RELACIÓN ENTRE RIESGOS ESTRATÉGICOS Y CIBERESILIENCIA EN EMPRESAS FINTECH

Relationship Between Strategic Risks and Cyberesilience in Fintech Companies

JOSÉ ANDRÉS PALACIO VALENCIA

ANA MARÍA GÓMEZ CARDONA

CARLOS DANIEL CACERES CORTES

Trabajo de Grado

Asesor

Ana María Corrales Estrada

UNIVERSIDAD EAFIT

ESCUELA DE ADMINISTRACIÓN

MAESTRÍA EN ADMINISTRACIÓN DE RIESGOS

MEDELLÍN

2022

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

La industria Fintech, cada vez de mayor relevancia en el mundo y en Latinoamérica, basa su operación y estrategia en las tecnologías de información, razón por la cual la gestión de sus riesgos se convierte en un pilar fundamental de la organización. El rápido aumento de la adopción tecnológica en el mundo y la exponencial exposición a los ciberiesgos, llevan al concepto de ciberesiliencia a tener cada vez mayor relevancia, como respuesta al aumento y la especialización de los impactos asociados a la materialización de estos riesgos, lo cual es una constante a nivel global para todo tipo de organizaciones. Este trabajo de investigación aborda, desde la perspectiva de riesgos estratégicos, el concepto de la ciberesiliencia como una buena práctica a implementar en el sector Fintech, específicamente en Colombia. Para esto se analizan cinco casos de estudio de empresas colombianas del sector Fintech, por medio de un análisis cualitativo. Este trabajo concluye que las compañías Fintech en la región, y principalmente en Colombia, aún requieren alcanzar una mayor madurez para la incorporación del concepto de ciberesiliencia como elemento estratégico.

Palabras clave: resiliencia, riesgos estratégicos, Fintech, ciberesiliencia

ABSTRACT

The Fintech industry, which becomes every time more relevant in the world and in the Latin American region, bases its operation and strategy on information technologies, which is why risk management has become a main pillar of these companies. The rapid increase of technological adoption in the world, and the exponential exposure to cyber risks, makes the concept of cyber resilience increasingly relevant, as a response to specialized and more impacts associated with the materialization of these risks. This paper addresses, from the perspective of strategic risks, the concept of cyber resilience as a good practice to be implemented in the Fintech sector, specifically in Colombia. For this purpose, five case studies of Colombian companies in the Fintech sector are analyzed through a qualitative survey including the aforementioned concepts. This paper concludes that Fintech companies in the region, and mainly in Colombia, still need to reach a greater maturity for the incorporation of the concept of cyber resilience as a strategic element.

Keywords: *resilience, strategic risks, Fintech, cyberresilience.*

INTRODUCCIÓN

En las últimas décadas los avances tecnológicos han impactado la forma en la que los seres humanos nos comunicamos y relacionamos, así como la manera en la que producimos y consumimos bienes y servicios. Entre los impactos destacados se encuentran las mega tendencias, las tendencias de los consumidores y las de las industrias, su uso frecuente nos ha llevado a que cada vez seamos más dependientes de este tipo de herramientas (Barretti Mascarenhas et al., 2021).

Como resultado de estos avances tecnológicos, el sector financiero tradicional ha empezado a transformarse al incorporar herramientas tecnológicas que aporten a eficiencias en el core de negocio por medio de menores costos. De esta forma, surgieron nuevas compañías con una estrategia basada en tecnología, y con el fin de ofrecer productos y servicios financieros, y competir a través de estos con el sector financiero tradicional (Lee & Shin, 2018). A estas nuevas compañías se les conoció más adelante como Fintech, por su abreviación de financial technology (Cheng & Qu, 2020).

Las compañías Fintech han cobrado mayor relevancia alrededor del mundo, entendidas como aquellas que ofrecen productos y servicios financieros al apalancar su modelo de negocio en la innovación y en las tecnologías de información. En su estudio sobre el impacto de las compañías Fintech, Weill (2020) adopta la definición del sector según el Financial Stability Board (FSB) como todos aquellos procesos tecnológicos que promueven la innovación financiera y aportan a la creación de nuevos modelos de negocio, aplicaciones o productos relacionados con los mercados, instituciones financieras y la prestación de servicios financieros.

El crecimiento de este sector ha sido bastante significativo, hasta tal punto que, en el año 2020, su comportamiento sirvió como referente para otras industrias al momento de atender la emergencia del entorno global causada por la pandemia de la COVID-19, pues otros sectores se vieron en la necesidad de adoptar las tecnologías de información en su modelo operativo debido a las restricciones mundiales. Incluso, la situación y la regulación llevaron al sector financiero tradicional a implementar nuevas soluciones y herramientas tecnológicas como las aplicaciones móviles o la banca en línea para continuar con la oferta de sus productos y servicios a sus clientes, aun con las restricciones sanitarias (Fu & Mishra, 2022).

La naturaleza y el modelo de negocio de las empresas Fintech las hace más susceptibles a los riesgos relacionados con la seguridad de la información, la ciberseguridad y los riesgos de continuidad de negocio, los cuales se materializan en el ámbito operativo y estratégico (Boot et al., 2021). Debido al alcance propuesto de esta investigación, la gestión de los riesgos operativos asociados a las Fintech se considera embebida dentro del modelo de negocio, y el mismo se enfoca en el concepto de la ciberesiliencia en el sector Fintech, desde la óptica de la gestión del riesgo estratégico.

El contexto para Colombia en relación con las estadísticas asociadas al Sector Fintech y los riesgos a los que se encuentra expuesto, se obtiene a través de los informes presentados por

Fortinet y la Alianza del Pacífico, los cuales evidencian un aumento significativo de los ciberataques, tanto a nivel global, como en Colombia, al generar impactos financieros, legales y reputacionales. De acuerdo con la firma de seguridad Fortinet (2022), durante 2021, se registraron 289 mil millones de intentos de ciberataques en América Latina y el Caribe, con un aumento del 600% con respecto al año anterior, de los cuales 11,2 millones fueron dirigidos a empresas colombianas. IBM (2022) identifica que las empresas del sector financiero y asegurador continúan como uno de los principales objetivos de los ciberataques, siendo blanco del 15% en Latinoamérica y del 22,4% a nivel mundial. Adicionalmente, de acuerdo con Finnovista, (2021) y el informe "Radar Fintech e Incumbentes 2021" de la Alianza del Pacífico y el BID, Colombia logró en la XV Cumbre de la Alianza del Pacífico la aprobación de los mandatos que implementaban la necesidad de generar y motivar la innovación para el sector financiero y poder digitalizar la economía en general. Con respecto a la regulación, bajo la premisa de que cada país tiene un esquema diferente según sus particularidades, se llegó a la conclusión de que la regulación aplicable a una muestra de empresas tomadas de la Alianza del Pacífico es adecuada (42% en promedio); sin embargo, en Chile y Perú (53% y 32% respectivamente), no se evidencia la existencia de regulación.

La Alianza del Pacifico se encuentra compuesta por cuatro países (Chile, Colombia, México y Perú) y se consolida como la mayor región en cuanto a Fintech dentro del continente. De acuerdo con el reporte de Finnovista (2021), en la región de la Alianza operan más de 1.100 compañías Fintech. Este número de compañías reflejan que el sector triplicó su tamaño en tan solo cuatro años, lo cual se puede atribuir a los avances en términos de regulación Fintech en México y Colombia.

La reciente crisis asociada a la pandemia del COVID-19 ha puesto en evidencia la importancia a nivel empresarial de anticiparse y adaptarse a los cambios, independientemente del sector en el que operen, llevando a las empresas a generar capacidades como la resiliencia organizacional (Dupont, 2019; The Business Continuity Institute & British Standards Institution, 2022).

Este trabajo busca entender la relación entre los riesgos estratégicos y la ciberesiliencia en las empresas del sector Fintech, con el objeto de identificar que estas estén en capacidad de hacer frente a los posibles incidentes cibernéticos, y evitar así que se ponga en peligro el cumplimiento de los objetivos estratégicos y su sostenibilidad en el tiempo. Adicionalmente, se busca identificar el nivel de madurez de las empresas Fintech en Colombia dentro del análisis con relación a la ciberesiliencia, para lo cual se utiliza el marco de ciberesiliencia "The Cybersecurity Capability Maturity Model" propuesto por (Barclay, 2014).

Con el propósito de entender el estado del sector Fintech frente a la implementación del concepto de ciberesiliencia en Colombia, y aportar a la investigación del tema en términos de riesgo estratégico, se analizaron los casos de cinco compañías colombianas del sector Fintech, y la forma en que se gestiona la ciberesiliencia y su relación con la gestión estratégica del riesgo, al considerar la rapidez con la que este sector debe adoptar tecnologías de acuerdo con el creciente aumento de los ciberiesgos.

La metodología de investigación empleada, de acuerdo con la pregunta de investigación, es cualitativa, exploratoria y descriptiva. Se seleccionó como herramienta para obtener

información de la realización de entrevistas, para lo cual se diseñó un protocolo de entrevista, el cual fue utilizado durante el desarrollo de estas, lo que posteriormente permitió realizar un análisis cruzado para determinar patrones de abordaje entre las diferentes compañías. Con el fin de garantizar la integridad y confidencialidad de la información proporcionada por las compañías analizadas, los resultados de este trabajo se presentan de manera consolidada.

Este documento se compone de las siguientes secciones: "Marco Teórico", en el que se hace referencia a la literatura existente sobre los conceptos de compañías Fintech, riesgos estratégicos y ciberesiliencia, incluyendo aquellos aspectos que se consideren relevantes para este análisis; "Aspectos Metodológicos", donde se explica la metodología utilizada para el desarrollo de las entrevistas y la recolección de la información; "Resultados", capítulo en el que se mencionan los principales hallazgos de las compañías analizadas de manera agregada; y finalmente, "Conclusiones y futuras líneas de investigación", donde se identifican posibles líneas de investigación derivadas de los resultados obtenidos y la información identificada dentro del marco teórico.

MARCO TEÓRICO

Los avances tecnológicos de las últimas décadas han llevado a las diferentes industrias a transformarse y dar paso a lo que hoy conocemos como la cuarta revolución industrial, la cual tiene en cuenta los avances en las tecnologías de información y su rápida adopción en todo tipo de organizaciones, lo que lleva tanto a la modificación de sus procesos y actividades, como a la transformación en sus modelos de negocio y objetivos estratégicos (Abbasi et al., 2021).

Una de las industrias más impactadas por los cambios y avances tecnológicos ha sido la de servicios financieros, al ser una de las industrias que impulsa la economía como un todo, dada su capacidad para financiar los diferentes sectores. De acuerdo con Lee & Shin (2018), estos avances se han generado tanto en el uso de las tecnologías de información, las cuales buscan eficiencias en el core de negocio financiero tradicional, así como en la creación de una nueva industria: las compañías Fintech, al incorporar nuevos modelos de negocio para ofrecer productos y servicios financieros. Adicionalmente, se han llevado a cabo acciones como la adopción de sistemas financieros en línea y la automatización de los procesos, buscando entregar a los clientes una mayor conveniencia y beneficios al momento de utilizar el servicio (Boot et al., 2021).

Durante los últimos años, el sector financiero ha cobrado mayor importancia, al ser objeto de transformaciones a causa de las tendencias y las recesiones mundiales (Deloitte, 2017). Este sector empezó a modificar su estrategia de negocio a través de la adopción de las tecnologías de información, lo cual trasladó los riesgos asociados a la tecnología de un nivel operativo y táctico, a un nivel estratégico (Deloitte, 2018). Esta adopción se aceleró aún más a causa de las restricciones de la pandemia del COVID-19, dentro de las cuales se encuentran las limitaciones al libre movimiento relacionadas con el miedo al contagio de la población, así como la restricción del uso del dinero en efectivo, debido a que era uno de los posibles medios de transmisión (Al Nawayseh, 2020).

Adicionalmente, se plantea que el sector financiero fue uno de los principales beneficiados de la cuarta revolución industrial, pues pudo optimizar sus costos y gastos de operación, aumentar su rentabilidad, acelerar la inclusión financiera y mejorar la experiencia del cliente (Boot et al., 2021). Sin embargo, dicho crecimiento también ha generado la aparición de nuevos riesgos, por lo que se requiere un soporte tecnológico robusto y eficiente para mitigarlos, y explotar las cualidades de las herramientas tecnológicas existentes (Jiao et al., 2021).

El abordaje del riesgo estratégico dentro de esta investigación, pese a que existen diversas definiciones de su concepto, se realiza de acuerdo con lo planteado por los autores Montoya & Rivas (2018) quienes lo definen en función de la desviación sobre el cumplimiento de los objetivos estratégicos, e identifican que existen algunas firmas consultoras y organizaciones internacionales que se refieren a este concepto como la incertidumbre y los errores que

pueden presentarse, tanto en la etapa de formulación, como de ejecución y desarrollo de la estrategia de las compañías.

Con relación al concepto de la ciberesiliencia, se toma como referencia lo expuesto por Dupont (2019), quien plantea que el sector Fintech se ha visto obligado a adoptar desde sus planteamientos y riesgos estratégicos la ciberesiliencia, definiéndolo como la capacidad de resistir, recuperarse y adaptarse a los impactos adversos causados por los riesgos cibernéticos. El concepto de resiliencia organizacional hace referencia a la capacidad de adaptación que tiene la organización al permear su cultura organizacional, al igual que las competencias y habilidades de sus empleados, para ser auto resilientes y contar con competencias como la adaptabilidad, resistencia, optimismo, autoeficacia, autoestima y confianza (Menéndez Blanco & Montes Botella, 2016). Para identificar el nivel de adopción de las anteriores competencias, Barclay (2014), propone su "The Cybersecurity Capability Maturity Model", como un marco de referencia aplicable a todo tipo de organizaciones, y el cual será empleado para evaluar el nivel de madurez en las empresas Fintech entrevistadas, su modelo propuesto propone 6 niveles que evalúan las capacidades y los niveles de madurez relacionados con el mejoramiento de los niveles de seguridad y la ciberesiliencia.

Luego de entender el contexto del sector financiero, y dentro de este, específicamente las empresas Fintech, así como la relación de estas con el riesgo estratégico y la ciberesiliencia, se ahonda en los conceptos propuestos en este trabajo.

SECTOR FINTECH

La palabra Fintech nace a partir de la abreviación de financial technology y se ha utilizado para referirse a las empresas que ofrecen productos y servicios financieros por medio de herramientas tecnológicas (Cheng & Qu, 2020). Gomber et al. (2018) afirman que este sector surgió en el siglo XXI por medio de la innovación en herramientas tecnológicas en los procesos que soportan la operación, y que no son perceptibles al cliente. Sin embargo, más adelante esta aproximación tecnológica fue adoptada para otros procesos de las compañías del sector financiero que sí tienen una relación directa con la experiencia del cliente (Gomber et al., 2018).

La revolución tecnológica de la década de 1990 produjo una reducción en los costos de las transacciones financieras, lo que llevó a la creación del e-finance: productos y servicios financieros ofrecidos a través de herramientas tecnológicas. Esta reducción en costos trasladó el uso de la tecnología a diferentes procesos de las compañías financieras, hasta el punto en que los bancos, por ejemplo, redujeron el tamaño y número de sus sucursales físicas para ofrecer su servicio por medio de herramientas y plataformas tecnológicas (Lee & Shin, 2018). Según Kou et al., (2021), los principales beneficios de la innovación tecnológica en los servicios financieros son su contribución al desarrollo de la industria por medio de la reducción de costos, la oferta de servicios de mejor calidad y el mejor servicio al cliente.

La situación actual permite el surgimiento de las Fintech 4.0, como empresas emergentes y tecnológicas que prestan servicios a los agentes económicos (personas naturales y personas jurídicas) de forma directa, y así obviar por medio de la tecnología a los intermediarios financieros convencionales y sus costos asociados (Belozyorov et al., 2020). En los últimos

años, estas compañías que ofrecen servicios financieros y tienen base tecnológica, han ganado cada vez mayor relevancia alrededor del mundo, lo que se puede explicar por la desconfianza de los consumidores en el sector tradicional, los menores costos asociados a su operación y a la agilidad de este tipo de empresas, en comparación al sector bancario tradicional (De Haan et al., 2020).

Se observa que la adopción masiva de herramientas financieras digitales se da principalmente por avances en los sistemas de pago electrónico, las nuevas políticas y leyes regulatorias (De Haan et al., 2020; Belozyorov et al., 2020), así como la aparición de servicios financieros de nueva generación, disponibles a través de dispositivos móviles con acceso a Internet, lo que se denomina “Fintech" (Belozyorov et al., 2020).

Carias et al., (2021) identifican que las pymes (pequeñas y medianas empresas) en algunas economías representan hasta cerca del 90% de empresas, las cuales significan un actor importante en la economía local de cada país, ya que contribuyen al desarrollo por medio de la creación de productos, empleos y pago de impuestos. Este planteamiento se observa también en los resultados del estudio Radar Fintech e Incumbentes de la Alianza Pacífico de Finnovista (2021), los cuales revelan que el crecimiento significativo del sector Fintech genera impactos importantes en las economías, pues es un mecanismo de inclusión financiera que permite el acceso a servicios financieros a microempresas, pymes o consumidores de bajos ingresos. Teniendo en cuenta tanto el músculo financiero de las pymes, como su sostenibilidad en el tiempo, es esencial evaluar los riesgos a los que estas se encuentran expuestas, incluidos aquellos asociados al uso de la tecnología, los mecanismos que pueden mejorar su eficiencia, y viabilizar un modelo de negocio sostenible (Abbasi et al., 2021).

El sector financiero ha reconocido la importancia del uso de la tecnología para mejorar su rendimiento y la satisfacción de los clientes (Paulet & Mavoori, 2020), lo que se relaciona con la necesidad de innovar en el uso de herramientas tecnológicas, con el fin de poder cumplir las expectativas de los clientes (Sybirianska et al., 2018). Es evidente pues que la innovación financiera ha puesto a disposición de los clientes una banca más fácil, accesible y en menor tiempo, al ubicar las necesidades del usuario en el centro del negocio (Paulet & Mavoori, 2020). Igualmente, el uso de las herramientas tecnológicas ha aportado a la disminución de los costos asociados a la operación y, por lo tanto, a una mayor eficiencia operativa (De Haan et al., 2020).

Tras entender los principales elementos de las compañías Fintech, vale la pena aclarar que su principal diferencia con el sector financiero tradicional radica en que, aunque ambos tipos de compañías puedan ofrecer los mismos productos y servicios, las Fintech nacen como empresas tecnológicas, y no con la robustez operativa que implica la creación de una empresa financiera tradicional (Jiao et al., 2021). Todos los procesos de las Fintech se basan en herramientas tecnológicas, a diferencia del sector financiero tradicional, en el que se han implementado nuevas herramientas, pero su modelo de negocio no se basa en tecnología (Sybirianska et al., 2018).

Aunque el sector Fintech es considerado limitado, dentro de él, se pueden categorizar las compañías según las características de la empresa o del producto o servicio ofrecido. Según Kou et al. (2021), las compañías Fintech más relevantes en el mundo son las de pagos y

transferencias, aunque también existen otro tipo de clasificaciones como las de ahorro, crédito y manejo de finanzas personales (PFM, por sus siglas en inglés), entre otras.

El aumento de la adopción tecnológica por parte de las compañías Fintech en el mundo, también se ha atribuido a los entes reguladores. En la actualidad, muchos países aplican políticas destinadas a ampliar el acceso del público a los servicios financieros, con el fin de aumentar la inclusión y educación financiera, tanto a nivel nacional como internacional. Estas políticas permiten que un mayor número de personas accedan a servicios financieros a través de soluciones tecnológicas que aporten a los indicadores de inclusión financiera y bancarización (Belozyorov et al., 2020).

Sector Fintech en Colombia

Según Finnovista (2021), equipo de investigación que monitorea la evolución y desempeño de las Fintech en América Latina, en los últimos años se ha logrado evidenciar un crecimiento, organización, y regulación en el sector Fintech, características que aportan a la consolidación de una primera ola de Fintech en la región. La industria se enfoca principalmente en ofrecer propuestas de valor directas a personas naturales y jurídicas en segmentos como préstamos (lending) y pagos, los cuales presentaron un crecimiento de rentabilidad generada por la pandemia de COVID-19. La revisión de la literatura permite identificar a Colombia y Perú como países que sobresalen por el crecimiento en el sector, frente a los demás países de la Alianza del Pacífico (Finnovista, 2021). La información relacionada con la Alianza del Pacifico entrega el contexto requerido para este trabajo al realizar una exhaustiva investigación sobre la evolución de las Fintech a nivel de Latinoamérica, la forma en que se encuentran reguladas y su nivel de adaptación al riesgo estratégico generado por el incremento de los incidentes cibernéticos, de forma general a nivel región y posteriormente desplegándolo por los países que hacen parte de la Alianza del Pacifico (Finnovista, 2021).

La incorporación y adopción de tecnologías por parte de la población, aumenta la importancia de la creación y desarrollo de las compañías Fintech en los países de la Alianza del Pacífico, esta transformación fue acelerada por la pandemia de la COVID-19 (Al Nawayseh, 2020). En línea con esta aceleración en la incorporación y adopción de tecnológicas por parte de la población, la revisión de literatura evidencia el aumento de los ciberataques en estas empresas, y la necesidad de desarrollar medidas para la mitigación y gestión de los riesgos estratégicos asociados a estos. El reporte Finnovista (2021) entrega una encuesta con datos relevantes sobre las tecnologías que las entidades financieras han aplicado tanto en sus procesos operativos, como en el desarrollo de sistemas de riesgos estratégicos. Este mismo reporte identifica que, a 2021, en Colombia operan 279 empresas en el sector, de las cuales 118 han iniciado operación en el año 2021, lo que posiciona al país como el segundo ecosistema Fintech más grande de la Alianza del Pacífico (precedido por México) y el tercero a nivel de la región (después de Brasil y México), impulsada a su vez, por la emergencia sanitaria de la COVID-19.

Menciona Rincón (2021) que en el caso de Colombia la asociación Colombia Fintech "agrupa más de 250 empresas del ecosistema de innovación financiera del país". De acuerdo con el reporte el tercer trimestre del 2021 se observó un incremento en la inversión mundial en estas compañías del 173%, que, en el caso de Colombia, genera ventas cercanas a los 3 billones de pesos al año y genera alrededor de 9.600 empleos. Como resultado de esto, Colombia ha incrementado su población bancarizada.

En Colombia, las empresas del sector Fintech por su tamaño y estructura pueden ser clasificadas, en su mayoría, como pymes, dado que el 89% de las Fintech registradas cuenta con menos de 100 empleados, para el 78% de estas su financiamiento o capital es inferior a los 500 mil dólares y para el 61% sus ingresos inferiores a 500 mil dólares al año (Decreto 1692 de 2020; Finnovista, 2021; Ley 905 de 2004).

La asociación Colombia Fintech (2022a) clasifica a las compañías según el producto o servicio ofrecido, de la siguiente manera: recaudación de fondos, banca virtual, monedas digitales, créditos, soluciones de aseguramiento (insurtech), manejo de finanzas personales (PFM), pagos digitales y soluciones regulatorias (regtech), entre otras. Para la prestación de estos servicios, las compañías Fintech emplean múltiples tecnologías, dentro de las cuales se encuentran principalmente las de finanzas abiertas y APIs (interfaz de programación de aplicaciones), Big Data (datos macro), cómputo en la nube, inteligencia artificial y machine learning (aprendizaje automatizado de las herramientas computacionales), biometría, billeteras móviles, blockchain, entre muchas otras (Finnovista, 2021).

El rápido desarrollo de las tecnologías para el sector financiero ha permitido el surgimiento y establecimiento de las empresas Fintech, aunque también su adopción trae como consecuencia una gran exposición a una nueva dimensión de riesgos relacionados con la seguridad de la información, la ciberseguridad y los riesgos de continuidad de negocio, los cuales se presentan tanto en el ámbito operativo como estratégico debido a las amenazas de ciberseguridad y las fallas inesperadas de los sistemas (Boot et al., 2021b; Uddin et al., 2020).

Tras el entendimiento del sector Fintech a nivel global y en Colombia, así como la identificación de su rápido crecimiento, la adopción acelerada de diversas tecnologías y como consecuencia, la exposición a nuevos riesgos operacionales y estratégicos (Jiao et al., 2021), este trabajo aborda, desde la perspectiva del riesgo estratégico, el concepto de la ciberesiliencia, como una buena práctica a implementar, en el sector Fintech en Colombia.

Regulación del Sector Fintech en Colombia

En Colombia, de acuerdo con (Finnovista, 2021), las compañías del sector Fintech presentan un crecimiento importante, sin embargo, a nivel regulatorio y de supervisión no se cuenta con una única autoridad, pues estas compañías responden a múltiples normativas aplicables, en dependencia del servicio ofrecido y el tipo de operaciones que realizan. En línea con lo anterior, Colombia Fintech (2022b) afirma que "Colombia no cuenta con una regulación Fintech específica; adicionalmente, las empresas Fintech deben cumplir distintas disposiciones, las cuales se encuentran en diferentes ámbitos del ordenamiento jurídico colombiano en dependencia del origen del financiamiento y de otras características particulares de cada una de las firmas".

Por ejemplo, en los casos de pagos digitales, en Colombia se tiene la necesidad de adaptar la normatividad vigente, al eliminar las retenciones de carácter tributario, permitiéndoles operar a las Fintech en igualdad de condiciones al sector bancario tradicional, lo cual es posible a través de la adopción obligatoria del open banking, que llevaría a una mayor bancarización de personas naturales y de empresas del sector pyme (Belozyorov et al., 2020; Rincón, 2021). En el caso de las compañías dedicadas al crowdfunding, estas son reguladas principalmente por el Ministerio de Hacienda y Crédito Público del Gobierno de Colombia, por medio de los decretos 1357 de 2018 y 1235 de 2020 (Finnovista, 2021). Las compañías que ofrecen sistemas de pago se encuentran reguladas por medio de la Superintendencia Financiera de Colombia (SFC) a través del decreto 2555 de 2010 y sus modificaciones, así como del decreto 222 de 2020, el cual promueve el acceso a productos transaccionales digitales (Finnovista, 2021; Rincón, 2021). Para la operación de factoring, la regulación se encuentra establecida de acuerdo con quién desarrolle esta actividad y sus clientes objetivos, identificándose a la Superintendencia Financiera de Colombia (SFC), la Superintendencia de Sociedades de Colombia o la Superintendencia de Economía Solidaria (Finnovista, 2021; Rincón, 2021), como ente regulador, de acuerdo con sus particularidades.

Actualmente en Colombia, se estableció a través de la Superintendencia Financiera de Colombia el Sandbox Regulatorio, el cual establece que las entidades reguladas y empresas Fintech con desarrollos tecnológicos regidos por la regulación, podrán probar hasta por dos años, productos, servicios y procesos o modelos innovadores, con la ayuda del regulador, previo a la etapa de supervisión (Rincón, 2021).

Frente a otros territorios, se identifica que el marco regulatorio europeo a través del Comité de Supervisión Bancaria de Basilea (2018), en su documento "Buenas prácticas e Implicaciones de los avances en tecno finanzas (fintech) para los bancos y supervisiones bancarios", establece que empresas que desarrollan actividades similares a las de la banca tradicional deben estar sujetas a las leyes y reglamentos establecidos para estos, al generar un marco regulatorio que integre el sector financiero. Adicionalmente, la Comisión Europea, con el objetivo de reducir los riesgos más comunes en el sector Fintech, busca implementar regulaciones específicas, a través del reglamento DORA (Digital Operational Resilience Act), esto debido al impacto que la materialización de los riesgos puede generar en este sector, y las posibles incidencias en el mercado financiero, por lo cual, el marco DORA establece los requisitos relacionados con la seguridad de las redes, con referencia a los sistemas de información y procesos con los que deberían contar las compañías financieras, necesarios para obtener un alto nivel de resiliencia operacional digital en entidades de diferente índole, entre las más destacadas: entidades de crédito, pasarelas de pago, compañías que ofrecen dinero electrónico, empresas de servicios de inversión, proveedores de servicios de suministro de datos, empresas de seguros y de reaseguros y proveedores terceros de servicios de TIC, lo que busca promover la resiliencia de las compañías al considerar las herramientas tecnológicas utilizadas, las cuales impulsan la creación de nuevas oportunidades de negocio (Comisión Europea, 2020). Esta regulación procura que las compañías del sistema financiero dispongan de las protecciones necesarias para lograr mitigar los ciberataques y otros tipos de riesgos a través de una adecuada gestión de la continuidad de negocio, para lo cual se incluirá un marco de supervisión para los proveedores

de servicios en la nube, al considerar que son un actor relevante al momento de proteger los datos de los diferentes grupos de interés (Comisión Europea, 2020; Comité Económico y Social Europeo, 2021).

En el caso de Colombia, a inicios del año 2022, el Gobierno Nacional, por medio de la Directiva Presidencial No. 02 de 2022 reitera la urgencia de adoptar una política pública en materia de seguridad digital. Para esto se impartieron directrices relacionadas con la gestión de riesgos dado el incremento de los incidentes cibernéticos con posibles impactos negativos en el entorno digital. Entre los principales dictámenes se encuentran el mantener actualizados los catálogos de sistemas de información, servicios y bases de datos, la solicitud y verificación de que los proveedores de servicios en la nube contratados cumplan de manera efectiva con los requerimientos mínimos en materia de ciberseguridad, la existencia de un procedimiento de gestión de incidentes que incluya la visión de seguridad digital, y la cooperación con las autoridades para soportar la contención, erradicación y recuperación ante incidentes y ataques digitales.

Posteriormente, en el mes de marzo se expidió el decreto 338 de 2022, el cual modifica el decreto único 1078 de 2015, al incluir un nuevo título donde se establecen los lineamientos generales para fortalecer la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital. Este tiene como objetivo blindar las infraestructuras críticas cibernéticas, especialmente las utilizadas para la prestación de servicios financieros, al mitigar los incidentes cibernéticos para el fortalecimiento de la seguridad digital. (Cybersecurity & Infraestrcuture Security Agency, 2021; Hernández, 2016).

En conclusión, las novedades informadas, los nuevos actores y las tendencias regulatorias, generan la necesidad de optimizar el marco regulatorio colombiano, así como establecer modelos y normativas que impulsen el crecimiento del sector hacia un modelo más eficiente, con menores costos, mejor servicio y un aumento de la inclusión financiera.

RIESGO ESTRATÉGICO EN COMPAÑÍAS FINTECH

Dentro de la gestión del riesgo organizacional, cada vez la gestión de riesgos estratégicos cobra mayor interés, aun siendo un concepto en desarrollo, especialmente en Latinoamérica (Deloitte, 2013). El riesgo estratégico se define como la desviación sobre el cumplimiento de los objetivos estratégicos (Montoya & Rivas, 2018). Bromiley et al., (2014) afirman que las primeras apariciones del concepto en la literatura se dieron entre 1985 y 1986, sin embargo, aún tras varias décadas, el término sigue siendo ambiguo y confuso, al hacer referencia a los eventos externos y las tendencias que pueden desviar el cumplimiento de los objetivos estratégicos (Bromiley et al., 2014). Dentro de la literatura el concepto se asocia a la incertidumbre, pues los eventos externos o las tendencias sobre las que se tenga certeza no deben considerarse riesgos, ya que serán un hecho, y la compañía debe prepararse para el momento en el que se materialicen. Bromiley et al., (2014) lo entiende como “la posibilidad de ocurrencia de un evento que pueda afectar la misión, visión, estrategia, objetivos y demás lineamientos organizacionales de alto nivel, con el fin de contrarrestarlo o transformarlo en oportunidades para la organización” (Nuñez et al., 2020).

Bromiley et al. (2014) cuestionan la gestión de riesgos de las empresas preguntándose si estas dan alcance a las necesidades de desarrollo, rentabilidad e ingresos sin considerarlos desde el componente estratégico, partiendo de este cuestionamiento se sugiere incorporar la gestión de riesgos estratégicos para monitorear el desempeño de la organización y gestionar oportunamente las variables del entorno que podrían afectar de manera importante los resultados de la organización e inclusive su continuidad.

Teniendo en cuenta la acelerada adopción tecnológica por parte de las empresas del sector financiero desde la década de 1990 (Lee & Shin, 2018), se observa una mayor susceptibilidad a los riesgos relacionados con la seguridad de la información, la ciberseguridad y los riesgos de continuidad de negocio, los cuales se materializan en el ámbito operativo y estratégico (Boot et al., 2021), debido a esto, las gestión de riesgos estratégicos se identifica como una herramienta clave para hacer frente a estos riesgos. En las Fintech, la gestión del riesgo estratégico es aún más incipiente debido al modelo de negocio basado en el uso de herramientas tecnológicas, por lo que se generan nuevos riesgos asociados a los cambios en el modelo operativo y estratégico de la compañía, tal y como lo menciona Jiao et al. (2021). Lo que representa un reto, ya que, para poder beneficiarse de la implementación de tecnologías, las compañías deben hacer frente a estos riesgos (Jiao et al., 2021).

Adicionalmente, debido a la naturaleza del negocio, de acuerdo con (Senyo & Osabutey, 2020) se concluye que existen riesgos inherentes a este, como la pérdida de activos financieros y de datos personales, los cuales modelan las decisiones estratégicas. En línea con esta conclusión, Senyo & Osabutey (2020) realizaron una investigación con el fin de identificar las razones por las que un usuario decide adoptar una tecnología, y se encontró que la confianza en los intermediarios y en el servicio tienen una correlación negativa con la adopción de la tecnología, lo que genera una relación directa entre la percepción por parte del cliente financiero con la seguridad de sus datos y activos, su confianza en el producto y la adopción de la tecnología.

CIBERESILIENCIA EN COMPAÑÍAS FINTECH

La ciberseguridad y las fallas inesperadas de los sistemas forman parte del contexto organizacional de las Fintech, al ser empresas de base tecnológica, lo que genera interés en la gestión de una nueva clasificación de riesgos (Uddin et al., 2020). Estos riesgos se sustentan en el uso de nuevas tecnologías como la inteligencia artificial y el uso del internet para poder ofrecer nuevas oportunidades a inversionistas locales y extranjeros (Jiao et al., 2021). Por otra parte, el crecimiento acelerado ha traído consigo beneficios y riesgos asociados a la sofisticación, frecuencia y severidad de los ciberataques, lo que genera un cambio en el enfoque tradicional para la gestión del riesgo, y abre espacio a la ciberseguridad al buscar proteger completamente la integridad de sus sistemas informáticos (Dupont, 2019).

El ritmo acelerado en el crecimiento de los ciberataques ha llevado a la ciberseguridad a evolucionar en la gestión de las ciberamenazas, lo cual genera que las organizaciones adopten el concepto de ciberesiliencia, el cual se basa en la capacidad organizacional para anticipar, detectar, soportar, recuperarse y evolucionar después de los incidentes cibernéticos de manera estratégica (Carías et al., 2020). La aplicación de este concepto responde a la necesidad de monitorear y proteger diferentes tipos de servicios tecnológicos en los que se

soporta la operación del negocio y la entrega del servicio. Las razones que generan la indisponibilidad de servicios tecnológicos críticos como el Internet y los canales de comunicación pueden afectar el desarrollo de las empresas del sector, al priorizar la afectación de estos servicios sobre la afectación de la información (Boot et al., 2021).

El World Economic Forum (2022) en su "The Global Risks Report 2022", identifica dentro del top diez de los riesgos que se agudizaron tras el inicio de la pandemia generada por el COVID-19 las fallas de ciberseguridad y su potencial de convertirse en una amenaza crítica para el mundo en los próximos cinco años, se estima que las fallas de ciberseguridad seguirán poniendo a prueba los sistemas del sector financiero en los próximos cinco años, dada la disminución paulatina de la percepción de su impacto en la próxima década, debido a la creciente preocupación de los riesgos de origen económico, sociales y medioambientales. Finalmente, se debe considerar el factor humano como una de las causas de la materialización de los incidentes cibernéticos, para lo cual este mismo informe evidencia que el 95% de los eventos de ciberseguridad están relacionados con el factor humano y representan aproximadamente el 43% del total de las brechas de seguridad.

En contraste con estas tendencias, la dependencia generalizada y el incremento en la complejidad de los sistemas digitales, así como el rápido aumento de las ciber amenazas superan la capacidad de las organizaciones para gestionar este tipo de riesgos de manera efectiva (Dupont, 2019; WEF, 2022). Esto se evidencia en las vulnerabilidades que persisten en antiguos sistemas de información, y en la adopción de nuevas tecnologías, lo cual genera el incremento gradual de las brechas de seguridad (WEF, 2022). Para el caso específico del sector financiero, los principales objetivos de los ataques se relacionan con el robo de información valiosa, de recursos financieros importantes, o para la solicitud de rescates por la información a cambio de grandes sumas de dinero (Dupont, 2019).

De acuerdo con Finnovista (2021), el 86% de las empresas Fintech en Colombia considera que existen ciber amenazas para su negocio y de estas, solo el 44% afirma tener una solución robusta para hacer frente a estas amenazas. Adicionalmente, el 42% de las empresas entrevistadas considera que actualiza sus sistemas de protección de manera adecuada, y el 8% no cuenta con una solución ni con acciones de mitigación. A pesar de estos esfuerzos, los ataques cibernéticos evolucionan continuamente y son cada vez más difíciles de predecir debido a su complejidad, pues se disminuye la capacidad de respuesta por parte de las organizaciones (BCI, 2022). Es por esto por lo que se consideran inevitables, no solo para las compañías Fintech, sino también para las grandes instituciones financieras tradicionales, sin importar la cuantía de las inversiones en tecnología para mitigar sus impactos (Dupont, 2019).

Según (Dupont, 2019), "la creciente sofisticación, frecuencia y gravedad de los ciberataques dirigidos a las instituciones del sector financiero ponen de manifiesto su inevitabilidad y la imposibilidad de proteger completamente la integridad de los sistemas informáticos críticos".

Por su parte, BCI menciona que "las organizaciones se esfuerzan por garantizar que cuentan con medidas de ciberseguridad a prueba de fallos, sin embargo, ir un paso por delante de los atacantes es un reto, sobre todo con el creciente número de ataques" (BCI, 2022).

En este contexto, el concepto de ciberesiliencia toma mayor relevancia, como un nuevo enfoque para que la organización pueda hacer frente a los rápidos cambios, que mantenga la continuidad del negocio a pesar de las situaciones desconocidas, inesperadas y adversas, y que sea sostenible independientemente de los cambios en el contexto (Bejarano et al., 2021; Carías et al., 2020). Adicionalmente, este contexto lleva a utilizar el concepto de ciberseguridad, el cual busca que las compañías cuenten con la capacidad de proteger la confidencialidad, integridad y disponibilidad de los activos de información, a través de la protección y detección, apoyados en la tecnología y los recursos humanos (Carías et al., 2020; Dupont, 2019), ambos conceptos relacionados con los riesgos de ciberseguridad. Sin embargo, desde el concepto de ciberesiliencia, se identifica la necesidad de realizar actividades a nivel organizacional para anticipar, detectar, entender, recuperar y evolucionar, a través de un enfoque holístico con la integración de varias áreas del conocimiento, incluyendo, pero no limitándose a la ciberseguridad (Bejarano et al., 2021; Carías et al., 2020). Las principales diferencias entre los conceptos de la ciberesiliencia y ciberseguridad tradicional según (Bejarano et al., 2021; Carías et al., 2020) se presentan en la Tabla 1.

Tabla 1: Diferencias entre los conceptos de ciberseguridad y ciberesiliencia.

Elementos del Concepto	Ciberseguridad	Ciberesiliencia
Objetivo	Proteger los sistemas de tecnología de la información.	Garantizar la continuidad del negocio, bajo el contexto de prevenir, detectar, contener y recuperar y minimizar el tiempo y el impacto al negocio.
Propósito	Estar a prueba de fallos.	Contar con la capacidad de adaptarse y continuar con los procesos y funciones de negocio.
Enfoque	Una sola capa de protección enfocada en aplicar la seguridad desde el exterior de la organización	Enfoque holístico, múltiples niveles de la protección y colaborativo (red de organizaciones).
Alcance	Gestión reactiva y protectora.	Gestión sistemática, proactiva y con enfoque holístico.
Plataforma Tecnológica	Incorporación de las mejores prácticas de seguridad para la industria TIC.	Integración de las mejores prácticas relacionadas con la seguridad industria TIC, continuidad del negocio y otras disciplinas.

Fuente: (Bejarano et al., 2021; Carías et al., 2020)

Finalmente, el concepto a utilizar para referirnos a la ciberesiliencia será el propuesto por Instituto Nacional de Ciberseguridad (2020), definido como “la capacidad de un proceso,

negocio, organización o nación de anticipar, resistir, recuperarse y evolucionar para mejorar sus capacidades frente a condiciones adversas, estrés o ataques a los recursos cibernéticos que necesita para funcionar".

Ciberesiliencia en el Sector Fintech en Colombia

El sector Fintech en Colombia, de acuerdo con Finnovista (2021), se encuentra conformado en su gran mayoría por pymes, lo cual significa que estas organizaciones cuentan con recursos limitados para hacer frente a los riesgos de ciberseguridad, aumentado su vulnerabilidad ante los ataques, en contraste con lo que puede suceder con las grandes instituciones financieras. Esto lleva a un impacto en su sostenibilidad, así como a la necesidad de abordar los riesgos relacionados con ciberataques con un enfoque diferente al tradicional, pues se requiere una capacidad organizacional que haga un uso eficiente de los recursos limitados que puede tener la organización, al adoptar un marco de referencia asociado a la ciberesiliencia, ajustado a la realidad de las pyme con el objetivo de garantizar los estándares de calidad, seguridad, disponibilidad, eficiencia e interoperabilidad del negocio. (Bejarano et al., 2021; Carías et al., 2020).

Este marco de referencia es propuesto por Carías et al. (2020), y se obtiene a partir de la comparación de 18 marcos de referencia propuestos por diferentes organismos e instituciones a nivel global, dentro de los cuales se identifican dimensiones asociadas a: gobernanza, gestión del riesgo, gestión de activos, gestión de amenazas y vulnerabilidades, análisis de incidentes, sensibilización y formación, seguridad de la información, procesos de detección y supervisión, y la gestión de la continuidad del negocio, intercambio de información y comunicación.

Al ampliar el alcance de la dimensión del intercambio de información y comunicación, a nivel de las iniciativas globales, Panetta (2018) destaca que las instituciones financieras de los países del G7 identifican que la seguridad del sector financiero requiere tanto del enfoque tradicional basado en estándares estrictos de ciberseguridad, así como de la cooperación entre las diferentes instituciones, reconoce adicionalmente que a nivel internacional la ciberseguridad se destaca como una prioridad estratégica, a la cual se le identifica su aporte a la iniciativa "Cyber Resilience Strategy for Financial Market Infrastructure". Para el entorno colombiano, el Ministerio de la Tecnología de Información y las Comunicaciones a través del Decreto 338 de 2022 adicionó al Decreto único 1078 de 2015, el cual regula el sector de las tecnologías de la información y las telecomunicaciones, algunos lineamientos generales para la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital, destacándose el establecimiento del modelo de gobierno para la seguridad digital, las instituciones participantes y los principios de colaboración que permiten el intercambio de información y el seguimiento de los incidentes. En este documento, se insta a los entes de regulación a expedir normativas para la protección de las infraestructuras críticas cibernéticas, dentro de las cuales se encuentran las empresas del sector financiero y de las TIC (CISA, 2021; Hernández, 2016).

Para entender la relación entre el riesgo estratégico y la ciberesiliencia, lo cual es el objetivo de esta investigación, se seleccionan las dimensiones de gobernanza y gestión de riesgos,

desde la óptica de la gestión de riesgos estratégicos para el diseño de la herramienta metodológica que se utiliza en el desarrollo de las entrevistas con las compañías dentro del estudio.

MODELO DE MEDICIÓN DE CAPACIDADES EN CIBERSEGURIDAD

Para la medición de la madurez y la adopción de las capacidades en ciberseguridad, se consideraron los modelos propuestos por el Instituto Nacional de Ciberseguridad (2020) y por Barclay (2014), The Cybersecurity Capability Maturity Model", adoptando este último para la presente investigación. El emplear los modelos de medición de capacidades como una herramienta de gestión para la organización, permite identificar el abordaje estratégico de la ciberseguridad.

(Barclay 2014), categoriza la etapa en la que se encuentran las organizaciones con referencia a su preparación para responder ante las amenazas y vulnerabilidades en constante evolución, que se desprenden de la adopción de la tecnología, a través de la evaluación de las capacidades que tienen que ver con los aspectos sociales, operativos, formativos, técnicos y organizacionales, proponiendo seis etapas para clasificar las organizaciones. Dichas etapas se comparan con el ciclo de vida del ser humano, así: indefinido/prenatal, básico/infante, inicial/niño, definido/adolescente, dinámico/adulto y optimización/sabio. El modelo propone indicadores para la valoración del nivel, teniendo en cuenta: la actitud ante amenazas y vulnerabilidades, el desarrollo tecnológico, la respuesta social y las medidas tomadas para el desarrollo de la organización, que se valoran a nivel tanto técnico, del negocio, legal y regulatorio, como operacional y en el desarrollo educativo y de capacidades dentro de la cultura organizacional.

Para entender la adopción de la ciberesiliencia, en las entrevistas se hace uso del anterior modelo, incorporando en el diseño de la herramienta metodológica los conceptos relacionados con esta, entre los que se destacan: garantizar la continuidad del negocio, la capacidad de adaptación y la adopción de un enfoque holístico para que la organización pueda "hacer frente a los rápidos cambios tecnológicos y los ciberriesgos asociados a estos" (Bejarano et al., 2021; Carías et al., 2020).

ASPECTOS METODOLÓGICOS

La metodología de investigación seleccionada para la realización de este trabajo de acuerdo con la pregunta de investigación es exploratoria y descriptiva, pues busca entender un fenómeno y sus componentes desde la literatura (Hernández et al., 2010). Para el desarrollo de la investigación, se realizó una revisión sistemática de literatura (Chicaíza et al., 2019), la cual entregó la definición de los conceptos relacionados en esta investigación, así como las relaciones entre ellos, objeto del análisis. El protocolo de investigación utilizado se presenta en la Tabla 2. La información recolectada en las entrevistas se analizó de manera cualitativa, con base en el marco teórico.

Tabla 2: Resumen Protocolo de Investigación

Elementos	Información / Resultado
Unidades de Análisis	Artículos, revistas y documentos relevantes cuyo contenido principal se centra en los vínculos entre: Fintech, gestión de riesgos, gestión de riesgos estratégicos, ciberesiliencia, ciberseguridad, resiliencia, desempeño, sostenibilidad
Tipo de Análisis	Exploratorio y descriptivo
Período de Análisis	2018-2022
Motores de Búsqueda	*Scopus and Web of Science*
Criterios de Búsqueda: (Asociación de palabras claves)	*Fintech and risk management* *Fintech and strategic risk management* *Fintech and resilience* *Fintech and cyber resilience* *Fintech and cybersecurity and resilience* *Fintech and performance and sustainability*
Número Total de Artículos Motores de Búsqueda	127
Búsquedas temáticas específicas	Artículos, revistas, reportes, entrevistas relacionadas informes sectoriales, legislación vigente, adopción tecnología, a
Número Total artículos temáticas específicas	45
Número Total de Artículos	172

A partir de la literatura identificada, inicialmente por los criterios de búsqueda, se identificó la necesidad de realizar búsquedas adicionales de aspectos específicos relacionados con los temas de investigación, principalmente información del Sector Fintech en Colombia y la regulación aplicable al sector. El proceso de selección de literatura se resume en la Tabla 3.

Tabla 3: Selección de Literatura

Búsqueda de Literatura	Revisión Preliminar Literatura		Análisis de Resultados	Incluidos en documento
	Revisión Adicional	Búsquedas Adicionales		
127	61	45	66	53

Posteriormente, se definió un instrumento metodológico que permitiera realizar un acercamiento con cinco empresas Fintech en Colombia, y entender por medio de entrevistas, el estado de las organizaciones frente a la ciberesiliencia y su relación con el riesgo estratégico, para finalmente contrastar con la información disponible sobre el fenómeno y sus componentes. Al considerar el número de compañías entrevistadas, la información

recopilada permitió realizar un análisis cruzado, sin llegar a resultados estadísticos. Cada una de estas compañías, desde los productos ofrecidos, hace parte de los principales tipos de compañías, de acuerdo con la asociación Colombia Fintech (Rincón, 2021), y la categorización del sector realizada por (Smith et al., 2020). Todas las empresas entrevistadas hacen parte de la asociación Colombia Fintech y se encuentran constituidas en el país. La distribución de los servicios en las diferentes compañías se observa en la Tabla 4, así como sus características específicas de segmento de clientes, tiempo de operación y número de empleados en la Tabla 5.

Tabla 4: Distribución por servicio ofrecidos

Fintech	Producto o servicio ofrecido			
	Lending	**Neobanco**	**Manejo de finanzas personales (PFM)**	**Pasarela de pagos**
A	x			
B	x			
C		x		
D			x	
E				x

Tabla 5: Distribución por servicio ofrecidos

Fintech	Principales características			
	Cliente objetivo	**Clasificación**	**Años de operación**	**Empleados directos**
A	Persona natural	Pyme	2	13
B	Persona natural	Pyme	1	5
C	Persona natural y jurídica	Pyme	1	19
D	Persona natural	Pyme	2	24
E	Persona jurídica que ofrece productos a persona natural (B2B2C).	Empresa mediana	3	32

Según la segmentación propuesta por Finnovista (2021), cuatro de las cinco empresas entrevistadas pertenecen al segmento de pymes acorde con la legislación colombiana (Decreto 957 de 2019; Ley 905 de 2004), pues cuentan con menos de 100 empleados, su financiamiento es inferior a los 500 mil dólares y tienen ingresos anuales menores a los 500 mil dólares. La compañía restante excede el límite de financiación, pero cumple con los demás criterios. Dado el tiempo de operación en el mercado colombiano, aún se realizan ajustes en sus modelos de negocio y, por lo tanto, la forma en la que se lleva a cabo su abordaje frente a las herramientas tecnológicas utilizadas y los riesgos asociados.

Las entrevistas se llevaron a cabo entre los meses de marzo y mayo del 2022, estas fueron realizadas de manera presencial y/o virtual, según la disposición del entrevistado. Creswell et. Al 2007 recomienda utilizar técnicas para controlar el sesgo en la entrega de información, para el desarrollo de esta investigación se utilizaron: la elaboración del formulario en función de lo identificado dentro de la revisión de literatura, la revisión del mismo con expertos, la realización de las entrevistas con el personal responsable de la toma de decisiones estratégicas frente a la ciberseguridad en las organizaciones, la aplicación del protocolo de entrevista siguiendo los mismos pasos en todas las sesiones, así como la participación de los integrantes del equipo de investigación en pleno, uno de ellos como entrevistador y los otros dos investigadores como observadores. El protocolo de entrevista fue construcción propia con base en el concepto de ciberesiliencia propuesto por (Bejarano et al., 2021; Carías et al., 2020). Las personas encuestadas hacen parte de la alta dirección de la compañía, para cada una de las empresas el entrevistado se relaciona en la Tabla 6.

Tabla 6: Segmentación Entrevistados

Fintech	Cargo Entrevistado
A	Director y CEO
B	Fundador y CEO
C	Líder de TI
D	Gerente financiero y de riesgos
E	Responsable de ciberseguridad

RESULTADOS

De acuerdo con (Finnovista, 2021; Rincón, 2021), Colombia es el tercer ecosistema Fintech en la región y se encuentra en el top diez de adhesión al modelo Fintech a nivel mundial, igualmente menciona que, a nivel de regulación, aun se presentan barreras importantes que permiten el desarrollo en algunos segmentos y la entrada de nuevos participantes al mercado. Los resultados de la investigación se observan tanto en la revisión de la literatura, como en la ejecución de las entrevistas. En ambos casos, la información de gestión y desempeño de las compañías del sector Fintech no es generalmente de carácter público, a diferencia de otros sectores, como lo es el sector financiero, dentro del cual los bancos, y demás compañías reguladas por la Superintendencia Financiera de Colombia deben reportar sus resultados financieros de manera trimestral y anual al mercado.

El protocolo de investigación definido para la realización de las entrevistas consideraba tanto la confidencialidad de la información, como de las partes que participaron en las entrevistas a solicitud de estas. Los resultados obtenidos serán presentados en función de: 1. Personas entrevistadas, 2. Definición del concepto de riesgo estratégico, 3. Riesgos asociados al uso de tecnología y medidas de gestión, 4. Definición del concepto de ciberseguridad, 5. Nivel

de madurez de la adopción de la ciberesiliencia. A continuación, se detalla el resultado de las entrevistas:

CARACTERÍSTICAS DE LOS ENTREVISTADOS

Durante la ejecución de la entrevista se realizó la siguiente pregunta a cada uno de los entrevistados:

"¿Puede contarnos por favor sobre sus funciones en la compañía y la relación que estas tienen con la gestión de riesgos?".

Tabla 7: Conocimientos entrevistados

Fintech	Conocimientos en Gestión de Riesgos	Conocimientos de los riesgos a los que se encuentra expuesta la compañía
A	No	Sí
B	No	Sí
C	No	No
D	Sí	Sí
E	Sí	Sí, limitándose a los riesgos cibernéticos.

DEFINICIÓN DEL CONCEPTO DE RIESGO ESTRATÉGICO

Durante la ejecución de la entrevista se realizaron las siguientes preguntas a cada uno de los entrevistados:

- "¿De qué forma se integra la tecnología dentro de la gestión de los riesgos estratégicos?"
- "¿Cómo se utilizan los recursos tecnológicos por parte de la alta dirección frente a la gestión de riesgos estratégicos?"

Tabla 8: Definición de riesgo estratégico y aplicación en la gestión de tecnología

Fintech	Tecnología en la Gestión de Riesgos Estratégico	Uso de los Recursos Tecnológicos por la Alta Dirección
A	No conoce los términos de gestión de riesgos.	Los recursos tecnológicos se utilizan cuando se materializa un evento de riesgo.
B	La compañía no aborda los diferentes tipos de riesgo, por lo que no se tiene conocimiento sobre los riesgos estratégicos empresariales.	No se tienen recursos tecnológicos destinados para la gestión de riesgos estratégicos.

C	Considera que los riesgos estratégicos son los eventos no deseados que generen impactos en la compañía.	Los recursos tecnológicos siempre están a disposición para el beneficio de la compañía, aunque no se cuenta con un plan que vincule la tecnología con los riesgos.
D	Los eventos que puedan poner en riesgo la propuesta de valor.	Al ser la tecnología la base de la operación, la gestión de riesgos se mitiga por medio de este tipo de herramientas.
E	Aquellos elementos que afectan la sostenibilidad de la compañía.	Se cuenta con un plan estratégico de ciberseguridad para mitigar los riesgos tecnológicos, aprobado por la alta dirección.

Vale aclarar que aún sin profundizar en el concepto de riesgos estratégicos, los cinco entrevistados mencionaron que la tecnología hace parte de su estrategia, pues es parte de su diferenciación frente al sector financiero tradicional, y la competencia. Fueron claros en hacer una relación directa entre la tecnología y sus modelos de negocio para una mejor optimización de los costos operativos, en línea con las anteriores definiciones de este tipo de compañías.

ENTENDIMIENTO DEL CONCEPTO DE CIBERESILIENCIA

Durante la ejecución de la entrevista se realizaron las siguientes preguntas a cada uno de los entrevistados:

- "¿Cómo se comprende el anticiparse a los ciberataques en su organización?"
- "¿Cómo se comprende el absorber los impactos de los ciberataques en su organización?"
- "¿Cómo se comprende el adaptarse como resultado de los ciberataques en su organización?"
- "¿Ha tenido materialización de eventos de riesgo cibernético?"

Tabla 9: Entendimiento del concepto de ciberesiliencia

Fintech	Anticipación a los ciberataques	Absorción de los Ciberataques	Adaptación como resultado Ciberataque	Materialización de Eventos cibernéticos
A	Implementación de soluciones de Ciberseguridad	Solución al evento en específico	Recuperación plataforma tecnológica	Si
B	Implementación de soluciones de Ciberseguridad	Solución al evento en específico	Restablecimiento backup de información	Si
C	Adopción Políticas de seguridad de la información	Prevención y contención. Atención del	Adaptación y fortalecimiento plataforma	Si

	Implementación de soluciones de Ciberseguridad	incidente presentado	tecnológica y de ciberseguridad	
D	Implementación de soluciones de Ciberseguridad	Aumento en la inversión y fortalecimiento de las plataformas de ciberseguridad	Fortalecimiento de las plataformas de ciberseguridad	Si
E	Adopción de Políticas y estrategias de seguridad de la información Implementación de soluciones de Ciberseguridad	Prevención y contención. Atención del incidente presentado	Adaptación y fortalecimiento plataforma tecnológica y de ciberseguridad	Si

La totalidad de las compañías analizadas afirmó haber tenido al menos un incidente sobre su plataforma tecnológica, sea de índole de ciberataque o de fallas técnicas en sus plataformas tecnológicas, por lo que se puede afirmar que el 100% ha sufrido la materialización de estos riesgos, una de ellas destaca que el incidente materializado tuvo como origen el factor humano.

Con respecto a las entrevistas, los resultados contrastan con lo planteado por (WEF, 2022) en su informe “The Global Risks Report 2022”, donde se indica que el 95% de los eventos de ciberseguridad están relacionados con errores humanos, representando aproximadamente el 43%, una de las compañías reportó un incidente con este origen.

Se resalta que uno de estos casos obedece al aprovechamiento por parte de delincuentes para el secuestro de la información de la compañía, en el que se buscó el rescate por la información. Los demás casos fueron asociados a fallas en los sistemas o relacionados con los proveedores de servicios. Todas han implementado soluciones de ciberseguridad y en dos de ellas el establecimiento de políticas relacionadas con la seguridad de la información, y frente a la absorción y adaptación se identifican acciones para la atención de evento presentado y el fortalecimiento de sus plataformas informáticas y de ciberseguridad.

Adicionalmente, tal y como fue planteado por Finnovista (2021), las personas entrevistadas consideran que existen ciberamenazas para su negocio y de éstas, solo dos, afirman tener una solución robusta para hacerles frente. Sin embargo, las tres restantes afirmaron que están en proceso de robustecer su sistema de seguridad, dado el poco tiempo que llevan en operación. Las cinco compañías ven necesario actualizar y optimizar sus sistemas de seguridad periódicamente, dado el acelerado crecimiento de los ciberataques y el creciente número de organizaciones que han sido víctimas de estos, pues consideran que es un eje central de su modelo de negocio.

DEFINICIÓN DEL CONCEPTO DE CIBERESILIENCIA

Durante la ejecución de la entrevista se realizaron las siguientes preguntas a cada uno de los entrevistados:

- "¿Conoce el concepto de ciberesiliencia?
- "¿Cómo se interpreta la ciberesiliencia organizacional en la empresa?"

Tabla 10: Adopción Ciberesiliencia para la gestión de ciberiesgos

Fintech	Concepto de Ciberesiliencia	Tipo de gestión en la compañía Ciberiesgos
A	No	Ciberseguridad como riesgo operativo
B	No	Ciberseguridad como riesgo operativo
C	No	Ciberseguridad como riesgo operativo
D	No	Ciberseguridad como riesgo operativo
E	No	Ciberseguridad como riesgo estratégico

Finalmente, sobre el concepto de la ciberesiliencia, aunque era un término conocido para las personas entrevistadas, por su mismo nombre asumieron que hace referencia a la capacidad de adaptación en el ámbito digital. Dado que estas compañías cuentan con pocos empleados vinculados, al profundizar en su alcance, y lo que busca el concepto en términos de cultura organizacional, en general, afirmaron que no se tiene una cultura instaurada en la compañía, asociada a riesgos cibernéticos, excepto cuando se refiere a su personal con funciones relacionadas con la ciberseguridad. Una de las compañías consideró que han adoptado en gran medida el concepto de ciberesiliencia, pues afirmó que la totalidad de sus empleados tiene conocimientos en términos de herramientas tecnológicas, por lo que considera que cuentan con las competencias y las habilidades para que estos puedan adaptarse tras un evento cibernético.

Al cierre de las entrevistas se explicó la diferencia entre abordar los riesgos cibernéticos desde la visión operativa y táctica de la ciberseguridad, así como el concepto de ciberesiliencia, el cual incorpora la visión estratégica, y la necesidad de contar con la capacidad de anticipar, detectar, entender, recuperar y evolucionar, a través de un enfoque holístico con la integración de varías áreas del conocimiento, incluyendo, pero no limitándose a la ciberseguridad (Carías et al., 2020), frente a esto, solo una de ellas (la compañía con un mayor monto de financiamiento) respondió que considera que su compañía está en proceso de implementar esta visión. Las demás afirmaron que aún su visión se queda en la de ciberseguridad tradicional y consideran que están lejos de llegar a incorporar este concepto como parte de la estrategia de la compañía.

En línea con lo planteado por (Lee & Shin, 2018) acerca de la rápida adopción de las tecnologías de información, las cuales buscan eficiencias en el core de negocio financiero tradicional, y permitieron la creación de la nueva industria de las compañías Fintech, a través de la incorporación de nuevos modelos de negocio, sistemas financieros en línea y la automatización de procesos, para ofrecer nuevos productos y servicios financieros. La rápida transformación digital a la que se ven expuestas las organizaciones del sector financiero, trae como consecuencia una gran exposición a una nueva dimensión de riesgos relacionados con la seguridad de la información, la ciberseguridad y los riesgos de continuidad de negocio, los cuales se presentan, tanto en el ámbito operativo como estratégico, debido a las amenazas de ciberseguridad y las fallas inesperadas de los sistemas (Boot et al., 2021b; Uddin et al., 2020).

Dos de las compañías entrevistadas manifiestan que actualmente desarrollan proyectos encaminados a garantizar la continuidad de su operación, a través de la implementación de infraestructuras alternas y sistemas de backup adaptados a sus necesidades.

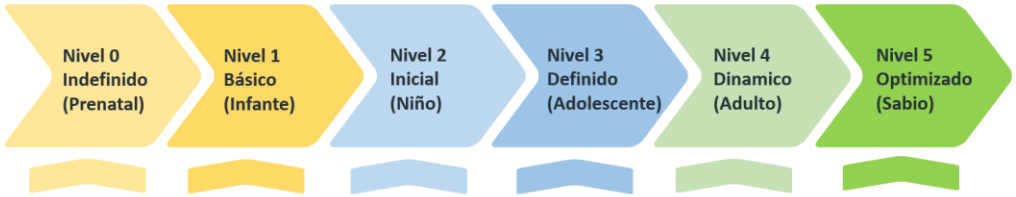
NIVEL DE MADUREZ DE LA ADOPCIÓN DE LA CIBERESILIENCIA

Durante la ejecución de la entrevista se realizaron las siguientes preguntas a cada uno de los entrevistados:

“De acuerdo con la tabla de la imagen adjunta, por favor indique:

- “¿cuál es el nivel de adopción de la ciberesiliencia en su empresa?”
- “¿Por qué considera que se encuentra en este nivel?”

Figura 1: Nivel de adopción ciberesiliencia



INDICADORES						
Actitud ante amenazas y Vulnerabilidades	En gran parte ignorante	Conciencia básica	Reactivo	Reactivo	Proactivo	Altamente proactivo
Desarrollo tecnológico	Conocimiento y uso limitado	Uso básico	Uso efectivo	Uso y aplicación efectivos	Innovación	Nivel generalizado de innovación
Respuesta social	Niveles limitados de conciencia, eficiencia y altamente inflexibles	Bajo nivel de conciencia, baja eficiencia e inflexibles	Nivel medio de conciencia, eficiencia y flexibilidad	Nivel medio alto de conciencia, eficiencia y flexibilidad	Alto nivel de conciencia, eficiencia y flexibilidad	Nivel generalizado de conciencia, eficiencia y flexibilidad
Medidas: **- Técnico** **- Negocio** **- Legales y regulatorio** **- Operacionales** **- Desarrollo de habilidades**	Indefinida / Limitada	Medidas ad-hoc no estructuradas	Medidas no estructuradas basadas en amenazas	Medidas estructuradas basadas en amenazas	Medidas basadas en Capacidades estructuradas	Medidas basadas en Capacidades altamente estructuradas

Fuente: Adaptado de (Barclay, 2014)

Tabla 11. Nivel de adopción ciberesiliencia modelo propuesto por Barclay (The Cybersecurity Capability Maturity Model)

Fintech	Nivel de madurez
A	Nivel 1 Básico
B	Nivel 1 Básico
C	Nivel 2 Inicial
D	Nivel 1 Básico
E	Nivel 3 Definido

Fuente: (Barclay, 2014)

Al ser presentada la información a cada una de las compañías, estás manifiestan que no conocen de manera previa, modelos de madurez para la ciberesiliencia, y afirman que su nivel de adopción es incipiente (Nivel 1 Básico y Nivel 2 Inicial), frente a lo planteado por el modelo. Solo una de las empresas establece que ha avanzado en su aproximación a los conceptos de ciberesiliencia (Nivel 3 Definido), al considerar que, a nivel humano (personal dedicado a la ciberseguridad), técnico, operacional y de negocio, cuentan con una capacidad de respuesta adecuada.

CONCLUSIONES Y FUTUROS TRABAJOS

Como se mencionó anteriormente, este trabajo tenía como objetivo entender el estado del sector Fintech frente a la implementación del concepto de ciberesiliencia en Colombia y aportar a la investigación del tema en términos de riesgo estratégico. Se considera que, tras entrevistar a diferentes compañías, el objetivo se cumplió y se logró analizar de manera cualitativa el nivel de madurez del concepto de ciberesiliencia en este tipo de compañías. En el marco teórico no se identificaron trabajos previos con este enfoque, por lo que se considera una contribución a este cuerpo del conocimiento.

A nivel global y en la región de la Alianza Pacífico, se presenta un crecimiento incremental de las compañías del sector Fintech, en el caso de Colombia esta se encuentra en el top diez de los países en la adopción de esta industria (Rincón, 2021), principalmente a través de los modelos innovadores de negocios, como el de lending y pagos digitales, enfocados en los segmentos de la población y de las compañías pymes que no se encuentran bancarizadas, a través del sector financiero tradicional (Finnovista, 2021).

En el último reporte de Finnovista (2021), se identificó que en Colombia operan 279 empresas en el sector, de las cuales 118 han iniciado operación en el año 2021, lo que posiciona al país como el segundo ecosistema Fintech más grande de la Alianza del Pacífico (precedido por México) y el tercero a nivel de la región (después de Brasil y México), impulsado a su vez por la emergencia sanitaria de la COVID-19, reflejado en un mayor porcentaje de la población colombiana bancarizada.

Al consultar información sobre la gestión de los riesgos estratégicos relacionados con ciberseguridad y la adopción de la Ciberesiliencia, como una buena práctica a implementar en el sector Fintech en el Colombia, se observa que esta es incipiente, lo cual se evidencia desde la revisión de literatura, y se confirma a través de la información obtenida en las entrevistas.

En Colombia, al no contar con una regulación Fintech específica, las empresas del sector cumplen con normatividad diversa, y se interactúa con múltiples entes de supervisión y control de su actividad (Colombia Fintech, 2022b). De acuerdo con esta situación, la Superintendencia Financiera ha impulsado el Sandbox Regulatorio como instrumento para definir una regulación uniforme, acorde a las necesidades de los diferentes segmentos y servicios atendidos por el sector Fintech, al igual que regulación del modelo de open banking. De igual forma, en el año 2022, el gobierno nacional avanza en la definición y adopción del Decreto 338 de 2022, el cual establece los lineamientos para fortalecer la gobernanza de la seguridad digital, y la protección de las infraestructuras críticas cibernéticas en Colombia, entre las que se encuentran el sector financiero y el sector TIC, sin desconocer que las nuevas exigencias para estas industrias impactarán el desarrollo del negocio Fintech (CISA, 2021; Hernández, 2016).

Para el desarrollo de este trabajo se entrevistaron cinco compañías del sector Fintech en Colombia en referencia al entendimiento y la adopción de los conceptos mencionados anteriormente. Las empresas entrevistadas cuentan con entre uno y tres años de operación en

el mercado. En las entrevistas desarrolladas manifestaron que cuentan con una gestión de los ciberiesgos a través de un enfoque tradicional en ciberseguridad, y que la adopción de la gestión estratégica de estos, a través de un marco de referencia integral como el propuesto por la ciberesiliencia, no ha sido adoptado, pero esperan incorporarlo en los próximos años como una buena práctica que permita preparar a la organización para hacer frente a la materialización de un evento cibernético, y continuar su negocio, respondiendo incluso a cambios de marcos regulatorios que impacten al sector.

Por esta razón se concluye que, en línea con la literatura disponible, las compañías Fintech en Colombia aún tienen un camino por recorrer para implementar el concepto de ciberesiliencia en su operación. El nivel de madurez en el que están se logra acercar a un enfoque de ciberseguridad, aunque aún quedan algunos elementos pendientes por cubrir. Teniendo en cuenta que la ciberesiliencia es un concepto más amplio y exigente, se entiende que no se ha implementado aún. Se esperaría que, a raíz de las tendencias regulatorias, y el rápido desarrollo de la tecnología, esta industria deba incorporar herramientas de gestión para mitigar los impactos de estos riesgos.

Frente a la relación entre la ciberesiliencia y la gestión de riesgos estratégicos, se puede concluir que, a partir de las entrevistas realizadas y en línea con la revisión de literatura, las compañías Fintech en el país abordan los riesgos derivados del uso de las herramientas tecnológicas con la visión de riesgo operativo, sin una incorporación dentro de la gestión de riesgos estratégicos. A pesar de que estas compañías cuentan con un core de negocio basado en tecnología, aún no se relacionan los ciberiesgos con la gestión de riesgos estratégicos. Se puede esperar que, al definir los ciberiesgos y su relación con la estrategia, así como con la promesa de valor de la compañía, las compañías Fintech se acerquen a gestionarlos con un mayor alcance, a través de un enfoque holístico con la integración de varías áreas del conocimiento, dentro de las cuales se incluyen tanto la ciberseguridad, como lo proponen los marcos y estándares en ciberesiliencia (Bejarano et al., 2021; Carías et al., 2020), así como los modelos de madurez para comprobar periódicamente su nivel de adopción (Carías et al., 2020; Barclay, 2014).

A partir de los resultados del presente trabajo, y los elementos desarrollados, se identifican como nuevas líneas de investigación, la relación entre la ciberesiliencia y la gestión de riesgos estratégicos tras la implementación de la nueva regulación que se encuentra actualmente en estudio por parte de la Superintendencia Financiera, adicional a las iniciativas del gobierno nacional a través del Decreto 338 de 2022, y las nuevas regulaciones que se desprendan de este, que obliguen a las empresas del Sector Fintech a reforzar la gestión estratégica de sus riesgos relacionados con los riesgos cibernéticos inherentes a sus plataformas tecnológicas y a sus modelos de negocio. Adicionalmente, se identifica una línea de investigación relacionada con la adopción de herramientas de gestión que permitan determinar niveles de madurez organizacionales dentro de las Fintech frente a la gestión de la ciberesiliencia, y la forma en la que estos niveles de madurez pueden relacionarse con la mitigación de los impactos generados por la materialización de riesgos estratégicos. Finalmente, se identifica una línea de investigación relacionada con los factores de éxito para la incorporación de los riesgos relacionados con la ciberesiliencia dentro de la gestión del riesgo estratégico en las empresas Fintech en Colombia.

REFERENCIAS

Abbasi, K., Alam, A., Du, M. (Anna) & Huynh, T. L. D. (2021). FinTech, SME efficiency and national culture: Evidence from OECD countries. *Technological Forecasting and Social Change*, *163*. https://doi.org/10.1016/j.techfore.2020.120454

Al Nawayseh, M. K. (2020). FinTech in COVID-19 and Beyond: What Factors Are Affecting Customers' Choice of FinTech Applications? *Journal of Open Innovation: Technology, Market, and Complexity*, *6*(4), 153. https://doi.org/10.3390/joitmc6040153

Barclay, C. (2014). Sustainable security advantage in a changing environment: The cybersecurity capability maturity model (CM2). *Proceedings of the 2014 ITU Kaleidoscope Academic Conference: Living in a Converged World - Impossible Without Standards?,* 275–282. https://doi.org/10.1109/Kaleidoscope.2014.6858466

Barretti Mascarenhas, A., Ugliano Garbelini, M., Claudia Duarte, A., Roberta Nesso Kokiso, C. & Abrahão Costa e Silva, M. (2021). *Associação entre Superconsumo e Efeito Priming no Comportamento de Compra Durante a Pandemia de COVID-19: Uma Reprodução Do Dilema Do Prisioneiro*. https://doi.org/10.29327/bels2021.354803

Bejarano, M. H., Rodríguez, R. J. & Merseguer, J. (2021). A Vision for Improving Business Continuity through Cyber-resilience Mechanisms and Frameworks. *2021 16th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–5. https://doi.org/10.23919/CISTI52073.2021.9476324

Belozyorov, S., Sokolovska, O. & Kim, Y. S. (2020). Fintech as a precondition for transformations on global financial markets. *Foresight and STI Governance*, *14*(2). https://doi.org/10.17323/2500-2597.2020.2.23.35

Boot, A., Hoffmann, P., Laeven, L. & Ratnovski, L. (2021). Fintech: what's old, what's new? *Journal of Financial Stability*, *53*. https://doi.org/10.1016/j.jfs.2020.100836

Bromiley, P., Rau, D. & McShane, M. K. (2014). Can Strategic Risk Management Contribute to Enterprise Risk Management? A Strategic Management Perspective. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2512477

Carías, J. F., Borges, M. R. S., Labaka, L., Arrizabalaga, S. & Hernantes, J. (2020). Systematic approach to cyber resilience operationalization in SMEs. *IEEE Access*, *8*, 174200–174221. https://doi.org/10.1109/ACCESS.2020.3026063

Carias, J. F., Borges, M. R. S., Labaka, L., Arrizabalaga, S. & Hernantes, J. (2021). The order of the factors does alter the product: Cyber resilience policies' implementation order. En *Advances in Intelligent Systems and Computing, vol. 1267 AISC*. https://doi.org/10.1007/978-3-030-57805-3_29

Cheng, M. & Qu, Y. (2020). Does bank FinTech reduce credit risk? Evidence from China. *Pacific Basin Finance Journal*, *63*. https://doi.org/10.1016/j.pacfin.2020.101398

Chicaíza, L., Riaño, M., Rojas, S. & Garzón, C. (2019). Revisión sistemática de la literatura en administración. *Documentos FCE-CID Escuela de Administración y Contaduría Pública*.

Circular 008 de 2018. [Superintendencia Financiera de Colombia]. *Imparte instrucciones en materia de requerimientos mínimos de seguridad y calidad para la realización de operaciones.*05 de junio de 2018.

Colombia Fintech. (2022a). *Directorio de Miembros*. https://www.colombiafintech.co/personas

Colombia Fintech. (2022b, mayo 2). *Regulación Fintech Colombia*. https://www.colombiafintech.co/lineaDeTiempo/articulo/regulacion-fintech-colombia

Comisión Europea (2020). *Reglamento del Parlamento Europeo y del Consejo sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014 y (UE) n.º 909/2014*. https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020PC0595&from=EN

Comité de Supervisión Bancaria de Basilea. (2018). *Buenas prácticas Implicaciones de los avances en tecnofinanzas (fintech) para los bancos y los supervisores bancarios*. https://www.bis.org/bcbs/publ/d431_es.pdf

Comité Económico y Social Europeo. *Dictamen del Comité Económico y Social Europeo sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148 y sobre la propuesta de Directiva del Parlamento Europeo y del Consejo sobre la resiliencia de las entidades críticas***.** Diario Oficial de la Unión Europea C 286/170 de 16 de julio de 2021.

Creswell, B. J. W. (1994). Design a qualitative research. *Qualitative Research*.

Cybersecurity & Infraestrcuture Security Agency. (2021). *Critical Infrastructure Sectors*. https://www.cisa.gov/critical-infrastructure-sectors

De Haan, J., Schoenmaker, D. & Wierts, P. (2020). Financial Markets and Institutions: A European Perspective (Chapter 1). *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3593322

Decreto 222 de 2020. [Ministerio de Hacienda y Crédito Público]. *Por el cual se modifica el Decreto 2555 de 2010 en lo relacionado con los corresponsales, las cuentas de ahorro electrónicas, los depósitos electrónicos, el crédito de bajo monto y se dictan otras disposiciones.* 14 de febrero de 2020.

Decreto 338 de 2022. [Ministerio de Tecnología de la Información y Comunicaciones]. *Por el cual se adiciona el Titulo 21 a la parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.*8 de marzo de 2022

Decreto 957 de 2019 [Ministerio de Hacienda y Crédito Público, Ministerio de Comercio, Industria y Turismo]. *Por el cual se adiciona el capítulo 13 al Título 1 de la Parte 2 del Libro 2 del Decreto 1074 de 2015, Decreto Único del Sector Comercio, Industria y Turismo y se reglamenta el artículo 2º de la Ley 590 de 2000, modificado por el artículo 43 de la Ley 1450 de 2011.* 05 de junio de 2019.

Decreto 1235 de 2020 [Ministerio de Hacienda y Crédito Público]. *Por el cual se modifica el Decreto 2555 de 2010 en lo relacionado con las reglas para la emisión en el mercado de valores, se reglamenta el artículo 2 del Decreto Legislativo 817 de 2020 y se dictan otras disposiciones*. 14 de septiembre de 2020.

Decreto 1357 de 2018 [Ministerio de Hacienda y Crédito Público]. *Por el cual se modifica el Decreto 2555 de 2010 en lo relacionado con la actividad de financiación colaborativa.* Diario Oficial No.50.671, de 31 de julio de 2018.

Decreto 1692 de 2020. [Ministerio de Hacienda y Crédito Público]. *Por medio del cual se modifica el Decreto 2555 de 2010 en lo relacionado con los sistemas de pago de bajo valor.* 18 de diciembre de 2020

Deloite. (2013). *Exploring Strategic Risk 300 executives around the world say their view of strategic risk is changing*. https://deloitte.wsj.com/riskandcompliance/files/2013/10/strategic_risk_survey.pdf

Deloitte. (2017). *The future of risk in Financial Services*. https://deloitte.wsj.com/riskandcompliance/files/2013/10/strategic_risk_survey.pdf

Deloitte. (2018). *Information technology risks in financial services*. https://www2.deloitte.com/global/en/pages/risk/articles/information-technology-risks-financial-services.html

Directiva Presidencial 02 de 2022 (2022). *Reiteración de la política pública en materia de seguridad digital*.

Dupont, B. (2019). The cyber-resilience of financial institutions: Significance and applicability. *Journal of Cybersecurity*, *5*(1). https://doi.org/10.1093/cybsec/tyz013

Finnovista. (2021). Radar Fintech e Incumbentes 2021. https://www.finnovista.com/wp-content/uploads/2021/12/Radar-Finovista-General-2021-4.pdf

Fortinet. (2022, February 8). *América Latina sufrió más de 289 mil millones de intentos de ciberataques en 2021*. https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-reporte-ciberataques-america-latina-2021

Fu, J. & Mishra, M. (2022). Fintech in the time of COVID-19: Technological adoption during crises. *Journal of Financial Intermediation*, *50*. https://doi.org/10.1016/j.jfi.2021.100945

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

Hernández, J. (2016). *Infraestructura Crítica Cibernética* (Asociación Colombiana de Ingenieros de Sistemas, Ed.). https://acis.org.co/archivos/Conferencias/2016/GuiaICC.pdf

Hernández, R., Fernández, C. & Baptista, P. (2010). Metodología de la investigación. 5ta Edición. En *Metodología de la investigación*.

IBM. (2022). *X-Force Threat Intelligence Index 2022 Full Report*. https://www.ibm.com/downloads/cas/ADLMYLAZ

Instituto Nacional de Ciberseguridad. (2020). *Metodología de evaluación de Indicadores para Mejora de la Ciberresiliencia (IMC).* https://www.incibe-cert.es/sites/default/files/contenidos/guias/IMC/imc_01_metodologia-evaluacion.pdf

Jiao, Z., Shahid, M. S., Mirza, N. & Tan, Z. (2021). Should the fourth industrial revolution be widespread or confined geographically? A country-level analysis of fintech economies. *Technological Forecasting and Social Change*, *163*. https://doi.org/10.1016/j.techfore.2020.120442

Kou, G., Olgu Akdeniz, Ö., Dinçer, H. & Yüksel, S. (2021). Fintech investments in European banks: a hybrid IT2 fuzzy multidimensional decision-making approach. *Financial Innovation*, *7*(1). https://doi.org/10.1186/s40854-021-00256-y

Lee, I. & Shin, Y. J. (2018). Fintech: Ecosystem, business models, investment decisions, and challenges. *Business Horizons*, *61*(1). https://doi.org/10.1016/j.bushor.2017.09.003

Ley 905 de 2004. *Por medio de la cual se modifica la Ley 590 de 2000 sobre promoción del desarrollo de la micro, pequeña y mediana empresa colombiana y se dictan otras disposiciones. Diario Oficial,* No. 45.628 de 2 de agosto de 2004.

Mejia R.C. (2013). *Identificación de riesgos*. Medellín: Fondo Editorial Universidad Eafit

Menéndez Blanco, J. M. & Montes Botella, J. L. (2016). What contributes to adaptive company resilience? A conceptual and practical approach. *Development and Learning in Organizations*, *30*(4). https://doi.org/10.1108/DLO-10-2015-0080

Montoya, C. & Rivas, L. (2018). Riesgo Estratégico: Contraste de perspectivas. *Red Pilares*.

Nuñez, M. A., Rivas-Montoya, L. M., Villanueva, E., Mejía, P., Montoya-Londoño, C. A. & Jaraba, I. (2020). *Riesgo Estratégico.* Medellín: Fondo Editorial Universidad Eafit.

Panetta, F. (2018). *Fintech and banking: today and tomorrow Speech by the Deputy Governor of the Bank of Italy*. https://www.bancaditalia.it/pubblicazioni/interventi-direttorio/int-dir-2018/panetta-120518.pdf

Paulet, E. & Mavoori, H. (2020). Conventional banks and Fintechs: how digitization has transformed both models. *Journal of Business Strategy*, *41*(6). https://doi.org/10.1108/JBS-06-2019-0131

Rincón E. (2021, October 9). Estudios demuestran que Colombia es el octavo del mundo en adherencia Fintech. *La República.* https://www.larepublica.co/finanzas/estudios-demuestran-que-colombia-es-el-octavo-pais-del-mundo-en-adherencia-fintech-3244664

Senyo, P. K. & Osabutey, E. L. C. (2020). Unearthing antecedents to financial inclusion through FinTech innovations. *Technovation*, *98*. https://doi.org/10.1016/j.technovation.2020.102155

Smith, J., Ben-Aron, D., Gonzalez A., Huang, M. & Richetta, M. (2020). *KoreFusion 2020 LATAM Fintech Report.* https://korefusion.com

Sybirianska, Y., Dyba, M., Britchenko, I., Ivashchenko, A., Vasylyshen, Y. & Polishchuk, Y. (2018). Fintech platforms in sme's financing: eu experience and ways of their application in Ukraine. *Investment Management and Financial Innovations*, *15*(3). https://doi.org/10.21511/imfi.15(3).2018.07

The Business Continuity Institute & British Standards Institution. (2022). *BCI Horizon Scan Report 2022*. https://www.bsigroup.com/globalassets/localfiles/en-gb/iso-22301/bci-horizan-scan-report/bci-horizon-scan-report-2022.pdf

Uddin, M. H., Mollah, S. & Ali, M. H. (2020). Does cyber tech spending matter for bank stability? *International Review of Financial Analysis*, *72*. https://doi.org/10.1016/j.irfa.2020.101587

Weill, L. (2020). L'impact des Fintech sur la structure des marchés bancaires. *Revue d'économie Financière*, *N° 135*(3). https://doi.org/10.3917/ecofi.135.0181

World Economic Forum. (2022). *The Global Risks Report 2022*. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf?_gl=1*105b5v1*_up*MQ..&gclid=CjwKCAjwnZaVBhA6EiwAVVyv9Couj0KIF9ZDFY8yQmOYZuI6NCrKsbzjsUKvY1S-4BbbwVUd4Yf83hoCa2AQAvD_BwE