracero de México, algunas cosas tenían sentido y algunas otras no, de manera nunca copiamos y pegamos las regulaciones de otros países, las tomamos como referencias, y lo que salió ganando fue la realidad de lo que pasaba en México de cómo se veía el mercado en México.

3. *Dentro de las Disposiciones de Carácter General de la Ley ITF para abordar la regulación de bancos, supervisión bancaria y gestión de riesgos ¿Se tomó en cuenta el análisis de mejores prácticas a nivel internacional? Por ejemplo, el Comité de Basilea de Supervisión Bancaria (BCBS), acuerdos de la OCDE, el Banco de México, etc. De ser así, ¿Cuáles fueron y por qué?* Respuesta. Más bien recibimos el ofrecimiento, por ejemplo del Banco Interamericano de Desarrollo (BID) y el Banco Mundial en términos de apoyos, nos brindaron recursos en términos de contratarnos un consultor, en términos de ayudarnos con algunos ejercicios de derecho comparado, o con la discusión de varios de los temas y los platicábamos con ellos, y esto fue algo mutuamente benéfico, puesto que al ser fintech algo nuevo ellos tampoco tenían la verdad de nada, tampoco tenían una experiencia internacional que yo no hubiera visto, o algo que yo no hubiera detectado en mi análisis, digamos yo como CNBV, más bien lo que yo necesitaba era poder discutir

las ideas, necesitábamos tener un espacio de discusión, de reflexión, y ahí puedo decir que la regulación fintech no la hice yo sólo en mi escritorio, más bien fue el resultado de discusiones, platicar, de ir, de conocer, de entrevistar, de tener miles de reuniones de muchas horas de estar reunidos en una sala de juntas, de discutir un tema, ver qué opina el Banco Mundial acerca de la estructura, de algún concepto, como lo ve el BID, como lo ve el secretario de hacienda, fue en ese sentido, no fue un trabajo de gabinete, y en ese sentido, el Banco Mundial y el BID nos ayudaron en el proceso, con algún documento donde reseñaban alguna estructura que se tenían que cuidar y que se tomaron en cuenta, nos ayudaran en temas de discusión, nos ayudaron en términos de acreditación del derecho de los participantes, de las entidades financieras, del senado y la cámara de diputados, en generar un momentum, es decir, algo que oliera a fintech, a que la gente se empezara a interesar, a enterarse del tema, a empezar a contemplar este fenómeno nuevo que venía de otro lado.

4. *¿Considera que el ataque a SPEI en Banxico se relaciona directamente con las Instituciones de Tecnología Financiera? De ser así, ¿De qué forma? ¿Considera que en las Disposiciones de Carácter General aplicables a las ITFs se tomaron en cuenta aspectos como: riesgos tecnológicos, cibernéticos y de fraude para operar con activos virtuales? De ser así ¿Qué aspectos cubre? En su opinión, ¿Por qué se tomaron en cuenta?*

5. *¿Cuáles son las entidades ITF que la comisión supervisa actualmente y por qué? ¿Qué nos puede decir de la situación actual en materia financiera y operativa de las entidades supervisadas por la CNBV?* Respuesta. En este momento no se está supervisando a ninguna entidad Fintech, la razón es porque la Ley que se publicó en marzo pasado, le dio un periodo transitorio a las entidades que por virtud de la propia Ley ya están haciendo actividades reservadas para las cuales adquieren

autorización, es decir, todas éstas plataformas en formas de crowfunding y todos estos proveedores de servicios de pagos electrónicos, es decir estos "iwallets" que ya operan en México, si venían operando antes de la entrada en vigor de la regulación, la Ley les concede un plazo transitorio para acudir a la Comisión y obtener la autorización, de manera que en este momento, no estamos en un plazo de estar supervisando, lo que estamos haciendo es que hace poco, específicamente el 10 de septiembre pasado emitimos la primera regulación secundaria necesaria para que estas entidades que están en el periodo transitorio y algunas nuevas que no lo están, acudan a la Comisión y soliciten su autorización, ese es el estatus, en este momento como tal no se está supervisando, más bien estamos formando las prácticas de supervisión, se está elaborando toda la infraestructura para recibirlas, esto tiene que ver con preparar la supervisión, los procesos de autorización, además de seguir emitiendo la regulación secundaria necesaria para que cuando entren en vigor al solicitar su autorización y empiecen a operar, ya operen con un marco legal completo, la Ley Fintech sólo establece un marco general, pero nos dio muchas facultades para incluir dentro de las Disposiciones de Carácter General aspectos ya más técnicos. Respecto de cuál es su situación financiera o cuál es su situación actual de éstas que están operando al cobijo del transitorio que la Ley les dio, no quisiera darte algo como "lo vemos bien o lo vemos mal" porque no tengo suficientes datos para hacer un análisis financiero y decir que van mal o que van bien, porque en este momento todavía no nos allegamos de esa información, es parte de lo que se tiene que diseñar para que cuando venga y empiecen a generar información y de esta manera podamos hace una supervisión en riesgos, -pero lo que si te puede decir-, es que normalmente las entidades fintech son muy ligeras en cuanta costos, porque están basados ampliamente en tecnología, ellos experimentan pérdidas durante varios años hasta llegar el punto de equilibrio, les cuesta trabajo, y en mi experiencia no he visto a alguna que llegue al equilibrio antes de los 3, 4 años de manera

que son entidades que si bien son ligeritas en cuanto a costos, son entidades que traen modelos nuevos y demás, y en lo que se ubican en el mercado, en lo que adquieren una posición en el mercado se tardan un poco de tiempo, y además ahora tienes que agregar el costo regulatorio que implica tener que cumplir con la Ley, y digamos que, cuando estábamos diseñando la regulación, cuando estábamos diseñando la Ley, lo que tratábamos de hacer no era necesariamente generar regulaciones que fuesen prohibitivas o cosas que les generaran cosos exorbitantes, pero si lo que tratamos de hacer es que una vez de que entran al terreno regulatorio, una vez de que se vuelven entidad financieras, porque en realidad eso son, a quien tenemos que tutelar es al público inversionista, y en ese sentido es que la atención está puesta ahí, y en este sentido establecimos requisitos regulatorios que lo que buscan es proteger a los inversionistas a través de mecanismos de transparencia, a través de mecanismos de buenos procesos, a través de buenos sistemas de control interno, de administración de riesgos que generen entidades que no sean autorizadas un día, y al día siguiente ya estén en problemas, es por eso que si debemos tener mucho cuidado de que las personas que van a entrar, sean personas que ya estén en el terreno de revisar actividades que son reguladas, que están tomando recursos del público, y como tal, amerita tener un grado de seriedad en cuanto a institucionalización.

6. *¿Qué opina de la creación y diseño de una estrategia integral de riesgos operacionales para su aplicación en ITFs? ¿Qué nos recomienda?* Respuesta. Cuando hablamos de las fintech los riesgos son muy distintos, hay un riesgo muy distinto entre, por ejemplo, operar un pago, al hacer una transferencia de recursos y entre realizar el fondeo de un proyecto de inversión, de tal forma que, actividades distintas generan riesgos distintos, y desde el punto de vista de la Comisión lo que realizamos es establecer en las Disposiciones de Carácter General elementos que son mínimos para la constitución de marcos de control interno de administración de riesgos, el primero

que emitimos es el de ciberseguridad para entidades como las instituciones financiamiento colectivo, y ahí lo que se trató de hacer es que en la medida en la que estas entidades, su principal contacto o su corte es por medios electrónicos una página de internet, o dispositivos de ese tipo, los riesgo principales que presentan provienen de estas plataformas, son riesgos de intrusión, riesgos de que se les caiga la página, riesgos de que no levanten la página a tiempo, riesgos de que no identifiquen claramente los recursos de donde vienen y a donde van, estos problemas se mitigan cumpliendo con las Disposiciones que emite la Comisión, que son mínimos que deben observar y de ahí para delate ellos pueden establecer muchos mecanismos. Las piezas del rompecabezas las hemos ido poniendo poco a poco, no podemos regular todo al mismo tiempo, porque ni yo puedo emitir tanta regulación al mismo tiempo ni ellos tienen la capacidad de absorber la regulación en un tiempo corto, es decir, son regulaciones que tenemos que ir calibrando, tenemos que ir viendo en atención a los riesgos específicos.

El riesgo que me señalas, que tiene que ver con el SPEI del Banco de México, son riesgos que se van a atender desde la regulación del Banco de México que se está fortaleciendo, que está en consulta pública en este momento o si no es que ya la publicaron, esa regulación lo que va a hacer es fortalecer justo ese nodo, el tema de cómo te conectas al SPEI, que características deben tener los proveedores que se conectan al SPEI, elementos de seguridad y demás, y eso sería aplicable directamente a estas entidades fintech, pero lo que tratamos de hacer es ir dosificando la regulación poco a poco, no es un ejercicio de un solo hit y acabamos, es algo que tenemos que ir calibrando con mucho cuidado, cuando empieza uno a conocer estas fintech te das cuenta que los recursos con los que cuentan son pocos, son entidades de 4 u 9 personas, que de manera que si yo pido la separación, por ejemplo, del riesgo operativo en las áreas del negocio, la separación entre las áreas de control y las áreas del negocio, pues básicamente en una fintech uno estará en una recamara y

el otro estará en la de al lado, es decir, hay realidades que se tienen que revisar cuando se haga la regulación y eso es lo que se tiene que tomar con suficiente seriedad, de manera que primero tenemos que conocer bien, tenemos ver cómo van evolucionando, tenemos que ir llevándolas poco a poco, de forma que la regulación que salga, no sea nada más una derivación del estándar de bancos, o una derivación de otro estándar que ya existe, se tiene que afinar mucho, en lo que no pasa eso, ya las propias entidades hemos detectado que algunas tienen buenos estándares de seguridad, algunas han contratado proveedores para robustecer su marco de administración de riesgos tecnológico, algunas otras tienen ya una separaciones, las más grandes han establecido estándares con base en líneas de defensa, han implementado mecanismos de identificación del usuario, es decir, la propia industria ha ido avanzando poco a poco, y lo que queremos hacer cuando toque la segunda parte de la regulación, que toca emitirla en 12 meses, tenemos que ver cuál es el estado de las cosas, tenemos que ver cuál es el estándar que la comisión establezca y ver cuál es la mejor manera de llevarlas entre lo que tienen y al punto en el cual los quiero llevar, pero es un proceso que requiere primero conocerlos, no hay una sola respuesta, lo modelos son distintos.

Apéndice B

Tabla B1

Categoría: Modificación regulatoria: (autorización, exención, permiso).

País	Descripción
Malasia	El Banco Central de Malasia adoptó el enfoque de director informal, para proporcionar orientación y asesoramiento a las Instituciones de Tecnología Financieras o empresas *Fintech* sobre las modificaciones o requerimientos legales y regulatorios que se puedan realizar, para alinear las propuestas con modelos de negocio o soluciones con las leyes y regulaciones vigentes en el país.
Canadá	La CSA evalúa los méritos de cada modelo de negocio, caso por caso, y las empresas que se registran o reciben apoyo pueden probar sus productos y servicios en todo el mercado canadiense. No obstante, la CSA destacó la implementación de cambios en el Marco Regulatorio de Valores según sea necesario, y en virtud de los avances de nuevas innovaciones tecnológicas, y se estableció que las empresas autorizadas para operar en el *Sandbox* deben permanecer sujetas a todos los requisitos regulatorios que puedan aplicarse.
Australia	Por lo general, una empresa debe tener una licencia AFS antes de que pueda lanzar al mercado un nuevo producto o servicio financiero. Sin embargo, en algunas situaciones, es posible probar estos productos o servicios sin una licencia. Por ello, la *Regulatory Guide* (RG) se compuso con base en tres componentes. Por una parte; ante la flexibilidad existente en el marco regulatorio o las exenciones previstas por la ley donde *no se requiera una autorizaciones*; la *exención de autorizaciones de Fintech* de ASIC que se apliquen a ciertos productos o servicios; y por último, las *exenciones de autorizaciones individuales y personalizadas* otorgadas por ASIC a un negocio en particular para facilitar las pruebas de productos o servicios.
España	El *Sandbox* permite, bajo la modalidad de exención, que las entidades *Fintech* e *Insurtech* disfruten de un periodo de pruebas en el que puedan ir alcanzando los requisitos de obtención ordinaria de una licencia, para operar, por ejemplo, en el mercado de valores, bancario, servicios de pago o asegurador, gradual y progresivamente, es decir, a medida que la entidad vayan alcanzando un cierto estado de maduración. Por otro lado, bajo la modalidad de no sujeción, el *Sandbox* permite que las entidades *Fintech* e *Insurtech* que realicen actividades no expresamente reguladas hasta la fecha

	empiecen a probar sus productos en un espacio de pruebas seguro o controlado permitiendo así lanzar este tipo de productos y servicios innovadores al mercado con el respaldo de los reguladores y con el consiguiente beneficio para el cliente final y para el propio mercado, aportando una mayor seguridad jurídica y confianza.	
Singapur	El MAS es el encargado de determinar los requisitos legales y regulatorios específicos que se flexibilizan dependiendo del producto financiero a probar, el tipo de solicitante y el tipo de innovación. Ejemplos de requerimientos regulatorios que no se flexibilizan: confidencialidad de la información del cliente, criterios de idoneidad, manejo de activos por intermediarios, normas para la prevención de lavado de dinero y financiamiento al terrorismo (PLDFT). Ejemplos de requerimientos que pueden ser relajados: composición del consejo de administración, calificación crediticia, cuotas de autorización, experiencia en la administración, activos mínimos líquidos, suficiencia de capital, capital mínimo pagado, reputación, entre otros.	
Hong Kong	*IA*	La IA es la encargada de determinar los requisitos legales y regulatorios específicos que se adaptan dependiendo del tipo de actividad en el desarrollo de tecnología de la industria de seguros.
	SFC	El SFC dirigió su actividad a entidades reguladas por la Ordenanza de Valores y Futuros (SFO) antes de que pueda lanzar al mercado un nuevo producto o servicio financiero innovador.
	HKMA	La HKMA es la encargada de determinar los requisitos legales y regulatorios específicos que se adaptan dependiendo del tipo de actividad que realizan los bancos y las entidades de tecnología financiera.
Reino Unido	Para realizar una actividad regulada en el Reino Unido, una entidad debe ser autorizada o registrada por la FCA, a menos que se apliquen ciertas exenciones. Las empresas exitosas deben solicitar la autorización o el registro correspondiente para realizar la prueba. La FCA cuenta con un proceso de autorización que se ajustan a las empresas que son aprobadas en el *Sandbox*.	

Fuente: Elaboración propia.

Tabla B2

Categoría: Entidad a la que está dirigido.

País	Descripción
Malasia	Fue creado para que se pudiese aplicar a: una entidades financieras establecidas por cuenta propia o en colaboración con una empresa *Fintech* o una empresa *Fintech* que tuviese la intención de solicitar o solicite la aprobación del BNM para participar en el *Sandbox*; una empresa *Fintech* que pretenda continuar operando, es decir, una empresa autorizada o registrada; y, una empresa que ya ha sido autorizada o registrada de acuerdo a la legislación vigente de Malasia.
Canadá	El CSA *Regulatory Sandbox* está abierto a modelos de negocios que son verdaderamente innovadores desde la perspectiva del mercado canadiense, además, señaló que los solicitantes pueden ir desde empresas de nueva creación, hasta empresas ya establecidas.
Australia	*Titular de una autorización o licencia ASF existente*. Para la obtención de una autorización a un intermediario existente, se definió que éstos pueden proporcionar servicios financieros australianos (AFS) o participar en actividades crediticias existentes o un concesionario de crédito como representante de esa autorización. Como regla general, en esa situación se estableció que el titular de la autorización debe tener un permiso que le autorice participar (por ejemplo, servicios financieros o actividad crediticia) que el interesado busque emprender en su nombre; y a menos que sea un empleado, director u organismo corporativo relacionado al concesionario, el concesionario debe designarlo como su representante autorizado (si es un concesionario de AFS) o como su representante de crédito (si es un concesionario de crédito). Se definió que esta opción solo es disponible si se está proporcionando los servicios en nombre del concesionario, pero no si está prestando los servicios en su nombre como un director. *Productos o servicios que no requieren autorización.* Se detalló que se aplicaría a productos que no están sujetos a los requisitos de autorización en los servicios financieros o las leyes de crédito al consumidor, por ejemplo, un cambio de moneda extranjera que se liquida de inmediato, el cual no está regulado por la Ley de Sociedades Anónimas; algunas transferencias electrónicas de fondos, donde no existe un acuerdo permanente entre el cliente y la persona que envía los fondos, no están reguladas por la Ley de Sociedades Anónimas; los productos de pago donde los pagos solo pueden

	hacerse a una persona que no se encuentre regulada por la Ley de Sociedades Anónimas; y el crédito otorgado a empresas, o con fines comerciales, que no está regulado por la Ley Nacional de Crédito. *Entidades que sean representantes autorizados o sean parte de la estructura corporativa de una empresa que tenga una licencia ASF*.
España	Se valoró la necesidad de diferenciar a aquellas entidades cuyas actividades estuvieran sujetas a autorización previa, respecto de aquellas que únicamente pudiesen prestar servicios adicionales al ámbito financiero. Para ello, se plantearon propuestas regulatorias independientes, destacando las que se muestran a continuación. *Asesoramiento y gestión patrimonial*. Se incluyeron cuatro tipos de entidades: las redes de inversión; las que prestan el servicio de asesoramiento en materia de inversiones de manera automatizada; aquellas que prestan servicio de gestión automatizada; y las plataformas de negociación. Dado que el principal obstáculo consistía en que para prestar estos servicios, las entidades debían de constituirse como Empresas de Servicios de Inversión (ESI), la propuesta consistió en simplificar de los requisitos para la autorización de las ESIS. *Finanzas personales*. Se contemplaron a los comparadores de productos financieros, así como las entidades que prestan servicios de optimización de finanzas personales. No obstante, al considerar que algunos de esos servicios podrían estar sujetos a la reserva de actividad a favor de las ESIs se planteó la simplificación de los requisitos exigidos a este tipo de entidades. *Financiación Alternativa*. Este vertical abarcó tanto a las entidades que proporcionan préstamos sin necesidad de garantía (Préstamos Raídos Online), así como las entidades de Crowdlending y Crowdfunding. Las barreras que se identificaron en relación a los Préstamos Rápidos Online se vincularon a mejor la definición de los préstamos usurarios y a la modificación de normativa, entre otros aspectos, relativo a la renuncia de contratos. Por tanto, se propuso un cambio normativo que se tradujo en una mayor precisión del concepto de préstamo usurario. *Crowdlending*. Dentro de la presente vertical se englobaron todas aquellas plataformas de financiación participativa que llevan a cabo una actividad de *Crowdlending* específica, la cual consiste en la oferta de financiación bajo la forma de préstamos a cambio de un rendimiento de dinerario. Su propuesta de cambio normativo se relacionó con las barreras derivadas de la Ley de fomento de la Financiación Empresarial (Ley 5/2015), así como a las especialidades en relación a la actividad concreta de *Crowdlending*.

Equity Crowdfunding. Este concepto englobo a diversas entidades cuya actividad principal se encuentra focalizada en la oferta de servicios dirigidos a facilitar el acceso de sociedades a obtener financiación en el mercado, principalmente *startups* o Pequeñas y Medianas Empresas. Las propuestas de cambio normativo se relacionaron con aquellas barreras normativas y de acceso a actividades derivadas de las limitaciones establecidas por la Ley 5/2015.

Crowdfunding/lending sobre activos o bienes tangibles. Se incluyeron a las entidades cuya actividad consiste en la captación de fondos con la finalidad de inversión en proyectos sobre activos o bienes tangibles. Las principales barreras y las propuestas de reforma se vincularon a los requisitos impuestos por la Ley 5/2015, así como el régimen aplicable a las Instituciones de Inversión Colectiva.

Servicios Transaccionales/Divisas. Se incluyeron a las entidades que cuentan con un aspecto en común, como el de evitar los costos derivados de la intermediación bancaria. Las barreras normativas incluidas en este vertical se asociaron con la reserva de actividad que la normativa recoge respecto de la actividad realizada por estas entidades. Por ello, la propuesta normativa fue la simplificación del régimen de acceso y de actividad aplicable a las entidades que prestan servicios de compra y venta de divisas.

Medios de pago. Se incluyeron a todas aquellas entidades que prestan medios de pago electrónicos. Las principales barreras que se detectaron se relacionaron a los requisitos exigidos para las entidades de servicios de pago, así como en relación al acceso, entre otros, al Sistema Nacional de Compensación Electrónica. Atendiendo a lo anterior, las principales propuestas de cambio normativo se asociaron con la garantía del acceso en igualdad al Sistema Nacional de Compensación Electrónica.

Infraestructura financiera. Se incluyeron a todas aquellas entidades Fintech cuya actividad consiste en la creación o mejora de la tecnología existente para la prestación de servicios financieros. Las principales barreras en relación a este vertical, derivaron en las normas técnicas de regulación, por lo que se propuso la atenuación de los requisitos de autenticación para aquellas entidades que prestan servicios de información sobre cuentas.

Criptocurrencies y Blockchain. Se consideró a las criptomonedas como un medio digital de intercambio, así como la tecnología en que estas se sustentan y el *blockchain* como el desarrollo del Marco de Innovación Regulatoria (*Regulatory Sandbox*) para operar en el mercado bajo asistencia de un supervisor.

	Insurtech. Se consideró a *Inurtech* como la aplicación de la tecnología al sector asegurador, donde se detectó que esta fue afectada por un régimen normativo que exige amplios requisitos económicos a las entidades, para realizar la actividad de aseguradora. De esta forma, la propuesta normativa pasó, entre otros aspectos, por aligerar los requisitos para aquellas actividades que realicen la función de aseguradora de forma restringida. *Identificación online de clientes.* Se incluyeron a aquellas entidades que proporcionan servicios destinados a identificar clientes a distancia a través de medios electrónicos. Dado que con la regulación vigente en España, la identificación online de clientes se ve limitada a los medios autorizados, por lo que se propusieron mecanismos para aumentar los medios aceptados para la identificación online de clientes. *Big Data*. Se incluyeron a todas aquellas entidades que generan valor añadido con la recogida de datos y consecuente gestión, análisis inteligente, incluyendo Inteligencia Artificial (IA) y generación de servicios utilizando, estos datos. Las principales propuestas de reforma se fijaron en los criterios interpretativos la normativa de protección de datos, que proporcione seguridad jurídica a la actividad desarrollada por las entidades y que se alineen con los avances tecnológicos, así como la actualización de determinada normativa del sector.
Singapur	Los lineamientos son de particular interés para las empresas que buscan aplicar la tecnología de una manera innovadora, para brindar servicios financieros que puedan o estén regulados por el MAS. El público objetivo incluye a entidades *Fintech* y entidades que ofrecen servicios profesionales que se asocian o brindan apoyo a dichas entidades.	
Hong Kong	*IA*	La IA Supervisa el desarrollo y la aplicación de la tecnología en la industria de Seguros.
	SFC	El SFC dirigió su actividad a las entidades que utilizan tecnologías innovadoras y demuestran un compromiso genuino y serio de llevar a cabo actividades reguladas mediante el uso de tecnología financiera *Fintech*.
	HKMA	El FSS dirigió su actividad a los bancos y entidades de tecnología financiera asociadas.
Reino Unido	El *Sandbox* regulatorio se dirige a entidades autorizadas, entidades no autorizadas que requieren autorización y negocios de tecnología.	

Fuente: Elaboración propia.

Tabla B3

Categoría: Criterios de elegibilidad.

País	Descripción
Malasia	Al considerar una solicitud para participar en el *Sandbox*, los tipos y el alcance de las flexibilidades regulatorias que pudieran otorgarse a las entidades *Fintech* que operan en un *Sandbox*, BNM tomó en cuenta los beneficios potenciales del producto, servicio o solución propuesto, tales como: el la eficacia, la seguridad, la accesibilidad y la calidad de los servicios financieros; la mejora de la eficacia y la eficiencia de la gestión de riesgos potenciales y las medidas de mitigación, de las instituciones financieras de Malasia; y, abrir nuevas oportunidades de financiamiento o inversiones en la economía de Malasia.
Canadá	Las empresas que deseen postularse deben estar preparadas para proporcionar pruebas en el *Sandbox* regulatorio, un plan de negocios y una discusión de los beneficios potenciales para los inversores, que incluya la forma en que minimizará los riesgos de los inversores. Además, se fijó que los aspirantes pueden solicitar la inscripción u obtener apoyo a través de un proceso de solicitud estándar.
Australia	No menciona
España	Se estableció un Marco de Innovación Regulatoria (MIR) en el que se incluyeron las autorizaciones definidas anteriormente, las cuales fueron dirigida a las entidades que logren cumplir con una serie de requisitos suscritos en el programa, estos pueden recibir una autorización temporal y limitada que permita a las *startups* realizar actividades relacionadas a entidades *Fintech* e *Insurtech* y probar cómo reaccionan sus productos y servicios en el mercado.
Singapur	El *Sandbox* regulatorio debe ayudar a fomentar más la experimentación de *Fintech* dentro de un espacio y duración bien definidos, en los que el MAS proporciona el soporte normativo necesario para aumentar la eficiencia; administrar mejor los riesgos; crear nuevas oportunidades; o mejorar la vida de las personas. Así mismo, el solicitante debe entender claramente el objetivo y los principios del *Sandbox*, y debe enfatizar que el *Sandbox* no está destinada y no puede usarse como un medio para eludir los requisitos legales y reglamentarios. Adicionalmente, el producto debe de ser diferente a los que actualmente existen, de lo contrario, el solicitante debe demostrar que se está aplicando una tecnología diferente, o la misma tecnología se aplica de manera diferente. Así mismo, el solicitante debe

	demostrar que ha cumplido con sus procedimientos debidamente, estos incluyen las pruebas del servicio financiero propuesto en el *Sandbox* regulatorio, y el conocimiento de los requisitos legales y regulatorios para implementar el servicio financiero propuesto.	
Hong Kong	*IA* *SFC* *HKMA*	No se menciona, sin embarco se acordó que, en conjunto la HKMA, el SFC y la IA lanzaron sus respectivos *Sandbox* regulatorios, por ello, si una empresa tiene la intención de realizar una prueba piloto de un producto *Fintech* multisectorial, puede solicitar el acceso a la *Sandbox* que considere más relevante o que encaje en la definición de alguna entidad regulada por cualquiera de las tres autoridades.
Reino Unido	Las solicitantes tienen que cumplir con una serie de requisito, los cuales determinan la necesidad de que las entidades solicitantes deban ofrecer innovaciones destinadas al mercado del Reino Unido, innovaciones nuevas y únicas. Además, la innovación debe ofrecer una buena perspectiva de los beneficios identificables para los consumidores, y debe de existir una verdadera necesidad de probar la innovación en el *Sandbox* propuesto por la FCA.	

Fuente: Elaboración propia.

Tabla B4

Categoría: Parámetros para la elaboración de pruebas.

País	Descripción
Malasia	El solicitante, debe realizar una evaluación adecuada para demostrar la utilidad y funcionalidad del producto, servicio o solución e identificar los riesgos asociados. Así mismo, se precisó que los solicitantes deben demostrar que tienen los recursos necesarios para respaldar las pruebas en el *Sandbox*. Esto incluye los recursos necesarios y la experiencia para mitigar y controlar los riesgos y pérdidas potenciales que surgen de la oferta del producto, servicio o solución, además de que deben tener un plan de negocios realista para implementar el producto, servicio o solución a escala comercial en Malasia después de salir del *Sandbox.*
Canadá	Las empresas solicitantes, deben presentar su modelo de negocios al personal de su regulador local de valores. La tarea del personal es analizar el modelo de negocio, en el cual, debe realizar preguntas y trabajar con la empresa para identificar los requisitos

	regulatorios para los cuales se necesita registro y/o exención libre. Así mismo, se definió que el personal y la empresa también pueden negociar sobre la elegibilidad de la empresa para participar en el *Sandbox* regulatorio de CSA, incluidos los límites y las condiciones que podrían imponerse. Posteriormente, la empresa debe presentar una solicitud a su regulador local de valores para registrarse y liberar los requisitos regulatorios, de tal forma que si se presentó de forma adecuada ante el regulador local de valores, la solicitud se puede hacer bajo el régimen de pasaportes australianos, lo que le da a la empresa acceso a los mercados de capital en múltiples jurisdicciones.
Australia	En virtud de la Ley de Sociedades Anónimas y la Ley Nacional de Protección del Crédito al Consumidor (Ley Nacional de Crédito Australiana), ASIC determinó que se deben evaluar las solicitudes de AFS y las autorizaciones de crédito como parte de su función como regulador de las industrias de servicios financieros y de crédito. Se definió que los intermediarios deben cumplir con una serie de obligaciones generales, como requisitos para hacer todo lo necesario para garantizar que los servicios cubiertos para que su autorización se presten de manera eficiente, honesta y justa; cumplir con las leyes y condiciones pertinentes para sus autorizaciones; tener soluciones adecuadas de resolución de conflictos y compensación para clientes minoristas; y tomar medidas para garantizar que sus representantes estén adecuadamente capacitados, sean competentes y cumplan con la ley. Además, se precisó que los intermediarios y sus representantes también deben cumplir con obligaciones específicas en la Ley de Sociedades Anónimas, la Ley de la Comisión de Valores e Inversiones de Australia (Ley ASIC), la Ley de Crédito Nacional y otras leyes de servicios financieros, como las normas de conducta y divulgación.
España	Sólo se mencionó que las entidades *Fintech* o *Insurtech* beneficiaria puede comenzar su actividad empresarial bajo la modalidad de exención para el caso de actividades reguladas o bien bajo la modalidad de no sujeción para el caso de actividades no expresamente reguladas.
Singapur	No los define previamente, no obstante se mencionó que dado que el *Sandbox* funciona en el entorno de producción, debe tener un espacio y una duración bien definidos para el lanzamiento del servicio financiero propuesto, dentro del cual se pueden contener las consecuencias de posibles fallas.

Hong Kong	*IA*	La IA determinó principios que se deben aplicar para la elaboración de pruebas que incluyeron límite y condiciones bien definidos; debe haber un alcance claramente definido en el *Sandbox*, que incluya tiempo y duración, o fecha de lanzamiento oficial esperada de la iniciativa al mercado, el tamaño y tipo de negocio de seguros, y usuarios específicos, la tecnología involucrada, los resultado esperado y los criterios de éxito del ensayo; así mismo, debe contar con los controles de gestión de riesgos y la protección del cliente, recursos y preparación de la aseguradora y una estrategia de salida del *Sandbox*.
	SFC	Con la finalidad de minimizar los riesgos para los inversionistas durante el período en que una empresa calificada opera en el *Sandbox*, la SFC puede imponer condiciones de licencia. Las condiciones de licencia pueden incluir la limitación de los tipos de clientes a los que la empresa puede atender o la exposición máxima de cada cliente, a fin de limitar el alcance y los límites del negocio de la empresa en actividades reguladas. En algunos casos, las condiciones de la licencia pueden requerir que la empresa establezca esquemas de compensación apropiados para los inversores, o que se someta a auditorías periódicas de supervisión por parte de la SFC. Además se espera que las empresas calificadas cuenten con medidas adecuadas de protección al inversor para abordar los riesgos o inquietudes reales o potenciales identificados cuando operan en el *Sandbox*.
	HKMA	La HKMA estableció que la administración de un banco autorizado para usar FSS debe garantizar limites en la implementación de definiciones claras sobre el alcance y las fases (si las hay) de pruebas piloto, los acuerdos de tiempo y terminación; medidas para proteger los intereses de los clientes; controles de compensación para mitigar riesgos asociados con un cumplimiento incompleto de los requisitos de supervisión; la preparación de los sistemas y procesos involucrados en la prueba y monitoreo cercano de la prueba; por último, se estableció que la FSS no debe utilizarse como un medio para eludir los requisitos de supervisión aplicables.
Reino Unido	El solicitante debe de contar con un plan de pruebas bien desarrollado con objetivos, parámetros y criterios de éxito claros, deben además, contar con pruebas realizadas hasta la fecha, contar con recursos para probar en el *Sandbox y* contar con protecciones para asegurar a los consumidores y proporcionar compensaciones adecuadas si es necesario.	

Fuente: Elaboración propia.

Tabla B5

Categoría: Colaboración y reportes.

País	Descripción
Malasia	Se precisaron requerimientos de aplicación, donde estableció que el solicitante debe presentar al BNM una carta de solicitud firmada por el Director Ejecutivo (CEO) del solicitante u oficial debidamente autorizado por el CEO. El solicitante también debe incluir los resultados clave que la prueba pretende lograr y los indicadores apropiados para medir dichos resultados. Posteriormente, especificó que el BNM debe informar al solicitante de su elegibilidad para participar en el *Sandbox*. A partir de entonces, se estableció que el BNM involucraría a los participantes en parámetros de prueba, como el alcance y la duración de la prueba, las flexibilidades regulatorias solicitadas y la frecuencia de los informes; medidas específicas para determinar el éxito o el fracaso de la prueba al final del período de prueba; una estrategia de salida si la prueba falla o se suspende; y un plan de transición para la implementación del producto, servicio o solución a escala comercial, luego de realizar pruebas exitosas y salir del *Sandbox*.
Canadá	Se precisó que las empresas que tengan la intención de operar en el CSA *Regulatory Sandbox* deben estar preparadas para proporcionar al personal de la CSA la información sobre sus operaciones para fines de monitoreo y recopilación de datos, y a su vez, éstas deben estar sujetas a revisiones de cumplimiento y vigilancia por la CSA.
Australia	Se definió que dentro de los 2 meses posteriores al final de la exención, la entidad debe enviar a la ASIC un breve reporte con los detalles de la prueba, que incluye información sobre los clientes, sobre la naturaleza de las quejas, aspectos o retos a los que se enfrentaron, requisitos regulatorios identificados como barreras e información financiera. Además, señaló que dicho reporte no podrá ser publicado, a menos de que se considere de interés para el regulador.
España	Sólo se menciona que AEFI es la principal asociación representativa del sector Fintech e Insurtech en España, la cual tiene como objetivo, colaborar y promocionar la interacción entre las principales entidades del mercado en España.
Singapur	El participante debe reportar al MAS sobre los avances de la prueba, de acuerdo al calendario previamente acordado entre ellos.

Hong Kong	*IA*	La IA ha establecido el Equipo de Facilitación de *Insurtech* para mejorar la comunicación con las empresas involucradas en el desarrollo y la aplicación de *Insurtech* en Hong Kong, así como para promover a Hong Kong como un centro de *Insurtech* en Asia. El objetivo del Equipo es facilitar la comprensión de la comunidad de *Insurtech* sobre el régimen regulatorio actual, así como, actuar como una plataforma para intercambiar ideas de iniciativas innovadoras de *Insurtech* y brindar asesoramiento sobre temas relacionados con *Insurtech,* según corresponda.
	SFC	Las empresas calificadas pueden ser puestas bajo un monitoreo y supervisión estrecha por parte de la SFC cuando operan en el *Sandbox*. En tales casos, el SFC puede participar en un diálogo más intenso con las empresas y puede resaltar las áreas de cumplimiento en las que pueden mejorar sus controles internos y la gestión de riesgos.
	HKMA	La HKMA creo una sala de chat que busca proporcionar comentarios de supervisión a los bancos y empresas tecnológicas en una etapa temprana cuando se están contemplando nuevas aplicaciones tecnológicas, lo que reduce el trabajo abortivo y acelera el despliegue de nuevas aplicaciones tecnológicas. Las empresas pueden acceder a la sala de chat a través de correos electrónicos, videoconferencias o reuniones cara a cara con el HKMA.
Reino Unido	Una vez que se solicita el acceso al *Sandbox* regulatorio, la FCA trabaja de manera abierta y transparente con el solicitante, para garantizar que en todo momento permanezca listo, dispuesto y organizado para cumplir con los estándares del *Sandbox.*	

Fuente: Elaboración propia.

Tabla B6

Categoría: Salida del Sandbox regulatorio.

País	Descripción
Malasia	Al finalizar la prueba, los participantes deben presentar un informe final que contenga: Resultados clave, indicadores de rendimiento clave frente a las medidas acordadas para el éxito o fracaso de la prueba y los resultados de la prueba; una cuenta completa de todos los informes de incidentes y resolución de quejas de los clientes; y, en el caso de una prueba fallida, las lecciones aprendidas de la prueba.

Canadá	Una vez completados los periodos de prueba, se precisó que el personal de la CSA debe revisar la solicitud de forma libre, para determinar los límites y las condiciones que se aplicarán a la empresa en el CSA *Regulatory Sandbox*, caso por caso, una vez que haya finalizado el periodo de prueba.	
Australia	Una vez transcurridos los 12 meses de exención, la empresa no podrá ofrecer el producto innovador hasta que cumpla con todos los requisitos legales y obtener la licencia ASF o establecer un acuerdo con una empresa que tenga licencia ASF.	
España	Se evalúan los resultados de las pruebas, y la autoridad supervisora tras consultar con el promotor decidirá sobre la caducidad de la licencia *Sandbox*.	
Singapur	Al salir del *Sandbox* regulatorio la entidad puede lanzar el producto al mercado solo si cumple condiciones previamente establecidas, es decir, MAS y la entidad deben estar de acuerdo en que la prueba cumplió con los resultados esperados y que la entidad puede cumplir con todos los requerimientos legales y regulatorios.	
Hong Kong	*IA*	El asegurador debe presentar al IA una estrategia de salida para la ejecución piloto si tiene que terminarse sin éxito, puesto que el *Sandbox* no es un medio para eludir los requisitos de supervisión aplicables y relacionados.
	SFC	Una vez que una empresa calificada ha demostrado que su tecnología es confiable y adecuada para su propósito, y que sus procedimientos de control interno han abordado adecuadamente los riesgos identificados, la empresa puede solicitar al SFC la eliminación o variación de algunas o todas las condiciones de licencia impuestas, por lo que puede llevar a cabo actividades reguladas y estar sujeto a la supervisión de la SFC en las mismas condiciones de las entidades con licencia que operan fuera del *Sandbox*.
	HKMA	No se menciona.
Reino Unido	Una vez que el solicitante haya sido autorizado por la FCA debe cumplir con estándares mínimos en todo momento, cumplir con las normas y principios relevantes para su negocio y enviar informes periódicos.	

Fuente: Elaboración propia.

Tabla B7

Categoría: Salida del Sandbox regulatorio.

País	Descripción	
Malasia	Al finalizar el período de prueba, la aprobación para participar en el *Sandbox* y cualquier flexibilidad regulatoria otorgada a los participantes expirará automáticamente, a menos que el participante haya obtenido una aprobación previa por escrito del BNM para una extensión del período de prueba. Sin embargo, se debe de considerar que el período de prueba inicial no debe exceder los 12 meses a partir de la fecha de inicio de la prueba. Para extender el período de prueba, los participantes deben enviar una solicitud por escrito al BNM a más tardar 30 días calendario antes de que finalice el período de prueba.	
Canadá	No se menciona	
Australia	ASIC puede otorgar una exención individual para extender el periodo de prueba la extensión es de 12 meses.	
España	De no cumplirse los resultados esperados, la concesión de una prórroga definida o indefinida, para el caso de que las actividades probadas aún no se encuentren reguladas tras esta fase o la obtención de una licencia ordinaria cuando las entidades *Fintech* o *Insurtech* hayan alcanzado la capacidad necesaria para cumplir con los requisitos habituales.	
Singapur	Se estableció que si existieran razones excepcionales por las cuales el servicio financiero propuesto no se pueda implementar en Singapur, el solicitante debe estar preparado para continuar contribuyendo de otra manera, además los escenarios de prueba, y los resultados esperados de la prueba en el *Sandbox* deben estar claramente definidos.	
Hong Kong	*IA*	No se menciona.
	SFC	Si la SFC considera que una empresa calificada que opera en el *Sandbox* no está en forma y no es adecuada para mantener la licencia, su licencia puede ser anulada.
	HKMA	No se menciona.
Reino Unido	Para los casos en los que no pueda emitir orientación individual o extensiones del periodo de prueba a entidades solicitantes, pero la FCA considera que está justificado a la luz de las circunstancias y características particulares del *Sandbox*, se puede emitir	

	cartas de *no acción de cumplimiento*. Mientras la entidad se ocupe de la FCA abiertamente, cumpliendo con los parámetros de prueba acordados y trate a los clientes de manera justa, la FCA aceptará la posibilidad de que puedan surgir problemas inesperados y no tomará medidas disciplinarias.

Fuente: Elaboración propia.

Tabla B8

Categoría: Forma de aplicar.

País	Descripción
Malasia	El BNM detalló formatos especiales e información específica para las entidades solicitantes.
Canadá	Para presentar una solicitud para aplicar en el *Regulatory Sandbox*, la entidad solicitante debe comunicarse con el regulador de valores en la jurisdicción donde se encuentra su oficina central. Para ello, se asignó a un personal dedicado, quien debe estar disponible para entidades *Fintech* que buscan asistencia para navegar el entorno regulatorio de valores.
Australia	No se necesita aplicar para obtener este beneficio, es decir, se determinó que si la empresa cumple con los requisitos de elegibilidad y sigue las condiciones previstas, tiene la exención por 12 meses. No obstante, el único requisito es que debe notificar a la ASIC antes de usar la exención de licencia y enviar determinada información, para que posteriormente ASIC notifique por escrito la fecha en que inicia su exención de licencia. Así mismo, la guía destaco claramente que el uso de la exención de la licencia no significa que la empresa haya obtenido la licencia o autorización ASF.
España	El supervisor competente debe analizar el proyecto presentado y los documentos que se acompañen y resolverá sobre la concesión o no de la licencia. Además, la autoridad supervisora tendrá la facultad de conceder licencias condicionadas al cumplimiento de determinados requisitos o, incluso, firmar protocolos individuales cuando considere necesario que ambas partes, supervisor y solicitante manifiesten por escrito los distintos compromisos asumidos para la concesión de la licencia.
Singapur	Existen formatos especiales e información específica que debe enviarse por correo electrónico a un oficial de revisión del MAS. Así mismo, se crearon tres etapas de aplicación como las que se mencionan a continuación:

		Etapa de aplicación: se recibe la aplicación y ya que tiene toda la información requerida tiene 21 días hábiles para informar al solicitante si tiene potencial para ser elegido. Etapa de evaluación: no existe un tiempo predeterminado, ya que la evaluación dependerá caso por caso. MAS le informará por escrito al solicitante el resultado. En caso negativo, el solicitante puede volver a aplicar. Etapa de experimentación: es la etapa de prueba. La entidad debe notificar a sus clientes que el producto que ofrece está en un *Sandbox* regulatorio, notificar los riesgos asociados, y obtener su consentimiento.
Hong Kong	*IA*	El IA cuenta con un grupo de trabajo *Future Task Force* (FTF) enfocado a promover la aplicación *Fintech* en la industria de seguros, misma que brinda orientación para la aplicación de un *Sandbox* regulatorio.
	SFC	El SFC creo un portal en línea de asesoramiento y seguimiento en línea.
	HKMA	El HKMA recomienda que los bancos y sus empresas tecnológicas asociadas que intenten acceder al FSS que se pongan en contacto con el HKMA antes de tiempo. El HKMA está listo para discutir con ellos individualmente sobre la flexibilidad de supervisión apropiada que se les puede proporcionar dentro del FSS.
Reino Unido	No es necesario aplicar para obtener este beneficio. Si la empresa cumple con los requisitos de elegibilidad y sigue las condiciones previstas por la FCA.	

Fuente: Elaboración propia.