Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

Zuly Julieth Manrique Alarcón

Corporación Universitaria Minuto De Dios - UNIMINUTO

Rectoría Bogotá

Facultad de Ciencias Empresariales

Programa de Especialización en Gerencia Financiera

febrero de 2025

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

Zuly Julieth Manrique Alarcón

Trabajo de Grado Presentado como requisito para optar al título Especialista en Gerencia Financiera

Asesor

Ph.D. Campo Elías López-Rodríguez

Docente Investigador de la Facultad de Ciencias Empresariales

Corporación Universitaria Minuto De Dios - UNIMINUTO

Rectoría Bogotá

Facultad de Ciencias Empresariales

Programa de Especialización en Gerencia Financiera

febrero de 2025

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

Dedicatoria

A mi familia, especialmente a mi esposo e hijos, por su apoyo, amor y paciencia incondicional

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

Agradecimientos

Agradezco a Dios por darme la sabiduría durante este proceso, a mi familia por su apoyo constante, a mis profesores por sus enseñanzas a lo largo de esta especialización y a todas las personas que, de alguna manera, contribuyeron al desarrollo de este trabajo.

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

Contenido

Resumen 9

Introducción 11

1. Problema 13

1.1. Descripción del problema 13

1.2. Pregunta de investigación 16

2. Justificación 17

3. Objetivos 20

3.1. Objetivo general 20

3.2. Objetivos específicos 20

4. Marco de referencia 21

4.1. Marco teórico 21

4.2. Marco legal 25

5. Metodología 27

5.1. Alcance de la investigación 27

5.2. Enfoque metodológico 28

5.3. Población y muestra 28

5.4. Instrumentos 29

5.5. Procedimientos 30

5.6. Consideraciones éticas 36

6. Resultados 38

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

6.1. Identificación conceptual de los tipos de amenazas cibernéticas más comunes que afectan las empresas 38

6.2. Magnitud e impacto económico de los riesgos en las finanzas corporativas de las empresas.....57

6.2.1.1. Introducción al Análisis Cuantitativo de Costos de Ciberataques..**¡Error! Marcador no definido.**

6.2.2. ¿Qué estrategias pueden implementar las instituciones financieras para recuperar la confianza de los clientes después de sufrir un ciberataque significativo?.**¡Error! Marcador no definido.**

6.3. Estrategias para minimizar y prevenir los riesgos cibernéticos en las finanzas corporativas.....66

6.3.1. ¿Qué tecnologías emergentes están mejorando la ciberseguridad en Fintech y cómo puede la inteligencia artificial ayudar a prevenir ataques cibernéticos?....**¡Error! Marcador no definido.**

6.3.2. ¿Cuál es el principal desafío en la implementación de protocolos de seguridad en el sector Fintech, cómo pueden estas empresas encontrar un equilibrio entre seguridad y experiencia del usuario?..... **¡Error! Marcador no definido.**

7. Conclusiones..... 72

8. Recomendaciones 76

Referencias bibliográficas 79

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

Lista de tablas

Tabla 1.Marco lógico para entrevista 32

Tabla 2. Estimación de costos de un ataque cibernético.....44

Tabla 3. Fuentes de estimación de costos en ciberataques 49

Tabla 4. Datos Generales de la Fintech del escenario hipotético.....58

Tabla 5.Desglose de Ingresos Mensuales 59

Tabla 6.Características del Ataque de Ransomware 61

Tabla 7. Impacto Financiero del Ataque.....61

Tabla 8. Desglose de Pérdidas Directas.....62

Tabla 9. Desglose de Pérdidas Indirectas.....62

Tabla 10. Desglose de Costos de Mitigación 63

Tabla 11. Distribución Recomendada de Inversión en Ciberseguridad (Nivel Intermedio) 64

Tabla 12.Análisis del Margen de Utilidad Neta (NPM) 64

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

Lista de figuras

Figura 1. Flujograma de entrevista 31

Figura 2.Flujograma de análisis documental.....36

Figura 3. Amenazas más comunes que enfrentan las empresas Fintech 39

Figura 4. Errores y estrategias de ciberseguridad para Fintech.....41

Figura 5.Caso de ataque cibernético en Fintech.....43

Figura 6.Estrategias de ciberseguridad y comunicación.....53

Figura 7.Tecnologías de Ciberseguridad 53

Figura 8.Cultura de ciberseguridad.....56

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

Resumen

La revolución digital ha transformado los servicios financieros mediante las Fintech de préstamos, pero ha aumentado su vulnerabilidad ante ciberataques sofisticados que amenazan su estabilidad financiera. Esta investigación analiza los principales riesgos cibernéticos que afectan las finanzas corporativas de estas empresas en Bogotá, identificando vulnerabilidades, evaluando impactos económicos y desarrollando estrategias de mitigación. El estudio es significativo porque estas amenazas generan implicaciones para todo el sistema financiero y la economía nacional. Metodológicamente, se emplea un enfoque mixto: cualitativo, mediante entrevista a experto en ciberseguridad; y cuantitativo, basado en documentación secundaria adaptada al contexto local. Esta investigación contribuye proporcionando información estratégica y recomendaciones para fortalecer la resiliencia financiera del sector Fintech de préstamos(lending) colombiano ante la creciente sofisticación de las amenazas digitales.

Palabras claves: Gerencia Financiera, riesgos financieros, finanzas corporativas, Fintech, ataques cibernéticos

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

Abstract

The digital revolution has transformed financial services through lending Fintech companies but has increased their vulnerability to sophisticated cyber-attacks that threaten their financial stability. This research analyzes the main cyber risks affecting the corporate finances of these companies in Bogotá, identifying vulnerabilities, evaluating economic impacts, and developing mitigation strategies. The study is significant because these threats have implications for the entire financial system and the national economy. Methodologically, a mixed approach is employed: qualitative, through an interview with a cybersecurity expert; and quantitative, based on secondary documentation adapted to the local context. This research contributes by providing strategic information and recommendations to strengthen the financial resilience of the Colombian lending Fintech sector in the face of increasingly sophisticated digital threats.

Keywords: Financial Management, financial risks, corporate finance, Fintech, cyber attacks

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

Introducción

La revolución digital ha impulsado la evolución del ecosistema Fintech, transformando los servicios financieros, ofreciendo soluciones innovadoras. Sin embargo, esta acelerada digitalización ha incrementado la exposición del sector a ciberataques cada vez más sofisticados, que amenazan la estabilidad financiera de estas organizaciones. Ante este desafío, resulta apremiante analizar a fondo los riesgos cibernéticos que enfrentan las empresas Fintech de préstamos y que comprometen su rentabilidad. Este análisis permitirá identificar vulnerabilidades específicas, evaluar los impactos potenciales en sus finanzas y desarrollar estrategias efectivas para mitigar las consecuencias económicas de estos, sentando así las bases para lograr un sector más seguro y preparado para los desafíos futuros.

En este contexto resulta significativo explicar la importancia de comprender y abordar las vulnerabilidades que actualmente presenta el sector Fintech de préstamos en Bogotá, debido a los crecientes ciberataques que enfrenta diariamente y los cuales pueden generar implicaciones sistémicas no solo a nivel empresarial, sino también para todo el sistema financiero llevando a impactar la economía del país. Por lo tanto, se busca fortalecer la infraestructura tecnológica, mejorar la toma de decisiones financieras preventivas en torno a fomentar una cultura de ciberseguridad y promover estrategias de protección financiera más robustas.

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

Esta investigación analiza la disrupción generada por las Fintech de préstamos en el sector financiero tradicional y la preocupante falta de conciencia sobre riesgos cibernéticos entre muchos empresarios. El estudio examina la creciente sofisticación de los ciberataques dirigidos específicamente a Fintech, identificando técnicas utilizadas por atacantes, Se aborda la importancia de la ciberseguridad como elemento clave para mantenerse vigente en el mercado cada vez más digital. Finalmente, se evalúan estrategias financieras preventivas que les permitan anticipar incidentes, cuantificar riesgos adecuadamente y desarrollar mecanismos de protección financieros adaptados a sus necesidades específicas.

En cuanto al diseño metodológico, se adoptó un enfoque mixto que combina herramientas cualitativas y cuantitativas para obtener una visión global del problema, para abarcar el aspecto cualitativo se realizó una entrevista a un experto en ciberseguridad donde se profundizó en los tipos de amenazas cibernéticas más comunes, estrategias de mitigación ante amenazas digitales, desafíos de investigación, regulación, capacitación, ciberesiliencia e inversión a consecuencia de ciberataques en empresas Fintech.

Con relación al análisis cuantitativo la propuesta inicialmente indicaba un análisis documental secundario relacionado con el impacto financiero de los ataques, pero la escasez de datos específicos del sector Fintech de préstamos (lending) de Bogotá, se optó por presentar un análisis numérico y modelos financieros detallados (tablas de costos, proyecciones de impacto financiero, escenarios hipotéticos con valores monetarios específicos), para cuantificar el fenómeno estudiado, sin embargo los resultados deben interpretarse más como estimaciones ilustrativas que como mediciones precisas de la realidad local.

En conclusión, esta investigación contribuye de manera significativa al análisis de las implicaciones financieras de los ciberataques en empresas Fintech de préstamos que operan en la

economía digital colombiana. Su principal aporte al sector productivo radica en proporcionar información estratégica y recomendaciones concretas para fortalecer la resiliencia financiera y garantizar la sostenibilidad operativa de estas empresas frente a la creciente amenaza de riesgos cibernéticos que pueden conducir a un riesgo económico sistémico.

1. Problema

1.1. Descripción del problema

La creciente adopción de tecnologías de la información por parte de las empresas y su necesidad de adaptarse a los cambios que se generan constantemente en un mercado globalizado ha llevado a que las organizaciones tomen la decisión de migrar algunos de sus servicios a entornos digitales, En búsqueda de optimizar sus operaciones, disminuir costos y ampliar su participación en el mercado, es por ello que han incorporado diversas soluciones tecnológicas; desde una página web corporativa, aplicaciones para dispositivos móviles, presencia en redes sociales, hasta software especializado para gestionar su contabilidad, entre otros.

La pandemia del coronavirus impulsó aún más este cambio, convirtiendo una tendencia gradual en una necesidad inmediata para las empresas, el sector financiero global no ha sido ajeno a esta evolución, puesto que ha experimentado una transformación significativa con el impulso de las empresas Fintech de préstamos, quienes usan tecnologías innovadoras permitiendo un acercamiento mayor a servicios financieros que en años anteriores se creía imposible su acceso para la mayoría de la población, esta digitalización acelerada ha expuesto las finanzas corporativas de estas instituciones, como se podrá evidenciar más adelante.

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

Según un informe de Colombia Fintech (2022) gran parte del crecimiento del ecosistema se debe a la pandemia ocasionada por el COVID-19. En particular, en los segmentos de pagos y billeteras digitales, los programas de estímulos económicos implementados por distintos gobiernos para apoyar a las personas más vulnerables impulsaron el crecimiento sustancial de estas plataformas. Además, Asobancaria. (2024) afirma que la dinámica expansiva de las Fintech ha implicado una inversión significativa por parte de los bancos en todo el mundo. Este crecimiento y la mayor interconexión entre el sector financiero y las Fintech han despertado importantes desafíos regulatorios y de seguridad.

En línea con lo anterior, según la organización para la Cooperación y el Desarrollo Económico, citando a González-Páramo (2017) menciona que dado el imparable proceso de digitalización del sector financiero inherente al fenómeno FinTech, pueden incrementarse los riesgos en términos de ciberseguridad, de modo que el sector financiero se haga más propenso a ciberataques y al cibercrimen. Esta preocupación da lugar a una nueva forma de regulación financiera dedicada a la salvaguarda de la estabilidad financiera en este ámbito.

Por otra parte, es importante tener presente que los ataques cibernéticos tienen un impacto significativo en las finanzas corporativas de las empresas, De acuerdo con el Fondo Monetario Internacional (FMI, 2017), existen dos tipos de costos asociados a los ataques cibernéticos. Por un lado, están los costos directos, que incluyen investigaciones forenses, asesoría legal, notificaciones al cliente, protección y seguridad al consumidor, y medidas posataque para mitigar sus efectos. Por otro lado, se encuentran los costos indirectos, los cuales son menos visibles, con efectos de más largo plazo y más difíciles de cuantificar exante (Ramírez et al., 2017).

Las causas de las vulnerabilidades incluyen el desconocimiento de gran parte de la población debido a la poca concientización sobre la importancia de la seguridad en el uso de las

tecnologías de la información y la comunicación, la baja capacitación para los empleados en cuestiones de seguridad cibernética, los crecientes puntos de entrada en los sistemas para los hackers. en resumen, la falta de inversión en infraestructura de seguridad cibernética para desplegar, proteger y actualizar estructuras y sistemas que protejan los activos digitales.

La evolución constante de las amenazas de este tipo y la creciente dependencia de los diferentes actores económicos de la sociedad en el uso de soluciones tecnológicas hacen que sea más difícil mantenerse protegido en un entorno cada vez más hiperconectado. Por esta razón, el objeto de estudio y la población de interés son las empresas Fintech de Bogotá las cuales día con día enfrentan ataques cibernéticos. Se determinarán qué tipos de riesgos son más comunes y cómo estos pueden impactar en las finanzas corporativas de las empresas.

Cabe resaltar que es el momento adecuado para impedir las derivaciones de esta problemática que incluyen la pérdida de información financiera y de datos de los clientes, la interrupción de los servicios, la reducción de la confianza de los clientes, de los accionistas en la empresa, gastos extraordinarios en cumplimiento legal y regulatorio. Esto puede resultar en una disminución de las ganancias y un aumento de los costos, lo que a su vez puede poner en peligro la continuidad de la compañía y dependiendo de la situación ocasionar un colapso financiero sistémico nacional.

La delimitación temporal establecida permite analizar la evolución e impacto de los riesgos financieros derivados de ciberataques durante un período crítico para el segmento de préstamos digitales (lending), que representa el 28.4% del ecosistema Fintech colombiano (Finnovista, 2024). Este subsector, el más relevante del mercado nacional, enfrenta vulnerabilidades particulares debido a los algoritmos de calificación crediticia y datos financieros sensibles que maneja. es por ello por lo que resulta imperativo que implementen

medidas de seguridad más robustas y proactivas para salvaguardar sus operaciones financieras, proteger la confianza depositada por sus usuarios y potenciar su capacidad de generación de empleo.

1.2. Pregunta de investigación

¿Cómo se caracterizan los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá?

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

2. Justificación

El sector Fintech, particularmente en el segmento de préstamos (lending) ha revolucionado los servicios financieros globales mediante soluciones tecnológicas más eficientes y accesibles. Sin embargo, esta acelerada digitalización ha incrementado la vulnerabilidad de estas empresas ante ataques cibernéticos que comprometen su estabilidad financiera y operativa. En Bogotá, epicentro financiero y tecnológico de Colombia los riesgos trascienden el ámbito empresarial individual, generando implicaciones sistémicas para todo el ecosistema financiero y la economía del país. Esta investigación responde a la necesidad apremiante de comprender y abordar estas vulnerabilidades, hasta ahora insuficientemente estudiadas en el contexto nacional.

Teniendo en cuenta que los ataques cibernéticos impactan las empresas Fintech en múltiples dimensiones. Más allá de las pérdidas económicas directas por sustracción de fondos, robo de datos o interrupción operativa, el daño reputacional resulta particularmente devastador. La pérdida de confianza de los clientes ante filtraciones de información personal o financiera produce contracciones en los ingresos y reducción de cuota de mercado. Adicionalmente, la competencia puede explotar la información sustraída para mejorar sus propios productos, agravando la posición competitiva de las empresas afectadas.

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

Este estudio contribuirá a fortalecer la seguridad y protección de información sensible en el sector Fintech. Al identificar y analizar los principales vectores de riesgo cibernético, facilitará la implementación de medidas preventivas que salvaguarden tanto la infraestructura tecnológica como los activos financieros. mejorará los procesos de toma de decisiones en materia de ciberseguridad, promoviendo la adopción de estrategias de protección financiera más robustas y adaptativas. Esto potenciará la resiliencia organizacional y la capacidad de respuesta ante incidentes, preservando el activo más valioso de estas empresas: la confianza y credibilidad ante clientes, colaboradores y el ecosistema financiero.

El proyecto trasciende la mera identificación de riesgos para evaluar metódicamente su impacto en indicadores financieros críticos, permitiendo cuantificar el efecto de los ciberataques en la rentabilidad y sostenibilidad financiera. Las estrategias de mitigación propuestas, fundamentadas en mejores prácticas internacionales de ciberseguridad y gestión de riesgos, contribuirán a fortalecer la resiliencia sectorial con un impacto social tangible: preservación de empleos, estabilidad del sector financiero y promoción de la inclusión financiera mediante servicios digitales confiables.

Metodológicamente, el estudio integra análisis cuantitativo y cualitativo para una comprensión holística de los riesgos cibernéticos y sus repercusiones financieras. Este enfoque riguroso no solo garantiza la validez de los hallazgos, sino que establece un referente para futuras investigaciones en finanzas corporativas y ciberseguridad. La investigación enriquece la literatura académica sobre gestión de riesgos financieros derivados de ataques cibernéticos en el sector Fintech de lending, un campo emergente de creciente relevancia.

El análisis se concentra en las empresas Fintech de Bogotá que ofrecen servicios de préstamos (lending), que constituyen una proporción significativa del sector nacional debido a la

evolución en la sofisticación de los ciberataques, permitiendo analizar tendencias y patrones en un contexto de alta vulnerabilidad. Los beneficiarios de esta investigación inician con las empresas Fintech que adquirirán conocimientos estratégicos para robustecer su estabilidad financiera y gestionar eficazmente los riesgos cibernéticos.

Asimismo, La sociedad se beneficiará de servicios financieros digitales más seguros y confiables. Los estudiantes participantes desarrollarán competencias especializadas en análisis de riesgos financieros y ciberseguridad, altamente valoradas en el mercado laboral actual. Finalmente, el programa de especialización de UNIMINUTO fortalecerá su prestigio académico al abordar desafíos cruciales para el progreso económico y social de Colombia, posicionándose como referente en la intersección entre seguridad digital y sostenibilidad financiera.

3. Objetivos

3.1. Objetivo general

Analizar los principales riesgos cibernéticos que afectan las finanzas corporativas de las empresas Fintech en la ciudad de Bogotá

3.2. Objetivos específicos

- Identificar conceptualmente los tipos de amenazas cibernéticas más comunes que afectan a las empresas Fintech en Bogotá.
- Evaluar la magnitud y el impacto económico que estos riesgos tienen en las finanzas corporativas de las empresas analizadas.
- Proponer medidas y estrategias para minimizar y prevenir los riesgos cibernéticos en las finanzas corporativas de las empresas del sector servicios en Bogotá.

4. Marco de referencia

4.1. Marco teórico

Los cambios tecnológicos acelerados han transformado absolutamente la forma en que interactuamos con los servicios financieros. Las Fintech representan una disrupción que puede mejorar la eficiencia en los intercambios financieros y resolver problemas de información mediante nuevas tecnologías y plataformas digitales (CNMC, 2018). las empresas Fintech han llegado a convertirse en un instrumento conveniente para los negocios, debido a que posibilitan la ejecución de transacciones alrededor del mundo de manera más dinámica, gracias a su agilidad, innovación y bajos costos; pues en el pasado las personas necesitaban trasladarse a diversos lugares para realizar todo tipo de transacciones (López Llorente, 2022; Rodríguez, & Rodríguez, 2021).

Actualmente hay un creciente uso de tecnología Fintech que ha revolucionado el panorama financiero global. El crecimiento de las compañías Fintech en el mundo ha sido exponencial. Solamente en 2021, se registraron en el mundo USD 210 billones y 5.684 negociaciones cerradas de inversión en Fintech (KPMG, 2022). En concordancia, El ecosistema Fintech en Colombia continúa consolidándose al experimentar un crecimiento estabilizado, con

un aumento del 6.8% en el número de emprendimientos en comparación con el 2023 (Finnovista, 2024).

Ante este progresivo uso de tecnologías financieras digitales, hay mayor preocupación por estar a la vanguardia tecnológica en un entorno cada vez más competitivo. De acuerdo con Ceballos Rincón y Castro Peñaloza (2022) “La evolución del modelo de negocio está enmarcada en la transformación digital, son miles de startups o sector Fintech los que están desafiando los múltiples productos y servicios que un banco puede ofrecer; este nuevo sistema, está cambiando por completo el horizonte del sector bancario tradicional". Asimismo, Asobancaria (2024) afirma que el aumento en el número de competidores en ese campo es prueba de que este es el presente y futuro del negocio financiero.

En respuesta a esta presión competitiva por mantenerse vigentes, las instituciones financieras se encargaron de desarrollar soluciones tecnológicas orientadas a mejorar la experiencia del usuario. Como lo expone (Jiménez Cardozo et al., 2024). La transformación digital en el sector bancario es un proceso fundamental para adaptarse a las demandas cambiantes de los clientes. En un principio cuando las Fintech empezaron a tener gran repercusión se consideraban una amenaza para la banca tradicional, pero con el pasar de los años este sistema de financiamiento alternativo se ha convertido en la puerta de acceso a la transformación (Barrera Rodríguez & Narváez Martínez, 2021).

Sin embargo, a pesar de este auge en el desarrollo tecnológico, existe una preocupante falta de sensibilización sobre la protección frente a amenazas cibernéticas inherentes a esta transformación digital. Según Finnovista (2023), más de la mitad de las empresas Fintech (50,5%) no reconocen la importancia crítica de fortalecer y actualizar sus sistemas de seguridad cibernética. Esta desatención contrasta con la realidad del panorama de amenazas, pues según

Asobancaria (2024), los ciberataques se han triplicado en la última década, siendo el sector de servicios financieros uno de los blancos preferidos por los atacantes.

Ya que no se han desarrollado medidas de protección en la misma proporción que los avances tecnológicos, muchas organizaciones se encuentran vulnerables ante ataques cada vez más sofisticados. Como argumenta el Foro Económico Mundial (2024). América Latina y África reportaron el mayor número de organizaciones insuficientemente ciber resilientes. Adicionalmente, las cifras adquieren aún mayor magnitud, pues los daños económicos de los ataques cibernéticos podrían sobrepasar el 1 % del producto interno bruto (PIB) en algunos países. En el caso de los ataques a la infraestructura crítica, esta cifra podría alcanzar hasta el 6 % del PIB (BID & OEA, 2020).

Estos servicios generan unos riesgos cibernéticos específicos que evolucionan constantemente. Como explica el Foro económico mundial (2025) el cibercrimen aumentó tanto en frecuencia como en sofisticación, marcado por ataques de ransomware, tácticas mejoradas con IA (como phishing, vishing y deepfakes). igualmente, los ciberataques han llevado a la ciberseguridad a evolucionar en la gestión de las ciber amenazas, 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).

Adicionalmente, estos riesgos impactan la operatividad y las finanzas corporativas de manera significativa. Según Asobancaria (2024), " un ataque a una institución financiera relevante, o a un servicio muy utilizado por los participantes del sistema financiero, se podría propagar con rapidez, causando perturbaciones importantes y minando la confianza de los consumidores financieros e inversionistas ". complementa el Foro económico mundial (2025)

afirmando que “el impacto de la ciberdelincuencia es de gran alcance: puede paralizar las operaciones, socavar la confianza y afectar a nuestra tecnología operativa e infraestructura crítica”.

Cabe destacar que estos ataques pueden llevar a la quiebra una empresa en corto o largo plazo dependiendo del tipo de intrusión. Dado el carácter sistémico del cibercrimen, las agencias reguladoras deben prestar especial atención a este riesgo, con el fin de evitar episodios que puedan terminar en crisis financieras (Clavijo Ramírez et al., 2017). En cuanto al impacto financiero de una pérdida de reputación, el sector financiero es el segundo más vulnerable a la pérdida de clientes (Organización de los Estados Americanos [OEA], 2018).

En las finanzas corporativas, es crucial desarrollar estrategias para enfrentar los retos de la ciberseguridad. Como establece el Foro económico mundial (2025). Existe la necesidad de que los líderes cuantifiquen los riesgos cibernéticos y sus impactos económicos para alinear las inversiones con los objetivos comerciales centrales y asignar un presupuesto suficiente a la contratación de profesionales de ciberseguridad.” (Aguilar, 2017) argumenta que “se requiere, desde ya, una alta inversión en ciberseguridad, dado que la falta de inversión producirá grandes problemas en organizaciones y empresas”.

Las estrategias financieras preventivas ante amenazas cibernéticas constituyen una ventaja. Según Ávalos Ochoa (2023)” la prevención de nuevos riesgos; debe incluir una sólida comprensión de las implicaciones en caso de materializarse las amenazas, mediante la presentación de escenarios, para informar futuras acciones que lleven a la decisión en el presente”. En el caso Fintech la automatización de los requisitos de cumplimiento y elaboración de informes regulatorios, y facilitando una mayor cooperación intersectorial y jurisdiccional (Mejía & Azar, 2021; López Rodríguez et al., 2022).

Para finalizar, La resiliencia financiera ante ataques cibernéticos es un elemento diferenciador. Conforme lo indica el Foro Económico Mundial (2025) “una estrategia que puede ayudar a las organizaciones es a ser resilientes es la contratación de seguros para cubrir los impactos de los ciberataques. Sin embargo, Entidades con un alto capital bancario pueden verse seriamente afectadas por el riesgo cibernético sin que el capital contribuya a moderar los efectos de su materialización (Ramírez et al., 2017).

4.2. Marco legal

El ecosistema Fintech en Colombia opera bajo un marco regulatorio que evoluciona continuamente para adaptarse a los desafíos de la digitalización financiera, tales como;

- Ley 527/1999: Base para transacciones electrónicas
- Ley 1266/2008: Derecho a "conocer, actualizar y rectificar la información recopilada" (Ley 1266, 2008)
- Ley 1273/2009: "Crea nuevos tipos penales relacionados con delitos informáticos" (Yustes, 2021) ante "ataques cibernéticos" crecientes (Centro Nacional de Seguridad Cibernética del Reino Unido, 2020)
- Leyes 1328/2009 y 1480/2011: Protección contra "daño reputacional derivado de los ciberataques" (Álvarez Flórez y Preciado Uribe, 2021)
- Ley 1581/2012: Exige "medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad de los datos" (Congreso de Colombia, 2012)
- Ley 1735/2014: "Promueve la inclusión financiera" (Colombia Fintech, 2022)

- Ley 1955/2019 y Decreto 1234/2020: Sandbox regulatorio para "pruebas tecnológicas sin licencia previa" (Yustes, 2021)
- Circulares 007-008/2018: Gestión de riesgos con "sanciones por incumplimiento" (SFC, 2021)

Complementan: Comité de Basilea ("escenarios relacionados con amenazas cibernéticas", 2021), ISO 27001 y Convenio Budapest para "perseguir delitos cibernéticos transnacionales" (Ministerio de Relaciones Exteriores, 2018).

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

5. Metodología

5.1. Alcance de la investigación

Se adopta un alcance exploratorio debido a la limitada documentación sobre el impacto financiero de los ciberataques específicamente en empresas Fintech de Bogotá, en especial en las que ofrecen prestamos o lending. Según Martínez y Ochoa (2023) "los estudios exploratorios resultan fundamentales cuando se abordan fenómenos emergentes o poco estudiados, permitiendo identificar variables críticas y establecer prioridades para investigaciones futuras". Esta aproximación es relevante considerando que "la adaptación de estándares internacionales de ciberseguridad al contexto financiero colombiano requiere un análisis previo de las condiciones locales y sus particularidades operativas" (Sánchez & López, 2023).

El alcance exploratorio se caracteriza por examinar fenómenos sobre los cuales existe poca información sistematizada, permitiendo identificar variables relevantes. Según Hernández y Fernández (2022), "los estudios exploratorios constituyen el primer acercamiento científico a problemáticas emergentes, facilitando la comprensión de sus dimensiones fundamentales". Este enfoque resulta valioso en sectores en transformación como el financiero-tecnológico, pues como señalan Ramírez y Contreras (2023) "la naturaleza dinámica de las amenazas cibernéticas demanda aproximaciones exploratorias para capturar la complejidad del fenómeno".

5.2. Enfoque metodológico

El enfoque metodológico mixto combina herramientas cualitativas y cuantitativas que permiten lograr una visión global de los principales riesgos que afectan las finanzas corporativas derivados de los ciberataques en las empresas Fintech de Bogotá, dicha información es esencial para contrastar diversas fuentes de información y detectar patrones comunes en la problemática estudiada. Además, proponer recomendaciones prácticas y aplicables.

En el aspecto cualitativo, se entrevistará un experto en consultoría de ciberseguridad, lo que permitirá conocer experiencias, estrategias de mitigación ante amenazas digitales y los desafíos específicos a consecuencia de ciberataques en empresas Fintech, La entrevista proporciona perspectivas valiosas y contextualizadas. Por otro lado, el enfoque cuantitativo se sustenta en un análisis documental de informes globales, estudios publicados y datos secundarios relacionados con el impacto financiero de los ciberataques. Que, aunque no provengan directamente de empresas Fintech locales, ofrecen indicadores o tendencias generales en el sector. Estos datos pueden servir como base para estimar el impacto financiero.

5.3. Población y muestra

La población objetivo son empresas Fintech de préstamos o lending de Bogotá, Colombia. El estudio emplea metodología mixta con muestreo no probabilístico por conveniencia. La fase cualitativa incluye entrevista a experto en ciberseguridad con siete años de experiencia. La fase cuantitativa analiza documentos técnicos, reportes sectoriales y bases de datos sobre ciberataques en el sector financiero-tecnológico de entidades reconocidas. La muestra documental abarca estadísticas de impacto financiero, métricas de pérdidas económicas, análisis de costos e indicadores de inversión en protección digital. Se excluyen documentos sin respaldo metodológico. Este enfoque mixto permitirá triangular información.

5.4. Instrumentos

Para el análisis de principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá, se ha seleccionado la técnica mixta de entrevista y análisis documental ya que las dos permiten recopilar datos en profundidad y obtener una comprensión detallada de las percepciones y experiencias de los participantes con relación a los riesgos cibernéticos puesto que la integración de ambas técnicas enriquece la investigación al permitir la triangulación de datos, lo que incrementa la robustez y fiabilidad de los resultados obtenidos.

Por un lado, la técnica de entrevista permite obtener información detallada a través de la conversación entre el investigador y el participante. Según Marshall y Rossman (2014), la entrevista es una técnica en la que se construye una conversación para obtener información relevante sobre el tema que se está investigando. Por otro lado, como señalan Johnson y Christensen (2020), "el análisis documental es una herramienta poderosa para obtener datos

cuantitativos confiables, especialmente cuando el acceso a información primaria es limitado" (p. 145). Además, la integración de ambos métodos se inscribe dentro del enfoque mixto, el cual permite combinar la profundidad cualitativa con la objetividad cuantitativa para lograr una comprensión más completa del fenómeno estudiado. En palabras de Creswell y Plano Clark (2011), "la integración de datos cualitativos y cuantitativos en una investigación mixta proporciona una comprensión más completa del problema de investigación que el uso de un solo enfoque" (p. 6)

5.5. Procedimientos

El procedimiento inicia con la definición del propósito de la entrevista y la selección del experto en ciberseguridad, estableciendo objetivos claros. Luego, se diseña un guion con preguntas abiertas, el cual se revisa y valida antes de la entrevista. Una vez programada y realizada la sesión, se transcribe e interpreta la información obtenida. Posteriormente, los hallazgos se contrastan con el análisis documental para garantizar coherencia y complementar la investigación. Finalmente, se elabora un informe que sintetiza los resultados y presenta recomendaciones estratégicas para mitigar los riesgos financieros en empresas Fintech ante ataques cibernéticos.

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

Figura 1. Flujograma de entrevista

Fuente: elaboración propia

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

Tabla 1.Marco lógico para entrevista

Objetivos específicos	Categorías orientadoras	Ejes de indagación	Preguntas
Objetivo 1: Identificar conceptualmente los tipos de amenazas cibernéticas más comunes que afectan a las empresas Fintech en Bogotá.	Seguridad informática en Fintech	Principales ataques y vulnerabilidades	- ¿Cuáles son las amenazas más comunes que enfrentan las empresas Fintech actualmente y qué tipos de datos suelen ser más vulnerables en estas plataformas?
		Errores comunes en la seguridad	¿Por qué algunas empresas Fintech subestiman la importancia de la ciberseguridad y cuáles son los errores más frecuentes en la seguridad cibernética de estas, qué estrategias pueden implementar para mejorar la gestión de sus protocolos de seguridad?

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

Objetivo 2: Evaluar la magnitud y el impacto económico que estos riesgos tienen en las finanzas corporativas de las empresas analizadas.	Consecuencias de un ataque cibernético	Impacto financiero y pérdida de confianza del cliente	¿Podría compartir un caso real (sin revelar información confidencial) donde un ataque afectó gravemente a una empresa Fintech, qué impacto financiero tuvo en el corto y largo plazo?
		Estrategias de mitigación y recuperación	- ¿Qué estrategias pueden implementar las instituciones financieras para recuperar la confianza de los clientes después de sufrir un ciberataque significativo?
Objetivo 3 Proponer medidas y estrategias para minimizar y prevenir los riesgos cibernéticos en las finanzas corporativas de las empresas del sector servicios en Bogotá.	Protección y prevención en ciberseguridad	Tecnologías emergentes en ciberseguridad	¿Qué tecnologías emergentes están mejorando la ciberseguridad en Fintech y cómo puede la inteligencia artificial ayudar a prevenir ataques cibernéticos?

	Desafíos en la implementación de medidas de seguridad	¿Cuál es el principal desafío en la implementación de protocolos de seguridad en el sector Fintech, cómo pueden estas empresas encontrar un equilibrio entre seguridad y experiencia del usuario?

Fuente: Elaboración propia

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

El flujograma inicia con la definición de criterios de búsqueda y la selección de fuentes confiables, asegurando la validez de los datos. Posteriormente, se lleva a cabo la recolección y revisión documental de informes, estudios y artículos relevantes. La información recopilada es clasificada según su relevancia y utilidad para el análisis. Luego, se realiza la evaluación de impactos con base en datos cuantificables, identificando tendencias y patrones. A partir de ello, se realiza un seguimiento y actualización de fuentes para garantizar la vigencia de la información. Finalmente, se elabora el informe final, consolidando los hallazgos mediante un enfoque analítico y basado en evidencia numérica.

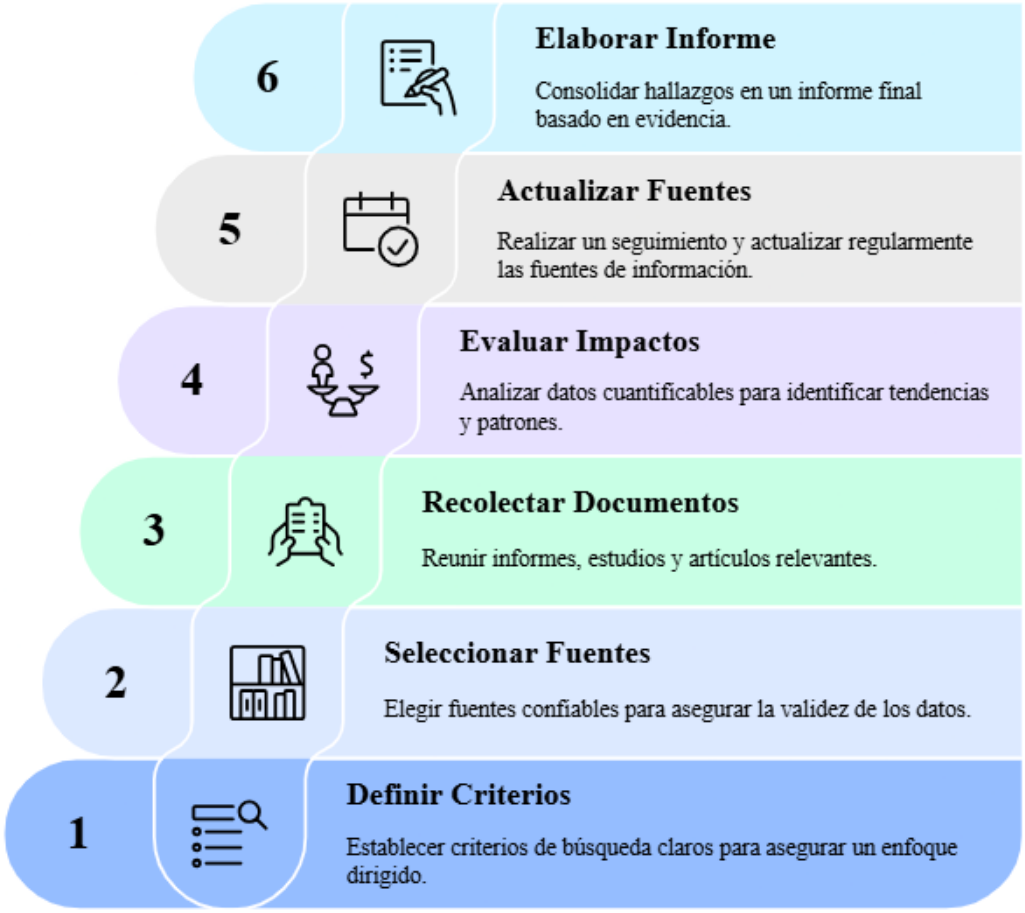

Figura 2.Flujograma de análisis documental

Fuente: elaboración propia

5.6. Consideraciones éticas

El proyecto implementará los principios éticos de Uniminuto mediante: Beneficencia, No maleficencia, maximizando beneficios y minimizando riesgos para los participantes; Justicia, asegurando selección equitativa y distribución justa de cargas y beneficios; y Respeto por las personas, aplicando consentimiento informado para proteger autonomía y confidencialidad. Se

anexarán documentos esenciales como consentimientos firmados, autorizaciones institucionales, aprobación del comité de ética y protocolos de manejo de datos sensibles, garantizando el cumplimiento de todos los estándares éticos requeridos.

6. Resultados

Una vez aplicada la entrevista al experto en ciberseguridad, se recopiló la siguiente información organizada según los objetivos específicos de la investigación:

6.1. Identificación conceptual de los tipos de amenazas cibernéticas más comunes que afectan las empresas

Las amenazas más comunes en empresas Fintech se dividen en dos, aquellas que quieren generar filtración es decir que el atacante ingresa al sistema por ejemplo ataques de phishing y spear phishing, Ingeniería social, vulnerabilidades en los servicios expuestos (mensajería, CHATBOTS, APIS ,WEB, bases de datos), Compromiso de credenciales y aquellos ataques que generan indisponibilidad de los servicios o ataques de Denegación de Servicio Distribuido tales como; Ataques de denegación de servicio (DDoS), Encriptación de información (Ramsonware y Malware),amenazas internas por empleados malintencionados, falta de capacitación o que hagan parte de un ataque de cadena de suministro.

En cuanto a los datos más vulnerables en orden de criticidad son:

- Datos personales de clientes y/o terceros (número de documento, nombres y apellidos, email, número de contacto, entre otros)
- Datos financieros (números de productos financieros, historiales de transacciones)

- Funcionamiento de la infraestructura tecnológica (Algoritmos propietarios y modelos de calificación crediticia que usa la empresa)
- Información de conocimiento de cliente o KYC (perfil del cliente, biometría, reconocimiento facial)

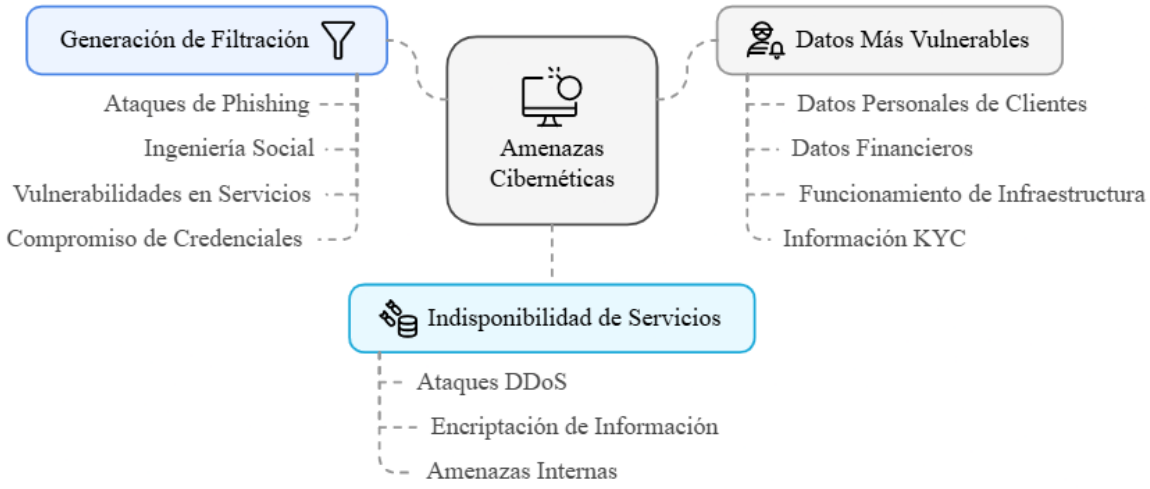

Figura 3. Amenazas más comunes que enfrentan las empresas Fintech

Fuente: Elaboración propia basada en la información suministrada por el experto en ciberseguridad

Las empresas Fintech enfrentan dos tipos principales de ataques cibernéticos,

siendo uno de los más críticos los ataques de ingeniería social y vulnerabilidades de día cero que hacen parte de las amenazas de filtración la razón principal por la que esta modalidad de ciberataque se ha convertido en el vector de amenaza más peligroso es porque en cualquier organización el ser humano es más propenso a errores por desconocimiento, adicionalmente los atacantes aprovechan las debilidades psicológicas de empleados y usuarios para penetrar los sistemas por medio de las diferentes herramientas que usan los ciberdelincuentes, sumando a esto

tener presente que por un ataque de filtración se puede llegar a generar indisponibilidad de los servicios lo cual generará mayores costos financieros a las organizaciones ya que pueden perder activos digitales, no generar ventas, dependiendo del ataque puede disminuir su reputación y perder clientes, además de incurrir en problemas legales por la pérdida de información confidencial de los clientes y de la compañía.

El interés de hacer sistemas funcionales para generar ingresos y el desconocimiento de los riesgos asociados al implementar estos servicios sumado al bajo interés en invertir en este rubro porque consideran que es un gasto innecesario en lugar de una inversión estratégica para la protección y sostenibilidad del negocio.

Errores más frecuentes

- Controles inadecuados para amenazas internas en colaboradores
- Ausencia de infraestructura tecnológica de contingencia para mitigar ataques de indisponibilidad por zonas
- Carencia de controles de seguridad periódicos
- No disponer de auditorías para los proveedores de servicios tecnológicos.

Estrategias para mejorar la gestión

- Realizar capacitaciones de ciberseguridad a los colaboradores de forma periódica que permita prevenir ser víctimas de Phishing o suplantación de identidad

- Implementar infraestructura de contingencia para los servicios tecnológicos críticos de la compañía esto permitirá en caso de catástrofe natural o ciberataque masivo restablecer la disponibilidad de los servicios de forma instantánea
- Estrategias para controles de seguridad
- Adoptar seguridad por diseño o arquitectura por servicio
- Desplegar estrategia Zero Trust para todos los sistemas de autenticación y casos de uso de monitoreo
- Respuestas de incidentes y plan de gestión de riesgos
- Integrar DevSecOps en el flujo de lanzamiento de un producto tecnológico

Figura 4. Errores y estrategias de ciberseguridad para Fintech

Fuente: Elaboración propia basada en la información suministrada por el experto en ciberseguridad

Las empresas Fintech priorizan su rentabilidad y ampliación de portafolio de servicios, descuidando la ciberseguridad la cual tendría que ir en paralelo a estos lanzamientos debido a que al momento de implementar nuevo software existe la posibilidad de que se hayan abierto puertas para los ciberdelincuentes, muchas veces este rubro no es tenido en cuenta por

desconocimiento ya que falta una cultura de ciberseguridad y regulación más estricta, es relevante mencionar que las empresas no contemplan esta inversión ya que lo ven como un gasto y no contemplan la posibilidad de sufrir un ataque cibernético que puede generarle un impacto negativo en sus finanzas.

Un caso significativo en el sector Fintech fue un ataque registrado en 2019, Donde un proveedor de servicios en la nube explotó una vulnerabilidad en la configuración del firewall de aplicaciones web de la compañía esto le permitió tener acceso a un aproximado de 100 millones de solicitudes de un producto financiero y acceso a aproximadamente de 6 millones de cuentas de clientes.

Impacto financiero a corto plazo:

- Multa por reguladores bancarios
- Acuerdo para resolver demandas colectivas de clientes
- Costos inmediatos de mitigación y respuesta
- Caída en el valor de sus acciones en los días posteriores al anuncio

Impacto financiero a largo plazo:

- Gastos millonarios en procesos de investigaciones, litigios y remediación
- Inversión considerable para mejoras de ciberseguridad
- Aumento en costos de primas de seguros cibernéticos
- Pérdida de ventaja competitiva en el sector Fintech emergente

Impacto en la confianza del cliente:

- Cancelaciones de servicios financieros
- Disminución en la adquisición de nuevos clientes

- Daño a la percepción de marca como innovador digital segura
- Inversiones en campañas de recuperación de confianza
- Escrutinio regulatorio aumentado que limitó la velocidad de innovación

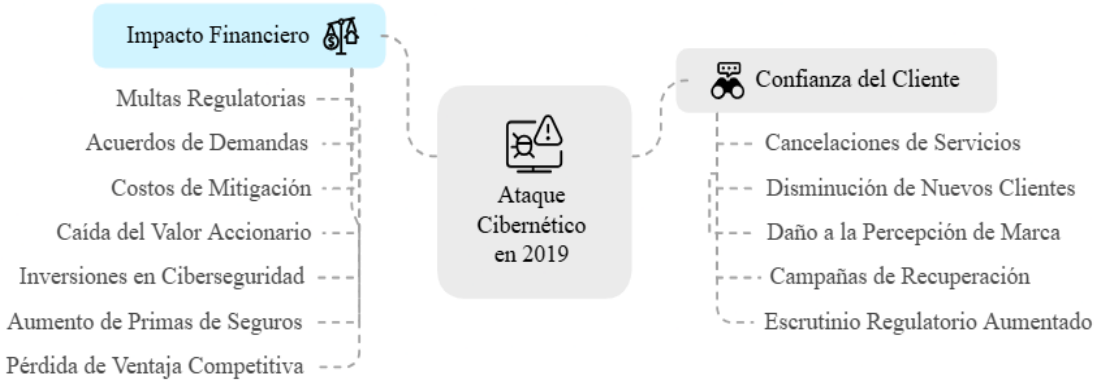

Figura 5.Caso de ataque cibernético en Fintech

Fuente: Elaboración propia basada en la información suministrada por el experto en ciberseguridad

Con el caso suministrado por el especialista se evidencia que el vector de ingreso que genero la ocurrencia del ataque fue humano por un colaborador de la compañía, eso se pudo evitar si la empresa hubiese implementado controles de ciberseguridad ya que al parecer no contaban con protocolos adecuados para mitigar este fallo, cabe resaltar que se evidencia una pérdida de confianza en sus clientes, un daño reputacional considerable que impacto la rentabilidad y desplazo la marca de su posicionamiento en el mercado.

El análisis cuantitativo de los impactos económicos de los ciberataques en el sector Fintech revela una dimensión crítica de los riesgos de ciberseguridad. Las tablas presentadas ofrecen una perspectiva de los costos potenciales que una empresa puede enfrentar tras un

incidente de seguridad digital, proporcionando un marco metodológico para comprender la magnitud financiera de estas amenazas.

Tabla 2. Estimación de costos de un ataque cibernético

Categoría de costo	**Tipo de costo**	**Componentes específicos**	**Estimación aproximada en USD**
Costos directos	Inmediatos	Investigación forense digital	$30,000- $150,000
		Asesoría legal especializada	$50,000 - $200,000
		Notificaciones y comunicaciones con clientes	$15,000 -$75,000
		Implementación de medidas de seguridad inmediatas	$75,000- $400,000
		Recuperación de sistemas	$100,000- $600,000
	Subtotal costos directos		**$270,000 - $1,425,000**
Costos indirectos	Reputacionales	Pérdida de confianza de clientes	$750,000 - $3,000,000

	Disminución en adquisición de nuevos clientes	$300,000 - $1,500,000
Operativos	Interrupción de operaciones	$150,000- $1,000,000
	Reducción de productividad	$100,000-$500,000
Regulatorios	Multas y sanciones	$300,000 $3,000,000
Legales	Potenciales demandas	$150,000 $1,500,000
Subtotal costos indirectos		$1,750,000 $10,500,000
Costo Total estimado		**$2,020,000 $11,925,000**

Fuente: Elaboración propia con datos de fuentes internacionales

Nota: Las estimaciones son aproximadas y pueden variar según el contexto específico de cada empresa Fintech. Se recomienda una evaluación personalizada.

La anterior tabla presenta una estimación de los costos asociados a un ciberataque, divididos en dos categorías principales:

- **Costos Directos**: incluyen gastos inmediatos y tangibles como: investigación forense digital, asesoría legal, notificaciones a clientes, implementación de medidas de seguridad, recuperación de sistemas.

- **Costos Indirectos** representan impactos más sutiles, pero potencialmente más devastadores que incluyen: pérdida reputacional, disminución en adquisición de clientes, interrupción operativa, reducción de productividad, multas regulatorias, potenciales demandas legales

Los costos directos derivados de un ciberataque representan los gastos inmediatos y tangibles en los que incurre una empresa Fintech para contener, investigar y mitigar los efectos del incidente. Estos costos son esenciales para la recuperación operativa y la protección de los activos de la empresa. A continuación, se presenta un desglose detallado de estos costos, que ofrece una estimación en USD:

- **Investigación Forense Digital** Tras un ciberataque, es crucial determinar la causa raíz, el alcance de la intrusión y los sistemas comprometidos. La investigación forense digital implica la contratación de expertos en ciberseguridad para analizar los registros del sistema, identificar las vulnerabilidades explotadas y rastrear la actividad de los atacantes. Estos servicios especializados pueden incurrir en costos significativos, dependiendo de la complejidad del ataque y el tamaño de la infraestructura afectada.
- **Asesoría Legal Especializada** Los ciberataques a menudo conllevan implicaciones legales, especialmente en el sector Fintech, donde se maneja información financiera sensible. La asesoría legal especializada es necesaria para evaluar las obligaciones de notificación de la empresa, cumplir con las regulaciones de privacidad de datos (como la Ley 1581 de 2012 en Colombia), y defenderse de posibles demandas. Los

costos de asesoría legal pueden variar según la gravedad de la violación de datos y la complejidad del marco legal.

- **Notificación y Comunicación con Clientes** En caso de una violación de datos que afecte a los clientes, las empresas Fintech están obligadas a notificar a los usuarios afectados y proporcionarles información sobre el incidente y las medidas que pueden tomar para protegerse. Los costos de notificación pueden incluir el envío de correos electrónicos, cartas o mensajes de texto a los clientes, así como la creación de líneas de atención al cliente para responder a las preguntas y preocupaciones. La gestión de la comunicación pública y la mitigación del daño reputacional también contribuyen a estos costos.

- **Implementación de Medidas de Seguridad Inmediatas:** Después de un ciberataque, es fundamental fortalecer las defensas de seguridad para prevenir futuros incidentes. Esto puede implicar la implementación de nuevas soluciones de seguridad, como firewalls, sistemas de detección de intrusiones, software antivirus y herramientas de cifrado. También puede requerir la actualización de los sistemas existentes, la aplicación de parches de seguridad y la realización de pruebas de penetración para identificar y corregir vulnerabilidades.

- **Recuperación de Sistemas:** Un ciberataque puede dañar o interrumpir los sistemas informáticos de una empresa Fintech, lo que requiere esfuerzos de recuperación para restaurar la funcionalidad y la disponibilidad de los servicios. Esto puede implicar la reparación o el reemplazo de hardware dañado, la reinstalación de software, la recuperación de datos de copias de seguridad y la realización de pruebas exhaustivas para

garantizar que los sistemas estén funcionando correctamente. La complejidad y el alcance de la recuperación del sistema pueden variar según la gravedad del ataque y la preparación de la empresa para la recuperación ante desastres

En conjunto, los costos directos asociados con un ciberataque pueden oscilar entre $400,000 y $1,900,000 USD, dependiendo de la magnitud y la complejidad del incidente, así como de la preparación y la capacidad de respuesta de la empresa. Es importante tener en cuenta que estas son solo estimaciones, y los costos reales pueden variar significativamente en función de las circunstancias específicas de cada ataque.

Costos Indirectos, sutiles, pero potencialmente devastadores

- **Pérdida de confianza del cliente**: El daño reputacional es particularmente devastador. Las filtraciones de información personal o financiera generan pérdida de confianza en los clientes, lo que se traduce en una disminución de ingresos y cuota de mercado.

- **Disminución en la adquisición de nuevos clientes**: La pérdida de confianza debido a brechas de seguridad afecta negativamente la capacidad de la empresa para atraer nuevos clientes.

- **Interrupción operativa:** Los ciberataques pueden afectar los sistemas de una Fintech, impactando su capacidad para ofrecer servicios y operar con normalidad, lo que genera pérdidas financieras.

- **Reducción de productividad**: El documento señala que la disminución de la productividad es un costo indirecto derivado de los ciberataques.

- **Multas y sanciones regulatorias:** Las Fintech enfrentan un escrutinio regulatorio creciente. Un ciberataque exitoso puede derivar en multas y sanciones significativas por incumplimiento de normativas de protección de datos y seguridad. Se hace referencia a las Circulares 007-008/2018, que destacan la gestión del riesgo y las posibles sanciones por incumplimiento.

- **Posibles demandas legales**: Las filtraciones de datos y otros incidentes de seguridad pueden generar demandas por de clientes afectados, inversionistas u otras partes, lo que conlleva gastos legales sustanciales y posibles acuerdos financieros.

Tabla 3. Fuentes de estimación de costos en ciberataques

Fuente	Año	Costo promedio brecha de seguridad	Metodología	Enlace de Descarga	Tipo de acceso

IBM Security	2023	$4.45 millones	Análisis global de 553 organizaciones	https://www.ibm.com/reports/data-breach	Requiere registro
Ponemon Institute	2022	$13.7 millones	86 organizaciones en 17 países	https://www.accenture.com/us-en/insights/security/cost-cybercrime-study	Parcialmente gratuito
Accenture	2022	$13 millones	Análisis en 16 industrias	https://www.accenture.com/us-en/insights/security/cyber-threat-intelligence	Requiere descarga
Deloitte	2023	$4.3 millones	Evaluación de riesgos financieros	https://www2.deloitte.com/global/en/pages/risk/cyber-strategic-risk.html	Requiere solicitud
McKinsey	2022	$5.2 millones	Análisis sectorial global	https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity	Acceso parcial
KPMG	2022	$4.8 millones	Estudio en empresas financieras	https://home.kpmg/xx/en/home/insights/2022/06/cyber-threat-report.html	Requiere registro

Fuente: Elaboración propia

Nota: Los datos y enlaces están sujetos a actualización

Consideraciones Metodológicas

1. Variables de Cálculo:

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

1. Tamaño de la empresa
2. Volumen de datos comprometidos
3. Sector financiero específico
4. Complejidad del ataque

2. Factores de Impacto:

5. Tiempo de respuesta
6. Efectividad de los protocolos de seguridad
7. Capacidad de recuperación

Advertencia: Los costos presentados son estimaciones basadas en estudios de mercado y requieren validación específica para cada organización

La anterior tabla ofrece un panorama comparativo de estimaciones de costos por brechas de seguridad según diferentes consultoras: el costo promedio de una brecha de seguridad oscila entre $4.3 y $13.7 millones, metodologías basadas en análisis globales que abarcan entre 16 y 553 organizaciones, variabilidad significativa que subraya la complejidad de la estimación precisa.

Demostrar a los clientes la implementación de una arquitectura integral de ciberseguridad diseñada para la detección y respuesta proactiva ante amenazas externas. Esta infraestructura incluye la aplicación de controles de endurecimiento avanzados para fortalecer el acceso a servicios de cara al cliente. Como garantía de calidad, todo el ecosistema de seguridad ha sido validado por entidades certificadoras reconocidas bajo estándares internacionales como ISO

27001 (SGSI), NIS y PCI, DSS, asegurando el cumplimiento de las mejores prácticas globales en protección de datos.

Desarrollar una campaña estratégica de comunicación a través de diversos canales de difusión, orientada a informar de manera transparente sobre las mejoras implementadas en materia de seguridad. Esta iniciativa busca no solo restablecer la confianza de los clientes actuales, sino también posicionar a la organización como referente en compromiso con la ciberseguridad ante el mercado y otras instituciones del sector.

Implementar un programa integral de alfabetización en ciberseguridad, proporcionando recursos educativos accesibles que empoderen a los clientes con conocimientos prácticos para la autoprotección de sus datos personales y financieros, fomentando así una cultura de responsabilidad compartida en materia de seguridad de la información, en colaboración con entidades reguladoras para garantizar una mayor difusión y alcance.

Adquirir seguros especializados en ciber riesgos constituye una estrategia fundamental para salvaguardar la estabilidad financiera de la compañía. Dado que se trata de un portafolio de naturaleza innovadora, es imperativo mantener una postura proactiva y dinámica en la gestión de estos instrumentos de protección, es decir revista coberturas y hacer evaluaciones periódicas debido a los cambios en las modalidades de ataques.

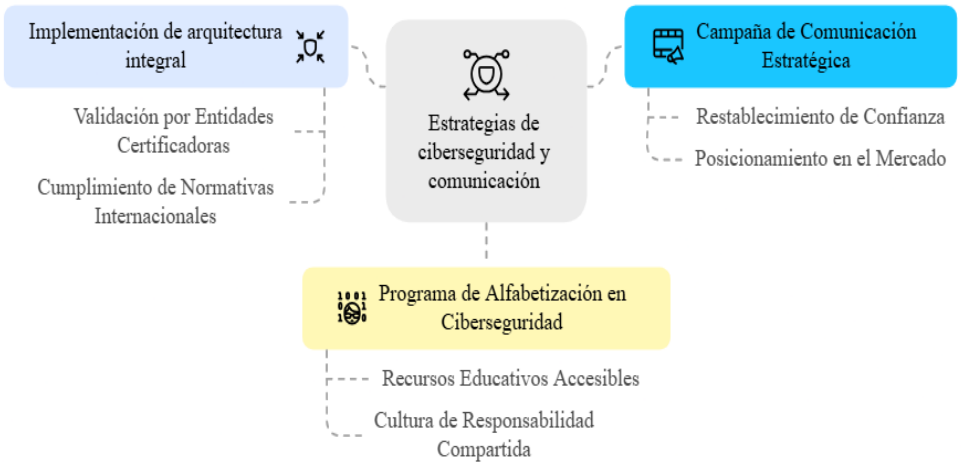

Figura 6.Estrategias de ciberseguridad y comunicación

Fuente: Elaboración propia basada en la información suministrada por el experto en ciberseguridad

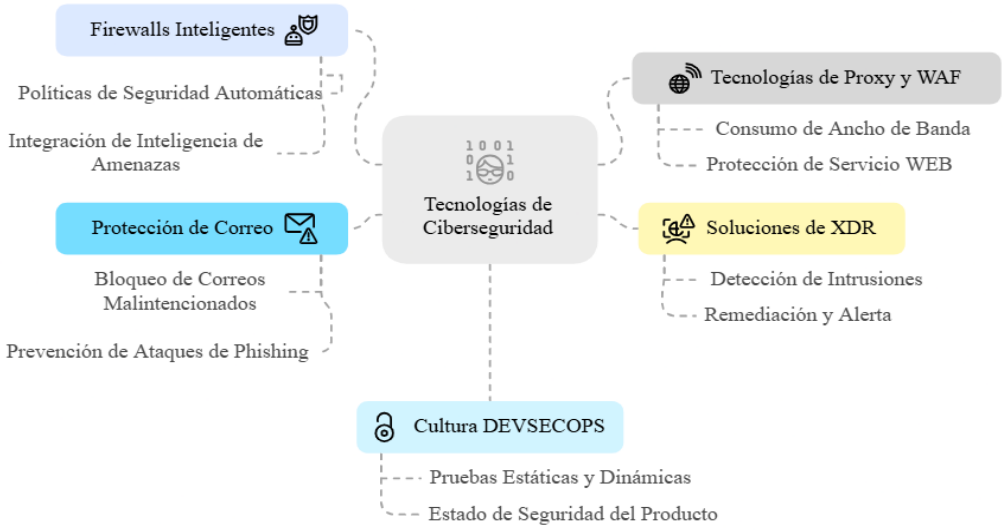

Figura 7.Tecnologías de Ciberseguridad

Fuente: Elaboración propia basada en la información suministrada por el experto en ciberseguridad

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

En el panorama tecnológico actual y de constantes cambios es imperativo integrar inteligencia artificial en temas de ciberseguridad que permita ampliar el alcance en inteligencia de amenazas permitiendo endurecer los complementos de cualquier arquitectura tecnológica mediante sistemas de detección predictiva y análisis de comportamientos sospechosos cada vez más sofisticados, también impulsar la adquisición de talento que formen equipos capaces de atender con agilidad y precisión, las demandas actuales en cuanto a amenazas en constante evolución**.**

El principal desafío para el sector Fintech es lograr un acuerdo a nivel gubernamental, privado y agencias internacionales para la implementación de protocolos de ciberseguridad por medio de regulaciones que blinden a las empresas del sector y a usuarios. En cuanto a las empresas Fintech su reto consiste en contar con una cultura en ciberseguridad y personal capacitado ya que a la fecha hay una escasez global de profesionales cualificados para ejecutar estas tareas, como se mencionó en la respuesta anterior hay muchas herramientas pero no personas que las empleen de manera óptima , personal que pueda elegir la infraestructura tecnológica para el servicio y poner en marcha los planes de trabajo delegados a los diferentes equipos para que esta estructura se incorpore correctamente.

La capacidad de una organización para anticiparse y gestionar riesgos cibernéticos se constituye como un activo estratégico fundamental en el entorno digital contemporáneo, donde la implementación de una arquitectura integral de seguridad, programas de alfabetización digital, comunicación estratégica y mecanismos de cobertura financiera no solo mitigan potenciales amenazas, sino que transforman la incertidumbre tecnológica en una oportunidad de

diferenciación, resiliencia y fortalecimiento organizacional, convirtiendo la prevención en el principal instrumento de protección empresarial

- Firewalls de última generación por medio de inteligencia artificial que permiten de acuerdo con el modelo de negocio crear políticas de seguridad de forma automática, adicionalmente estos ya vienen con una serie de utilidades que permiten integrar fuentes externas de inteligencia de amenazas (IOC) anti DDoS, spam y firmas de Malware.
- Contar con tecnologías de proxy y WAF a través de modelos de machine learning como CLOUDFLARE que permitan limitar el consumo de ancho de banda y proteger el servicio WEB
- Contar con una solución de XDR que cuenta con un módulo de inteligencia artificial en las estaciones de trabajo que permita detectar, contener, remediar y alertar una posible intrusión
- Contar un servidor para protección de correo que ayude a bloquear cualquier correo donde su contenido o encabezado sea malintencionado, esto para prevenir posibles ataques de phishing orientados a los colaboradores.
- Ya sea una infraestructura ONPREMISE o CLOUD es importante contar con la cultura DEVSECOPS dentro de sus pipelines que permitan sondear el producto a nivel de código con pruebas estáticas, dinámicas y a nivel de complementos o librerías y sistema operativo contenedor lo cual permitirá saber o mostrar el estado de seguridad de este nuevo producto donde será importante.

En resumen, la inteligencia artificial se encuentra implícita en la mayoría de las herramientas de ciberseguridad actuales, ya que los fabricantes de estas han incorporado modelos de predicción y aprendizaje autónomo de las tendencias en cuanto ataques cibernéticos y vulnerabilidades recientes, lo que impulsará la detección y respuesta de comportamientos sospechosos de manera eficiente y proactiva. Cabe resaltar que el éxito de un sistema seguro viene de la mano del personal capacitado en ciberseguridad que pueda sacar provecho de estas utilidades.

En cuanto a cultura de ciberseguridad se integran temas tales como; programas de capacitación, simulación de ataques controlados y aplicación de lecciones aprendidas.

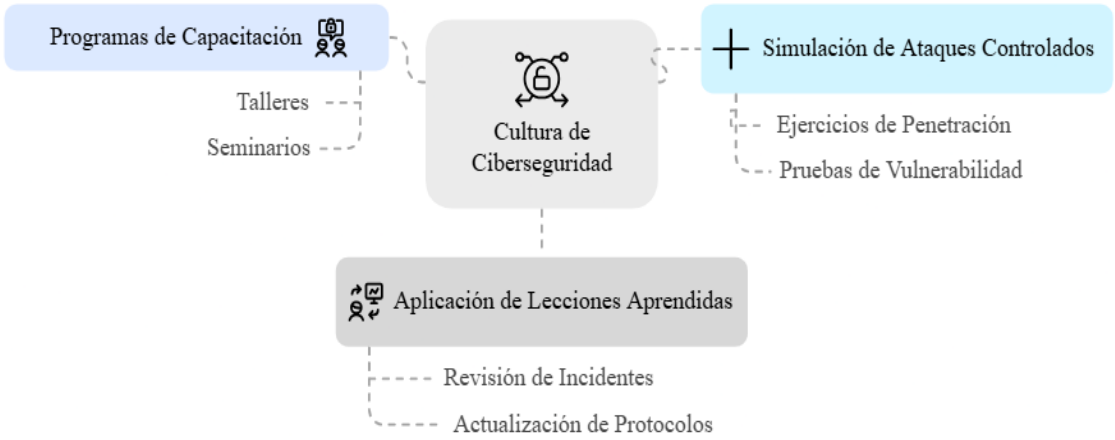

Figura 8.Cultura de ciberseguridad

Fuente: Elaboración propia basada en la información suministrada por el experto en ciberseguridad

La consolidación de un marco regulatorio integral en ciberseguridad demanda una colaboración estratégica entre el sistema gubernamental y el sector Fintech, orientada a desarrollar matrices de riesgo estandarizadas que configuren un protocolo unificado de

protección de activos digitales. Esta aproximación normativa no solo busca garantizar el resguardo de los intereses del sector financiero tecnológico, sino también salvaguardar los bienes y la información de los clientes, estableciendo lineamientos homogéneos que permitan a las organizaciones Fintech demostrar ante los entes de supervisión su compromiso con la gestión proactiva de riesgos cibernéticos y la seguridad integral de los ecosistemas digitales.

6.2. Magnitud e impacto económico de los riesgos en las finanzas corporativas de las empresas

Bogotá, consolidada como el epicentro financiero y tecnológico de Colombia, afronta una creciente vulnerabilidad en su floreciente sector Fintech ante el avance de amenazas cibernéticas sofisticadas. Estos riesgos digitales no solo comprometen a empresas individuales, sino que representan una amenaza sistémica para la integridad del ecosistema financiero nacional y la estabilidad económica del país.

La concentración del 62% de las empresas Fintech colombianas en la capital otorga a la ciudad una responsabilidad estratégica en el fortalecimiento de las defensas cibernéticas sectoriales es por ello que resulta imperativo implementar acciones preventivas inmediatas y coordinadas para salvaguardar este ecosistema digital de consecuencias devastadoras: filtración de información financiera sensible, compromisos masivos de datos personales, parálisis operativa de servicios esenciales, deterioro de la confianza del consumidor e inversionista, y la cascada de costos asociados al incumplimiento regulatorio en un entorno normativo cada vez más exigente.

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

Ante la escasez de estudios de casos públicos y documentados sobre el impacto financiero de incidentes cibernéticos en empresas Fintech colombianas, he optado por desarrollar dos casos hipotéticos basados en tendencias globales y características del ecosistema financiero digital de Bogotá. Estos escenarios simulados permiten cuantificar de manera ilustrativa las repercusiones económicas que enfrentarían las empresas del sector ante distintos tipos de incidentes.

Si bien estos casos no representan situaciones reales específicas, han sido construidos incorporando parámetros realistas del mercado local, incluyendo: tamaños típicos de empresas Fintech bogotanas, estructuras de costos prevalentes en el sector, comportamiento documentado de clientes ante incidentes de seguridad, y el marco regulatorio financiero colombiano vigente. Este enfoque permite visualizar y dimensionar tangiblemente cómo los riesgos cibernéticos se traducen en impactos concretos en las finanzas corporativas.

A continuación, se presentan un escenario hipotético que ilustran diferentes vectores de ataque y sus consecuencias financieras. Caso: Ataque de Ransomware en una Fintech hipotética

Tabla 4. Datos Generales de la Fintech del escenario hipotético

Característica	**Valor**
Nombre	Fintech Bogotana (préstamos/lending)
Usuarios totales	4.000.000
Usuarios activos	875.000
Saldo promedio por usuario	$120.000 COP ($30 USD)
Fondos en custodia	$480.000.000.000 COP ($120.000.000 USD)
Ingresos mensuales totales	$1.400.000 USD

Margen operativo	25%
Número de empleados	180
Salario promedio diario por empleado	70 USD

Fuente: Elaboración propia

Tabla 5.Desglose de Ingresos Mensuales

Fuente de Ingreso	**Monto (USD)**	**Porcentaje**	**Descripción**	**Base de Cálculo Exacta**
Ingresos por float	$700.000	50,0%	Rendimientos por inversión temporal de saldos de usuarios	$120.000.000 en custodia × 7% anual ÷ 12 meses = $700.000
Comisiones por retiros en cajeros	$150.000	10,7%	Ingresos por retiros en cajeros automáticos	83.333 retiros × $1,80 promedio por retiro = $150.000
Transferencias interbancarias premium	$80.000	5,7%	Comisiones por transferencias especiales o prioritarias	20.000 transf. de alto valor × $3,00 + 10.000 transf. inmediatas × $2,00 = $80.000
Servicios premium	$50.000	3,6%	Servicios financieros adicionales de valor agregado	7.000 suscripciones × $5,00 + 10.000 servicios individuales × $1,50 = $50.000

Marketplace dentro de la aplicación	$120.000	8,6%	Comisiones por ventas en plataforma integrada	$3.000.000 en ventas × 4% comisión promedio = $120.000
Productos financieros de terceros	$110.000	7,9%	Comisiones por venta de productos financieros externos	15.000 seguros × $4,00 + 2.500 créditos × $10,00 + 1.250 inversiones × $20,00 = $110.000
Datos analíticos anonimizados	$40.000	2,9%	Monetización de datos agregados de comportamiento	8 suscripciones corporativas × $4.000 + 4 reportes específicos × $2.000 = $40.000
Otros ingresos operativos	$150.000	10,7%	Ingresos complementarios diversos	Divisas (30.000 × $1,50 = $45.000) + B2B ($35.000) + Cashback ($30.000) + Pagos (40.000 × $1,00 = $40.000) = $150.000
Total	$1.400.000	100%		

Fuente: Elaboración propia

Tabla 6.Características del Ataque de Ransomware

Parámetro	**Valor**
Tipo de ataque	Ransomware (cifrado de servidores principales)
Duración inactividad total	48 horas (2 días)
Duración recuperación parcial	3 días
Capacidad operativa durante recuperación	70%
Monto del rescate	$100.000 USD (no pagado)

Fuente: Elaboración propia

Tabla 7. Impacto Financiero del Ataque

Categoría	**Monto (USD)**	**Base de Cálculo Exacta**
Pérdidas Directas	$135.333	Suma de ingresos perdidos y pérdidas por datos
Pérdidas Indirectas	$2.145.000	Suma de impacto reputacional, fuga clientes, costos legales, multas y seguros
Costos de Mitigación	$405.050	Suma de recuperación sistemas, inversión seguridad, personal y cumplimiento
IMPACTO TOTAL	$2.685.383	Suma de las tres categorías anteriores
Tiempo de recuperación	5 días	Inactividad total (2 días) + Recuperación parcial (3 días)

% de ingresos mensuales	191,8%	Impacto total ÷ Ingresos mensuales ($1.400.000) × 100

Fuente: Elaboración propia

Tabla 8. Desglose de Pérdidas Directas

Componente	**Monto (USD)**	**Base de Cálculo Exacta**
Ingresos perdidos	$135.333	($1.400.000 ÷ 30 días × 2 días) + ($1.400.000 ÷ 30 días × 3 días × (1 - 0,7)) = $93.333 + $42.000 = $135.333
Pérdidas por datos	$0	$0 (No se materializó la filtración de datos en esta simulación)
Total, Pérdidas Directas	$135.333	Suma de los componentes anteriores

Fuente: Elaboración propia

Tabla 9. Desglose de Pérdidas Indirectas

Componente	**Monto (USD)**	**Base de Cálculo Exacta**
Impacto reputacional	$750.000	Tomado de la información suministrada en la tabla 2. Estimación de costos de un ataque cibernético
Fuga de clientes	$1.050.000	Usuarios activos × Tasa de fuga × Valor por cliente = 875.000 × 0,03 × $40 = $1.050.000

Costos legales	$150.000	Tomado de la información suministrada en la tabla 2. Estimación de costos de un ataque cibernético
Multas regulatorias	$0	$0 (No se materializaron en esta simulación)
Aumento en seguros	$195.000	Prima anual × Porcentaje de aumento = $650.000 × 0,3 = $195.000
Total, Pérdidas Indirectas	$2.145.000	Suma de los componentes anteriores

Fuente: Elaboración propia

Tabla 10. Desglose de Costos de Mitigación

Componente	**Monto (USD)**	**Base de Cálculo Exacta**
Recuperación de sistemas	$100.000	Tomado de la información suministrada en la tabla 2. Estimación de costos de un ataque cibernético
Inversión en ciberseguridad	$220.000	Costo fijo de implementación de nuevas medidas de seguridad
Gastos de personal	$85.050	(Empleados × Salario × Días inactividad × 1,5) + (Empleados × Salario × Días recuperación × 1,25) = (180 × $70 × 2 × 1,5) + (180 × $70 × 3 × 1,25) = $37.800 + $47.250 = $85.050
Cumplimiento regulatorio	$0	$0 (No se materializó en esta simulación)

Total, Costos de Mitigación	$405.050	Suma de los componentes anteriores

Fuente: Elaboración propia

Tabla 11. Distribución Recomendada de Inversión en Ciberseguridad (Nivel Intermedio)

Área de Inversión	Porcentaje	Monto (USD)
Sistemas de respaldo y recuperación	30%	$66.000
Soluciones EDR/XDR	25%	$55.000
Monitoreo 24/7 y SOC	20%	$44.000
Capacitación en ciberseguridad	15%	$33.000
Pruebas de penetración regulares	10%	$22.000
Total	**100%**	**$220.000**

Fuente: Elaboración propia basada en la sugerencia del experto en ciberseguridad entrevistado

Tabla 12.Análisis del Margen de Utilidad Neta (NPM)

Concepto	**Valor Calculado**	**Base de Cálculo**	**Interpretación**
Pre-Ataque (15% impuesto)	21,3%	($1.400.000 × 25%) × (1 - 15%) ÷ $1.400.000 × 100%	Rentabilidad normal de la empresa antes del incidente
Post-Ataque Sin Pago	6,2%	[(($1.264.667 × 25%) - ($2.685.383 ÷ 12)) × (1 - 15%)] ÷ $1.264.667 × 100%	Rentabilidad reducida pero positiva al distribuir el impacto en 12 meses

Reducción del margen	15,1 puntos	21,3% - 6,2%	Representa una caída del 70,9% en la rentabilidad de la empresa
Periodo de absorción del impacto	12 meses	Impacto total ÷ 12	Tiempo estimado para distribuir el impacto manteniendo rentabilidad positiva

Fuente: Elaboración propia

El análisis previo resalta la significativa vulnerabilidad financiera de las empresas Fintech de prestamos en Bogotá ante los ciberataques. estos hallazgos indican que un solo incidente de Ransomware puede erosionar gravemente la rentabilidad, reduciendo el margen de utilidad neta del 21.3% al 6.2%, lo que representa una caída del 70.9% en la rentabilidad. Este impacto está impulsado en gran medida por las pérdidas indirectas, en particular la fuga de clientes ($1.050.000) y el daño reputacional ($750.000), que en conjunto representan el 79.9% del impacto total.

Si bien este escenario proporciona una ilustración valiosa de las posibles consecuencias financieras, es importante reconocer ciertas limitaciones. En primer lugar, los supuestos utilizados para calcular componentes clave, como la tasa de fuga de clientes ('Tasa de fuga') del 3% y el impacto reputacional de $750,000, las cuales se basan en la opinión brindada por el experto entrevistado. Asimismo, el período de recuperación estimado, entre otros.

Por último, Dado que el 80% del impacto total proviene de pérdidas indirectas como el daño reputacional y la fuga de clientes, es evidente que la ciberseguridad, cuando se aborda

estratégicamente, representa una inversión de alto rendimiento tanto en la resiliencia financiera como en la construcción de una confianza duradera con los clientes, en lugar de ser simplemente un costo para minimizar."

6.3. Estrategias para minimizar y prevenir los riesgos cibernéticos en las finanzas corporativas

Dado el impacto financiero significativo de los ciberataques en las empresas Fintech de préstamos (lending), como se evidenció en la Sección 6.2, adoptar un enfoque proactivo y estratégico frente a la ciberseguridad no es simplemente una cuestión técnica, sino un elemento central de la gestión del riesgo financiero. Las siguientes estrategias están diseñadas para minimizar los riesgos cibernéticos, proteger los activos financieros y, en última instancia, mejorar la resiliencia financiera y la sostenibilidad a largo plazo de las Fintech en Bogotá. Estas estrategias enfatizan un cambio de paradigma: dejar de ver la ciberseguridad como un centro de costos y reconocerla como una inversión generadora de valor.

6.3.1 Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) orientado a los resultados financieros

Adoptar un SGSI robusto, basado en marcos internacionales como ISO 27001, ISO 27002 y NIST 800-53, es fundamental para establecer una base sólida de ciberseguridad. No obstante, para asegurar su relevancia y efectividad, el SGSI debe estar alineado directamente con los objetivos financieros de la Fintech. Esto implica:

- **Asignación de recursos basada en riesgos:** Implementar una matriz de riesgos (siguiendo ISO 27005 o NIST 800-53B) para priorizar las inversiones en seguridad según el posible impacto financiero de diferentes amenazas cibernéticas. Por ejemplo, asignar más recursos a la protección de sistemas que gestionen transacciones de alto valor o datos sensibles de clientes.
- **Auditorías financieras periódicas de los controles de seguridad:** Evaluar regularmente la eficacia de los controles y detectar áreas donde las inversiones no estén generando los resultados esperados.
- **Documentación del Retorno sobre la Inversión en Seguridad (ROSI):** Rastrear y documentar los beneficios financieros de las inversiones en seguridad, como la reducción de primas de seguros, la evitación de pérdidas por ataques y la mejora en la retención de clientes.
- **Evaluación continua:** Integrar evaluaciones de vulnerabilidades y procesos de Declaración de Aplicabilidad (SoA) para garantizar una alineación constante con las amenazas emergentes y las prioridades del negocio.

6.3.2 Fortalecimiento de la gestión del riesgo financiero mediante la integración de la ciberseguridad

Las metodologías tradicionales de gestión del riesgo financiero deben ampliarse para incorporar explícitamente los riesgos cibernéticos Esto requiere:

- **Cuantificación de la exposición al riesgo cibernético:** Desarrollar métodos que permitan calcular el impacto financiero potencial de los ciberataques en métricas clave como ingresos, rentabilidad y flujo de caja.
- **Planeación de escenarios para la resiliencia financiera:** Realizar simulaciones del impacto financiero de distintos escenarios de ataque cibernético y definir estrategias para mitigar dichos impactos.
- **El ciberseguro como herramienta financiera:** Evaluar opciones de ciberseguros para transferir parte del riesgo financiero asociado a los ataques. Sin embargo, se debe analizar cuidadosamente el alcance, las exclusiones y las condiciones de las pólizas.
- **Metodologías específicas:** Definir el alcance y los objetivos financieros, crear un inventario de hardware, software y versiones utilizadas.
- **Prevención de ataques:** Establecer controles contra ransomware y protocolos estrictos para la realización de transacciones de alto valor.

6.3.3 Monitoreo proactivo y respuesta ante incidentes con enfoque financiero

Un monitoreo efectivo y una respuesta adecuada a incidentes son fundamentales para minimizar el daño financiero de los ciberataques. Esto implica:

- **Monitoreo en tiempo real de transacciones financieras:** Implementar sistemas que vigilen en tiempo real las operaciones financieras para detectar actividades sospechosas que puedan indicar fraudes o ataques.

- **Planes de respuesta a incidentes enfocados en el impacto financiero:** Desarrollar planes que prioricen la protección de activos financieros y la rápida recuperación de las operaciones económicas.
- **Equipo de respuesta financiera ante incidentes:** Establecer un equipo especializado con conocimientos en ciberseguridad y finanzas para gestionar eficazmente los incidentes que afecten las finanzas.
- **Vigilancia activa:** Implementar sistemas de detección de intrusos y monitoreo de transacciones sospechosas.
- **Procedimientos y roles definidos:** Crear procedimientos específicos para incidentes financieros y establecer claramente las responsabilidades del equipo de respuesta.

6.3.4 Prácticas de desarrollo seguro para aplicaciones financieras (OWASP)

Dado que las empresas Fintech dependen en gran medida del software, es esencial aplicar prácticas de desarrollo seguro para prevenir ataques cibernéticos. Esto incluye:

- **Integración del Top 10 de OWASP:** Implementar controles que aborden las 10 vulnerabilidades críticas más comunes en aplicaciones web, con énfasis en aquellas que afectan directamente a las aplicaciones financieras, como inyecciones, fallas de autenticación y scripts maliciosos.
- **Implementación de OWASP SAMM:** Aplicar seguridad desde el diseño del producto tecnológico.

- **Pruebas de seguridad regulares:** Realizar pruebas de penetración y revisiones de código periódicas en las aplicaciones financieras para detectar y corregir vulnerabilidades.
- **Capacitación en codificación segura:** Capacitar a los desarrolladores en prácticas de programación segura para evitar errores desde la fase de desarrollo.

6.3.5 Protección de datos y resiliencia para la información financiera

Proteger los datos financieros es esencial para mantener la confianza del cliente y cumplir con las normativas vigentes. Esto implica:

- **Clasificación y protección de los datos:** Aplicar un esquema de clasificación que identifique y categorice los datos financieros según su sensibilidad y criticidad, y aplicar los controles de seguridad adecuados.
- **Cifrado de datos financieros:** Asegurar los datos tanto en tránsito como en reposo mediante técnicas de cifrado.
- **Respaldos y recuperación de datos:** Implementar una estrategia de respaldo y recuperación sólida, siguiendo la regla 3-2-1 (3 copias, en 2 formatos distintos, 1 fuera de línea).

Al implementar estas estrategias, las Fintech en Bogotá pueden transformar su enfoque de ciberseguridad, pasando de un gasto reactivo a una inversión proactiva que protege sus activos financieros, mejora su ventaja competitiva y construye una relación de confianza duradera con

sus clientes. En última instancia, una postura sólida en ciberseguridad no solo previene ataques, sino que garantiza la salud financiera y la sostenibilidad del sector Fintech a largo plazo. Este análisis y las estrategias propuestas han sido desarrolladas tomando como base, en gran medida, el curso de estrategia de seguridad informática para empresas, impartido por Escalona, R. en Platzi (s.f.)

7. Conclusiones

Los hallazgos de la investigación confirman la creciente amenaza de los ciberataques a las instituciones financieras, especialmente a las empresas Fintech, como se ha destacado en la literatura existente por organismos como el FMI y el Foro Económico Mundial (2025). Se coincide en que el cibercrimen ha aumentado en frecuencia y sofisticación, incluyendo ataques de Ransomware y tácticas mejoradas con IA (como phishing, vishing y deepfakes). lo cual se alinea con los desafíos identificados en el sector Fintech de Bogotá (Rodríguez & Linares, 2021).

Sin embargo, la investigación profundiza en las implicaciones financieras específicas para las Fintech en una economía en desarrollo como lo es la colombiana, un aspecto que no siempre se aborda en detalle en la literatura general sobre ciberseguridad. Adicionalmente se cuantificó el impacto de la pérdida de reputación tras un ataque de Ransomware, mostrando que las pérdidas indirectas (fuga de clientes, daño reputacional) superan las pérdidas directas, lo cual es consistente con la vulnerabilidad del sector financiero a la pérdida de clientes según la Organización de los Estados Americanos (OEA, 2018)

Por otra parte, también se evidencia una brecha importante entre las recomendaciones teóricas y su aplicación práctica en el sector Fintech de Bogotá. A pesar de que marcos internacionales como ISO 27001 y NIST 800-53 ofrecen lineamientos integrales de ciberseguridad, las empresas Fintech enfrentan limitaciones en recursos, regulación y desconocimiento, lo que les impide invertir y adoptar medidas robustas. Además, muchas de estas compañías "perciben los costos en ciberseguridad como un gasto, y no como una inversión estratégica" (Escalona, R., 2025), desconociendo el impacto económico que un ciberataque puede generar.

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

El estudio presenta limitaciones al enfocarse en un único sector durante un periodo específico, pudiendo variar los resultados en otros contextos. La escasez de información financiera sobre costos cibernéticos generó estimaciones potencialmente subjetivas ante la falta de fuentes más robustas para fundamentar premisas y comparar resultados. Se destaca la carencia de análisis sectoriales que aborden estas vulnerabilidades, pues la literatura existente tiende a enfatizar aspectos positivos, descuidando la evaluación crítica de riesgos e implicaciones tanto a nivel individual como sectorial.

La investigación cumplió exitosamente su objetivo inicial al caracterizar los principales riesgos cibernéticos que afectan las finanzas corporativas del sector Fintech bogotano. Mediante un riguroso enfoque metodológico mixto, que combinó revisión bibliográfica exhaustiva y entrevista con especialista en ciberseguridad, se identificaron patrones de vulnerabilidad predominantes, destacando particularmente la filtración de datos y los ataques de denegación de servicio. El análisis reveló deficiencias críticas en los controles organizacionales, especialmente frente a amenazas internas, evidenciando la necesidad urgente de implementar protocolos de seguridad más robustos y proactivos en estas instituciones financieras emergentes.

En segundo lugar, El estudio logró evaluar la magnitud e impacto económico de los riesgos cibernéticos. mediante la simulación de un ataque ransomware, revelando pérdidas financieras sustanciales que afectan directamente la rentabilidad empresarial. Esta modelación cuantitativa permitió visualizar la erosión del margen de utilidad neta, la cual debe interpretarse más como estimación ilustrativa que como medición precisa. La ausencia de datos empíricos específicos sobre el impacto financiero real de ciberataques en empresas Fintech bogotanas constituyó precisamente la justificación para desarrollar este escenario simulado, contribuyendo así a llenar un vacío significativo en la literatura especializada.

Finalmente, se cumplió con el objetivo de proponer estrategias preventivas contra riesgos cibernéticos en las finanzas corporativas, estableciendo un marco integral que transforma la ciberseguridad de gasto reactivo a inversión estratégica. Las medidas propuestas, fueron diseñadas específicamente para fortalecer la resiliencia financiera de las Fintech. Este enfoque multidimensional comprende sistemas de gestión orientados a resultados financieros, mecanismos de cuantificación de exposición al riesgo, protocolos de respuesta a incidentes con perspectiva financiera y metodologías de desarrollo seguro adaptadas al contexto local, destacando la necesidad de soluciones personalizadas y desarrollo de capacidades institucionales.

Esta exploración identifica tres líneas prioritarias para investigaciones futuras. Se requieren urgentemente análisis cuantitativos sobre el retorno de inversión de estrategias de protección digital específicas para las Fintech, superando la dependencia de literatura internacional que no refleja adecuadamente las realidades locales. Asimismo, resulta crucial desarrollar evaluaciones económicas sobre costos de implementar medidas preventivas en los modelos de negocio digitales regionales, información actualmente escasa pero fundamental para decisiones estratégicas informadas. Paralelamente, existe una notable carencia de documentación sistemática sobre casos reales de ciberataques en el ámbito financiero-tecnológico colombiano.

Se recomienda profundizar en dos áreas complementarias de investigación. Primero, analizar la regulación gubernamental y los mecanismos de colaboración interempresarial para la adopción generalizada de estándares de ciberseguridad en el sector Fintech (Mejía & Azar, 2021). Segundo, implementar estudios que evalúen el desempeño financiero a largo plazo de empresas que realizan inversiones estratégicas en ciberseguridad, proporcionando evidencia empírica sobre el valor y retorno económico de estas iniciativas. Estos enfoques permitirán desarrollar marcos metodológicos robustos para identificar patrones de ataque específicos y

diseñar protocolos de respuesta económicamente viables y efectivos para las empresas Fintech bogotanas.

8. Recomendaciones

Esta investigación, si bien proporciona información valiosa sobre el impacto financiero de los riesgos cibernéticos en las empresas Fintech de Bogotá, reconoce ciertas limitaciones en su ejecución. La dependencia de escenarios hipotéticos, aunque necesaria debido a la escasez de datos. Ante la carencia de estudios de casos públicos y documentados sobre el impacto financiero de incidentes cibernéticos, introduce un grado de incertidumbre en los hallazgos. Para mitigar esto, se hizo un esfuerzo por fundamentar los escenarios en parámetros realistas del ecosistema Fintech de Bogotá, incluyendo tamaños típicos de empresas, estructuras de costos predominantes, comportamiento documentado de los clientes y el marco regulatorio financiero colombiano vigente.

Estos escenarios simulados permiten cuantificar de manera ilustrativa las repercusiones económicas que enfrentarían las empresas del sector ante distintos tipos de incidentes. Sin embargo, futuras investigaciones deberían priorizar la recopilación y el análisis de datos del mundo real para validar y refinar estos hallazgos, así como mejorar la recopilación de información para la revisión de expertos. Además, solo se analizó un tipo de ataque, cuando en realidad existen ocasiones en donde el ecosistema enfrenta diversas amenazas cibernéticas al mismo tiempo.

A pesar de estas limitaciones, esta investigación a combinar análisis cuantitativo con conocimientos cualitativos de expertos en ciberseguridad, se ofrece una perspectiva más holística que los enfoques puramente técnicos o financieros. Este enfoque interdisciplinario se alinea con el creciente reconocimiento de la ciberseguridad como un imperativo estratégico para los

negocios, que requiere la colaboración entre expertos técnicos y responsables financieros. En cuanto al impacto financiero de una pérdida de reputación, el sector financiero es el segundo más vulnerable a la pérdida de clientes

Esta exploración subraya la urgente necesidad de continuar estudiando las dimensiones financieras de la ciberseguridad en el sector Fintech. A medida que estas empresas se vuelven cada vez más críticas para la estabilidad financiera y el crecimiento económico de Bogotá y Colombia, es fundamental mejorar la infraestructura y reducir la incidencia de ciberataques en este ámbito. El estudio aporta una comprensión sobre la importancia de corregir la percepción errónea de que la ciberseguridad es un costo adicional en lugar de una inversión estratégica fomentando la cultura de ciberseguridad y en búsqueda de regulación más estricta

Por ello, se invita a la universidad, facultad, programas académicos y colegas a continuar esta investigación, explorando no solo el impacto financiero de los ciberataques, sino también los costos de implementación de una cultura de ciberseguridad empresarial. Estudios financieros sobre elección de seguros cibernéticos los cuales resultarían especialmente valiosos. Tales investigaciones permitirían construir modelos predictivos más robustos, facilitando desarrollar estrategias de mitigación financiera acordes con el panorama contemporáneo, transformando así la protección digital de un gasto reactivo a una inversión estratégica con retorno cuantificable.

Con base en los hallazgos de esta investigación, se recomienda que las empresas Fintech en Bogotá prioricen la implementación de medidas de ciberseguridad robustas y adopten estrategias financieras proactivas. Estas estrategias deben incluir desarrollar mecanismos para cuantificar la exposición al riesgo cibernético e integrar su análisis en la gestión financiera corporativa. Asimismo, establecer equipos de respuesta con enfoque económico, implementar metodologías como OWASP para desarrollar aplicaciones seguras, y considerar la contratación

de ciberseguros, Estas acciones no solo protegerán los activos financieros, sino que también fortalecerán la confianza y fidelización de los clientes y consolidará el sector.

Es fundamental fomentar una cultura de concienciación sobre ciberseguridad entre todos los empleados y actores clave del sector Fintech, promoviendo prácticas responsables y el intercambio de información sobre amenazas y vulnerabilidades emergentes. Esto incluye Implementar un esquema de clasificación de datos para identificar y categorizar la información financiera según su sensibilidad y criticidad, realizar pruebas y auditorías periódicas e Implementar procesos de Declaración de Aplicabilidad.

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

Referencias bibliográficas

Álvarez Flórez, J. A., & Preciado Uribe, D. J. (2021). Evolución del fraude informático: una problemática en las organizaciones bancarias colombianas.

Aljaber, B., & Alrico, A. (2019). Security and privacy in cloud computing: A comprehensive review. Journal of Network and Computer Applications, 126, 193-208. https://doi.org/10.1016/j.jnca.2018.11.005

Aguilar, L. J. (2017). Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguridad 4.0). Cuadernos de estrategia, (185), 19-64.

Asobancaria. (2024). Fortalecimiento institucional para la estabilidad financiera. https://publicaciones.asobancaria.com/wp-content/uploads/Libros/2024/fortalecimiento-institucional-para-la-estabilidad-financiera.pdf

Barrera Rodríguez, A. F., & Narváez Martínez, L. E. (2021). Fintech como fuente de financiación alternativa en Colombia e India.

BID y OEA (2020). Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe. Banco Interamericano de Desarrollo y Organización de Estados Americanos. https://publications.iadb.org/es/reporte-ciberseguridad2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

Black, F., & Scholes, M. (1973). The pricing of options and corporate liabilities. Journal of political economy, 81(3), 637-654.

Bolaño, I. M. (2012). Caracterización de los delitos informáticos en Colombia. Pensamiento Americano, 5(9).

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

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

Clavijo Ramírez, F., Osorio, D., & Yanquen, E. (2017). Recuadro 7: Riesgo cibernético: Relevancia y enfoques para su regulación y supervisión. Banco de la República. Recuperado de https://d1b4gd4m8561gs.cloudfront.net/sites/default/files/publicaciones/archivos/rref_recuadro_7_2017.pdf

Ceballos Rincón, O. I., & Castro Peñaloza, B. S. (2022). ii. Los modelos de negocio fintech y su aplicación a la generación de valor de las pymes.

Centro Nacional de Seguridad Cibernética (NCSC). (2020). Annual review 2020. Recuperado de https://www.ncsc.gov.uk/annual-review/2020

Chen, Y., & Chiu, C. (2020). The effect of cyber security education on individuals' cyber security behavior. Computers & Education, 145, 103561. https://doi.org/10.1016/j.compedu.2020.103561

Chu, C., & Hu, P. J. (2018). The impact of cyber-attacks on organizational reputation and brand trust. Computers & Security, 78, 1-11. https://doi.org/10.1016/j.cose.2018.05.005

CNMC (2018). «Estudio sobre el impacto en la competencia de las nuevas tecnologías en el sector financiero (FINTECH)». E/CNMC/001/18.

Colombia Fintech. (2022). Inversión en la industria Fintech: Actualidad del entorno de negocios. https://colombiafintech.co/static/uploads/BEN-29-11OCT2022.pdf

Escalona, R. (2025). Curso de estrategia de seguridad informática para empresas [Curso en línea]. Platzi. https://platzi.com/home/clases/9441-ciberseguridad-en-empresas/68514-la-experiencia-de-platzi-con-iso27001/

Espinal, J. (2019). Fintech: la revolución de los servicios financieros a través de la tecnología.

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

Espinel Maldonado, D. (2023). Ciberseguridad y ética digital en los servicios financieros FINTECH de la economía digital.

Fernández, C. (2022). Modelos de gestión financiera para inversiones en tecnologías emergentes de ciberseguridad

Finnovista, Banco Interamericano de Desarrollo, y BID Invest (2024). Fintech en América Latina y el Caribe: un ecosistema consolidado con potencial para aportar a la inclusión financiera regional. https://doi.org/10.18235/0013032

Finnovista. (2024). Finnovista Fintech Radar Colombia: VII edición. https://www.finnovista.com/wp-content/uploads/2024/05/RADAR-COLOMBIA-ESPANOL-3.pdf

Foro económico mundial. (2024). Global Cybersecurity Outlook 2024. Accenture. Recuperado de https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

Gómez, E., & Martínez, R. (2022). Transformación digital acelerada post-pandemia: cambios permanentes en el consumo de servicios financieros.

González-Páramo, J. M. (2017). Financial innovation in the digital age: Challenges for regulation and supervision. Revista de estabilidad financiera, 32, 9-37.

Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2024). Sesión I: Competencia, Fintechs y Open Banking – Contribución de España. https://one.oecd.org/document/DAF/COMP/LACCF(2024)4/es/pdf

Hernández, R., & Fernández, C. (2022). Metodología de la investigación aplicada a estudios financieros digitales. Editorial McGraw-Hill.

Hull, J. C. (2015). Risk management and financial institutions. National Bureau of Economic Research.

Análisis de los principales riesgos en las finanzas corporativas ante los ataques cibernéticos en las empresas Fintech de Bogotá

Jiménez Cardozo, M. S., Morales Maya, L., Robledo Gómez, D., & Velandia Vargas, J. J. (2024). Transformación digital: la experiencia del usuario en el sector financiero (Bachelor's thesis, Especialización en Gerencia de Proyectos).

Jiménez, S. R. G., & Banda-Ortiz, H. (2021). Impacto en el precio de las acciones de los bancos debido al ataque cibernético al SPEI. Panorama Económico, 16(33), 119-136.

Kim, H., & Shin, D. (2018). An analysis of malware propagation in computer networks. Computers & Security, 74, 47-58. https://doi.org/10.1016/j.cose.2017.11.002

KPMG. (2022). Pulse of Fintech H2'21: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2022/02/pulse-of-fintech-h2-21.pdf

Liang, H, Lin, C., & Hsiao, H. (2019). A comprehensive study of mobile device security: Threats, solutions, and future directions. Information Management & Computer Security, 27(2), 194-209. https://doi.org/10.1108/IMCS-02-2018-0026

López Rodríguez, C. E., De la Hoz Solano, V. M., & Becerra Rozo, C. A. (2022). Financial risks in the operation of special service transportation in the hotel sector in Bogota, Colombia. *Financial Management*, *4061*, 2979.

López Llorente, S. (2022). Ecosistema fintech en Colombia.

Martínez, J., & Ochoa, P. (2023). Evaluación de riesgos cibernéticos en instituciones financieras emergentes: Un enfoque metodológico para Latinoamérica. Innovación Digital y Finanzas, 12(3), 87-102.

Mejía, D., & Azar, K. (2021). Políticas de inclusión financiera y las nuevas tecnologías en América Latina (Serie: Iniciativas para la recuperación en la pospandemia, Documento de políticas para el desarrollo No. 6). Corporación Andina de Fomento (CAF). https://scioteca.caf.com/bitstream/handle/123456789/1755/Pol%C3%ADticas%20de%20inclusi

%C3%B3n%20financiera%20y%20las%20nuevas%20tecnolog%C3%ADas%20en%20Am%C3%A9rica%20Latina.pdf?sequence=4&isAllowed=y

Ocampo., & Santa Catarina. (2017). Fintech: tecnología financiera. Oficina de Información Científica y Tecnológica para el Congreso de la Unión, 6.

Organización de los Estados Americanos (OEA) (2018). Estado de la ciberseguridad en el sector bancario en América Latina y el Caribe. Recuperado de https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

Ramírez, L., & Contreras, . (2023). Modelos predictivos de amenazas cibernéticas en entornos financieros digitales. Revista de Seguridad Informática y Finanzas, 15(2), 210-227.

Ramírez, C. (2021). Adopción de tecnologías financieras durante la crisis sanitaria: análisis del crecimiento en América Latina.

Ramírez, F. C., Osorio, D., & Yanquen, E. 1. (2017) ¿Qué es el riesgo cibernético y por qué es relevante para la estabilidad financiera?.

Rodríguez, C. E. L., & Linares, J. K. C. (2021). Propuesta para la disminución del riesgo en el otorgamiento de crédito: Un estudio de caso en el sector salud colombiano. *Cooperativismo & Desarrollo*, *29*(121), 57-88.

Rodríguez, C. E. L., & Rodríguez, M. A. E. (2021). Riesgo operacional: comportamiento de sus factores en el sector bancario de Bogotá Colombia. *Revista Venezolana de Gerencia: RVG*, *26*(6), 439-456.

Rubaceti, N. A. B., Giraldo, S. R., & Sepúlveda, M. Z. (2022). Una revisión bibliográfica del Fintech y sus principales subáreas de estudio. Economicas Cuc, 43(1), 83-100.

Sánchez, C., & López, R. (2023). Adaptación de estándares internacionales de ciberseguridad al sector financiero colombiano. Cuadernos de Ciberseguridad y Economía Digital, 7(4), 113-129.

Sun, Z., Chen, W., & Wang, Q. (2018). The security risks of mobile devices in the workplace. Journal of Business Continuity & Emergency Planning, 12(2), 121-129. https://doi.org/10.1108/JBCEP-03-2017-0026

Velandia-Pacheco, G. J., & Escobar-Castillo, A. E. (2019). Investigación en auditoría forense: Revisión de publicaciones SCOPUS 1976-2018. Revista Criminalidad, 61(3), 279-298.

Wlodarczyk, A. (2018). Cybersecurity risks in small and medium-sized enterprises. Journal of Entrepreneurship, Management and Innovation, 14(2), 7-17. https://doi.org/10.7341/20181427

Zhang, L., Lu, Y., & Gao, L. (2017). Phishing attacks and prevention techniques: A review. Journal of Network and Computer Applications, 93, 81-93. https://doi.org/10.1016/j.jnca.2017.03.008

Zhou, Y., & Lu, L. (2019). Understanding cyber security threat and defense mechanisms. Future Generation Computer Systems, 96, 464-476. https://doi.org/10.1016/j.future.2019.06.009