RIESGOS Y VULNERABILIDADES INFORMÁTICAS EN EL USO DEL FINTECH COMO INNOVACIÓN EN SERVICIOS FINANCIEROS DE LA ECONOMÍA DIGITAL COLOMBIANA

JESSICA PAOLA AMADO DIAZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
AÑO 2021

RIESGOS Y VULNERABILIDADES INFORMÁTICAS EN EL USO DEL FINTECH COMO INNOVACIÓN EN SERVICIOS FINANCIEROS DE LA ECONOMÍA DIGITAL COLOMBIANA

JESSICA PAOLA AMADO DIAZ

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

YENNY STELLA NUÑEZ
Directora de Trabajo de grado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C
AÑO 2021

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá, Fecha sustentación

DEDICATORIA

A la Universidad Nacional Abierta y a Distancia y a sus Maestros por siempre querer mostrarnos de una forma dinámica, innovadora y objetiva las nuevas perspectivas con las que podemos enfocar nuestra formación permanente a nivel profesional, ya que esto le agrega gran valor a mi carrera haciéndome una persona más crítica y con un alto nivel estratégico.

AGRADECIMIENTOS

A mi familia, por su constante apoyo incondicional y motivación para acrecentar mi formación profesional. A los docentes que han sido un soporte constante en cada uno de mis procesos de aprendizaje, quienes me han motivado a ser mejor persona y profesional.

TABLA DE CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

AMENAZA

Las amenazas siempre existen y son aquellas acciones que pueden ocasionar consecuencias negativas en la operativa de la empresa. Comúnmente se indican como amenazas a las fallas, a los ingresos no autorizados, a los virus, uso inadecuado de software, los desastres ambientales como terremotos o inundaciones, accesos no autorizados, facilidad de acceso a las instalaciones. [1]

ATAQUE

El ataque es un intento organizado e intencionado causado por una o más personas para causar daño o problemas a un sistema informático o red[2].

FINTECH

Estas son un dominio de actividad en el cual las empresas tecnológicas utilizan las tecnologías de la información y la comunicación para crear y/u ofrecer servicios financieros de forma más eficaz y menos costosa.

RIESGO

El riesgo es la probabilidad de que una amenaza se convierta en un desastre. La vulnerabilidad o la amenaza, por separado no representan un peligro, pero si se juntan, se convierten en un riesgo, o sea, en la probabilidad de que ocurra un desastre. [3]

SEGURIDAD DE LA INFORMACIÓN

Es más que un problema de seguridad de datos en los computadores; debe estar básicamente orientado a proteger la propiedad intelectual y la información importante de las organizaciones y de las personas[4].

---

[1] CARRASQUEL, Dórela. Diagnóstico y prevención de vulnerabilidades en redes de datos. [en línea]. 2017. Disponible en: https://carrmen.jimdo.com/riesgo-informatico

[2] EcuRed. Ataque Informático. [en línea]. Cuba. 2017. Disponible en: https://www.ecured.cu/Ataque_informático

[3] Unisdr. El riesgo. 2017. 9 p. Disponible en: https://www.unisdr.org/2004/campaign/booklet-spa/page9-spa.pdf)

[4] TARAZONA, Cesar. Amenazas informáticas y seguridad de la información. [en línea]. 137 p. Disponible en: https://revistas.uexternado.edu.co/index.php/derpen/article/view/965/915

VULNERABILIDAD

Son una debilidad en la tecnología, o en los procesos relacionados con la información, y como tal, se consideran características propias de los sistemas de información, o de la infraestructura que las contiene[5].

STARTUP

Una Startup es una organización humana con gran capacidad de cambio, que desarrolla productos o servicios, de gran innovación, altamente deseados o requeridos por el mercado, donde su diseño y comercialización están orientados completamente al cliente. Esta estructura suele operar con costos mínimos, pero obtiene ganancias que crecen exponencialmente, mantiene una comunicación continua y abierta con los clientes, y se orienta a la masificación de las ventas.

BLOCKCHAIN

Es una base de datos distribuida donde cada nodo o usuario en la red ejecuta y registra transacciones agrupándolas en forma de bloques.

[5] TARAZONA. Op Cit, Pág. 137

RESUMEN

Este trabajo presenta los riesgos y vulnerabilidades informáticas de las Fintech en el sector financiero, mostrando como la seguridad para la gestión del riesgo bajo este esquema Fintech, busca incursionar de forma segura en los modelos financieros, bajo un esquema de computación en la nube. Las Fintech se convierten para el sector financiero en una oportunidad para mejorar los servicios, de forma acorde con el mercado actual, garantizando la seguridad, disponibilidad e integridad de la información de los clientes.

Se explican las Fintech desde su tecnología, infraestructura, seguridad de la información y operatividad, se presentan definiciones dadas al término Fintech tanto de autores académicos como del sector empresarial, también se analiza como las Fintech revolucionaron la industria financiera tradicional y el impacto positivo que género, además, se exponen algunas clasificaciones dadas a estas empresas con el fin de proponer una estrategia metodológica que proporcione los lineamientos de seguridad que mejore constantemente el entorno digital.

Palabras Clave: Fintech, sistema financiero, vulnerabilidades, riesgo, seguridad de la información, economía digital.

ABSTRACT

This paper presents the risks and computer vulnerabilities of Fintech companies in the financial sector, showing how security for risk management under this Fintech scheme seeks to safely enter financial models, under a cloud computing scheme. Fintech companies become an opportunity for the financial sector to improve services, in accordance with the current market, guaranteeing the security, availability and integrity of customer information.

Fintech is explained from its technology, infrastructure, information security and operability, definitions given to the term Fintech are presented by both academic authors and the business sector, it is also analyzed how Fintech revolutionized the traditional financial industry and the positive impact it has. In addition, some classifications given to these companies are exposed in order to propose a methodological strategy that provides security guidelines that constantly improve the digital environment.

Keywords: Fintech, financial system, vulnerabilities, risk, information security, digital economy.

INTRODUCCIÓN

Las Fintech representan hoy una alternativa en el entorno de las finanzas, generando una gran demanda digital en cuanto a la cantidad de clientes que hacen uso de ellas. Pero el principal reto está, en que puedan coexistir dentro de un ecosistema que les permita la integración y colaboración con las instituciones tradicionales haciéndolas sostenibles en el tiempo. Las Fintech ofrecen soluciones financieras propiciadas por la tecnología, y en palabras de Chishti y Barberis[6], este ecosistema hace que la industria crezca a un ritmo acelerado, pues son muchos los servicios a los que se puede acceder, gracias a las aplicaciones o plataformas digitales que proporciona.

La relevancia que están teniendo las Fintech en el sector financiero y el rápido crecimiento de las mismas, es lo que nos lleva a estudiar más detalladamente cómo funcionan y en qué medida pueden cambiar el mundo financiero, por ello este trabajo permite un análisis del estado actual de la ciberseguridad del modelo Fintech usado en el sistema financiero colombiano.

En la primera parte se explica la tecnología utilizada por las Fintech su infraestructura, la seguridad de la información, su operatividad, y la forma como este proceso disruptivo ha generado nuevas formas de interacción con las entidades financieras, con una actitud innovadora en ámbitos estratégicos como la experiencia del cliente y con un enfoque sobre los productos, mostrando nuevas formas de trabajar, una transformación digital con nuevos modelos de negocios bajo la regulación de las autoridades competentes.

Al comparar el modelo financiero tradicional con las Fintech, se muestra como estas lo han puesto contra la pared, obligándolo a adaptarse a estas nuevas tecnologías para ofrecer servicios financieros innovadores. Además, de que como organización tiene la misión de proteger la información de los usuarios con una buena gestión del riesgo, pues las Fintech ofrecen nuevas posibilidades a las personas, consolidando políticas de operación y comportamiento que otorgan una mayor seguridad.

Por último, se propone la metodología Magerit, la cual, proporciona los lineamientos para minimizar considerablemente el riesgo de que la información de los usuarios se vea afectada debido a la ocurrencia de un evento que comprometa la confidencialidad, disponibilidad e integridad, mediante la implementación de una metodología de gestión del riesgo se podrá controlar y evitar eventos que comprometan la integridad de la organización.

[6] CHISHTI, Susane y BARBERIS, Janos. El Futuro es Fintech, Una guía para inversores, emprendedores y visionarios para entender la nueva revolución tecnológica. USSA. 2016. Taurus. 213 p.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Las Fintech 1.0, (1886- 1967) se habló entonces de una infraestructura; esta es una era en la que podemos empezar a hablar de globalización financiera. Comenzó con tecnologías como el telégrafo, así como ferrocarriles y barcos de vapor que permitieron por primera vez una rápida transmisión de información financiera a través de las fronteras. Además, la década de 1950 nos trajo tarjetas de crédito para aliviar la carga de llevar efectivo. Primero, Diner‘s Club presentó el suyo en 1950, American Express Company lo siguió con su propia tarjeta de crédito en 1958.[7].

Fintech 2.0 (1967- 2008) Este período marca el cambio de lo analógico a lo digital y está liderado por instituciones financieras tradicionales. Fue el lanzamiento de la primera calculadora de mano y el primer cajero automático instalado por el banco[8]. Esto significo entonces, que en la década de 1980 se introdujo la banca en línea, que tuvo su florecer en los 90 con el internet y el comercio electrónico.

Fintech 3.0 (actualidad), la crisis financiera del 2008 permitió un cambio de mentalidad del cliente minorista, reconociendo quien es el que tiene los recursos y la legitimidad para brindar servicios financieros, generando una crisis de reputación en la banca tradicional.
La combinación de una serie de cuatro factores sobrevenidos como consecuencia de dicha crisis constituyó la tormenta perfecta que está permitiendo la transformación radical que vive el sector financiero en la actualidad: Cambio en la percepción sobre la banca tradicional, Transformación del marco regulatorio, Necesidad de los legisladores de atender a las demandas políticas y las Condiciones económicas[9].

Lo anteriormente mencionado, hizo que los bancos invirtieran en nuevas tecnologías que les permitieran implementar nuevos métodos mejorando los sistemas ya existentes. Hablamos de la industria Fintech que sugiere según Herrera y Vadillo[10] una interacción virtual entre productores y consumidores que son quienes generan valor a través de la tecnología digital, sin excluir la posibilidad de la interacción física entre ellos. Por otra parte, Singapurwoko[11] manifiesta que la industria Fintech tiene múltiples facetas como los préstamos de igual a igual, los

[7] ORTIZ, Ángel Eulises. Historia de las Fintech, origen, evolución. [en línea]. HostDimeBlog. 2020. Disponible en: https://blog.hostdime.com.co/historia-de-las-fintechorigen-evolucion/
[8] ORTIZ, Op cit.
[9] RAMIREZ, Javier. Retos regulatorios de las Fintech 3.0, en busca del equilibrio entre estabilidad, innovación y competitividad. 2009. 21 p.
[10] HERREA, Diego y Vadillo Sonia. Sandbox regulatorio América Latina e Caribe para o ecosistema FinTech e o sistema financiero. 2018. 7 p.
[11] SINGAPURWOKO, A.. Do Financial Technology Startups Disrupt Business and Performance of Financial Institutions in indonesia? International Journal of Business & Management Science, 9, 2019. 67-81 p.

servicios de pago con dispositivos móviles crowdfunding, sistemas de comercio en línea y aprovisionamientos de mercado. Por su parte, Vasiljeva y Lukanova[12] definen la industria Fintech como una industria que se orienta para adaptarse a prestar servicios financieros a privados e industrias, con el objetivo de proveer al cliente soluciones eficientes y a los precios más bajos, asegurados por la innovación y la tecnología.

La banca comercial tradicional ha venido tras la crisis financiera perdiendo la confianza de sus clientes, especialmente por la falta de transparencia. Es aquí donde las empresas Fintech han sido la alternativa financiera que no solo ha arreglado el nivel de desconfianza sino, que, los ha preparado para el cambio que supone, pues da mayor agilidad en los tramites, mayor accesibilidad a los servicios y la transparencia, estas han sido las ventajas que, condicionadas con el uso de la tecnología, se han convertido en el medio exclusivo para intermediar con las Fintech. Pues unas de las grandes ventajas que tienen las Fintech es la capacidad de adaptarse a las necesidades de los clientes logrando una gran fidelización, pues al conocer más a fondo a cada cliente, es más probable que se encuentren y ofrezcan a los consumidores los productos exactos que necesitan, cuando los necesitan. Por otro lado, los datos de la tecnología Fintech proporciona a las instituciones financieras una visión más clara de lo que hacen sus clientes con su dinero. Además, el poder de la nube que tienen este tipo de empresas. La tecnología Fintech ha sacado partido de esta herramienta para ofrecer productos y servicios financieros específicos para sus clientes en tiempo real.

Por ello, es de anotar que como consecuencia de estos cambios tecnológicos que suceden a gran escala en la actualidad, el sector empresarial y financiero está sometido a riesgos que amenazan su información, debido justamente al crecimiento de hackers, programas maliciosos e incluso usuarios internos considerados peligrosos, que afectan directamente a la información que se transmite a través de las redes informáticas de las mismas. Entonces, la gestión de riesgo se convierte en la filosofía para las empresas Fintech, pues sin estas los servicios que prestan dejan de ser seguros, sustentables y estables. Por ello cuando se toma en cuenta este factor, se valora como una responsabilidad social, con transparencia y calidad, pues quien sale beneficiado es el usuario. Además, cuando una empresa se expone a vulneraciones de identidad, robo de datos, es aquí donde el usuario demanda profesionalismo, conocimiento, transparencia y seguridad, pues la Fintech es una empresa moderna y en fase de crecimiento, que tu empresa sea vulnerable e insegura afecta, también, la reputación general de la industria Fintech y pone en tela de juicio su capacidad de soportar la economía digital y móvil.

Uno de estos cambios ha sido el crecimiento de las Fintech y de la forma tan acelerada que han ido cobrando más fuerza; una señal clara de este crecimiento es

[12] VASILLEJA, Tatjana y LUKANOVA Kristina. Commercial Banks and Fintech Companies in the Digital Transformation: Challenges for the Future". Journal of Business Management, vol. 11. 2016. 25-33 p.

que la inversión global en empresas Fintech pasó de 4.050 millones de dólares, en 2013, a 12.200 millones, en 2014, y a 22.000 millones, en 2015.[13]

Además, también hay que tener en cuenta otro factor importante: la seguridad de la información. Víctor González[14], experto en Ciberseguridad, destacó que las Fintech son empresas altamente vulnerables debido al uso intensivo de tecnología y datos. El experto considera que es indispensable que se encuentren apoyadas por una sólida estrategia de ciberseguridad. El uso intensivo de la tecnología conlleva sus propios riesgos y al combinarse con modelos de negocio financieros surgen riesgos adicionales, siendo los principales la comisión de delitos y fraudes cibernéticos, y las áreas grises de operación que aún no cuentan con regulaciones establecidas para su control.

El sector Fintech, por tanto, enfrenta una paradoja mientras más estricto es el modelo de ciberseguridad, menos optimizado se vuelve el modelo de negocio, por ello es vital la confianza de los usuarios en las herramientas de las que hace uso el sector empresarial.

1.2 FORMULACIÓN DEL PROBLEMA

¿Qué tipos de riesgos y vulnerabilidades financiera genera utilizar las Fintech en el sector empresarial?

[13] SKAN, Dickerson y MASOOD. Fintech, Regtech y la importancia de la ciberseguridad. 2014. 38 p.
[14] GONZALES, Victor. La ciberseguridad. [en linea]. España. 2018. Disponible en https://es.linkedin.com/in/victorjgonzalezarcos

2 JUSTIFICACIÓN

Esta investigación, plantea el problema de seguridad que enfrentan aquellas entidades financieras que implementan tecnología innovadora a la hora de ofrecer sus servicios y productos, las Fintech han revolucionado notablemente y su uso de igual manera.

Por ello, aquellos países que han favorecido la inclusión financiera también han evidenciado obstáculos relacionados con la seguridad digital en el sector bancario, convirtiéndose este en un elemento indispensable a tener en cuenta en relación con la innovación financiera.

Lo anteriormente dicho hace, que, los temas de ciberseguridad sean muy importantes para las empresas, ya que, los clientes son quienes no ven al entorno digital como un espacio confiable y seguro a la hora de realizar sus trámites, esta desconfianza entonces afecta el uso de dichos canales digitales perturbando el impacto positivo esperado. Además, la globalización ha traído consigo una especial acentuación en el sector financiero, permitiendo un contexto donde los criminales cibernéticos se encuentran con condiciones atractivas para hacer uso sofisticado de recurso que ponen en alto riesgo el dinero y por tanto la información de los agentes económicos.
Entonces las entidades financieras afrontan un gran reto: diseñar un modelo de seguridad en la nube que garantice la autenticidad y salvaguarda de la información de sus usuarios, así como de sus productos y servicios, bajo esquemas más agiles como son los despliegues en la nube. Por ello, se plantea la metodología Magerit que actualiza cada uno de sus componentes, llegando a renovar cada uno de los programas, permitiendo crear nuevos sistemas de información a la vanguardia de la tecnología, logrando trabajar un proceso de planificación para establecer las debilidades internas, evitando que la información sea desviada o manipulada.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Analizar el estado actual de la ciberseguridad del modelo Fintech usado en el sistema financiero colombiano

3.2 OBJETIVOS ESPECÍFICOS

- ✓ Explicar las Fintech desde su tecnología, infraestructura, la seguridad de la información y su operatividad como nuevo mecanismo de negocio en el sector financiero.

- ✓ Comparar el modelo financiero tradicional y las Fintech en relación con el control de los riesgos financieros e informáticos dentro de una tendencia de innovación, desarrollo y validación de nuevos modelos de negocio.

- ✓ Proponer una estrategia que proporcione lineamientos de seguridad que contribuya en la mejora de un entorno digital a partir de la confidencialidad, disponibilidad e integridad de la información en el sistema financiero colombiano.

4 MARCO REFERENCIAL

Como primera instancia esta monografía busca hacer un análisis en los procesos de gestión de riesgo las vulnerabilidades informáticas a las que está expuesta la economía digital, al aplicar los modelos Fintech en el sector empresarial, que garanticen la seguridad de la información de los clientes, desde un enfoque teórico y conceptual.

4.1 MARCO TEÓRICO

4.1.1 Historia de la Fintech

La primera entidad de normalización a nivel mundial fue la BSI (British Standards Institution), responsable de publicaciones como la BS 5750 en 1979 (ahora ISO 9001) o BS 7750 de 1992 (ahora ISO 14001), así la norma BS 7799 de BSI da a luz en 1995[15]y su objetivo fue difundir un conjunto de buenas prácticas para la gestión de la seguridad de la información. Luego de varios años de modificaciones, adiciones y evolución en el tema, se llega al estándar ISO/IEC 27001, que fue aprobado y publicado como estándar internacional en octubre de 2005.
La aplicación de la norma permite disminuir posibles riesgos de vulnerabilidades en los sistemas informáticos y en la información general manejada por el personal de una empresa, además de mejorar los servicios prestados, teniendo una mejor organización en los procesos aumentando la competitividad de la empresa ya que salvaguarda la información de los usuarios.

Según Barberis y Buckley.[16], señalan en un nivel más amplio que Fintech se refiere a soluciones financieras basadas en tecnología. Asimismo, aportan tres hechos a la historia de Fintech. La primera es que Fintech no es un desarrollo nuevo en la industria de servicios financieros en términos de los vínculos que han existido entre las finanzas y la tecnología a lo largo de la historia. En segundo lugar, señalan que el sector de servicios financieros es un gran consumidor de productos y servicios de TI en todo el mundo y que estos modelos comerciales no son una tendencia reciente. Y finalmente, el autor sugiere que el término Fintech engloba todos los productos y servicios que ofrecen las industrias tradicionales del sector financiero. Es decir, no se limita a un sector en particular.

[15] LÓPEZ NEIRA, Agustín y RUIZ SPOHR, Javier. El portal de ISSO 27001. [en línea]. 2013. Disponible en: https://www.iso27000.es/index.html
[16] ARNER, Duglas; BARBERIS, Janos y BUCKLEY, Roos.The Evolution of Fintech: A New Post- Crisis Paradigm?. 2015. 37 p.

Arner[17] dijo que la interrelación entre los servicios financieros y la tecnología de la información tiene una larga historia y ha evolucionado durante tres períodos diferentes para demostrar esta evolución y ha construido una línea de tiempo.

Tabla 1. Línea de tiempo

FECHA	1866-1967	1967-2008	2008-Presente	
Era	Fintech 1.0	Fintech 2.0	Fintech 3.0	Fintech 3.5
Geografía	Global/Desarrollado	Global/Desarrollado	Desarrollado	Emergentes/Desarrollado
Elemento clave	Infraestructura/ Computarización	Tradicional-Internet	Mobil-Starups -Nuevos participants	
Cambio de origen	Enlaces	Digitalización	Crisis Financiera 2008/Smartphone	Ventaja Competitiva (Tecnologia)

Fuente: Datos obtenidos de Arner. 2016. 7 p.

La evolución de este concepto o modelo económico es parte de una transformación digital, con miles de startups y el sector FinTech cuestionando todos los productos y servicios que los bancos pueden ofrecer. Este nuevo sistema cambiará por completo la visión del sistema bancario tradicional.

Según Noya[18], las empresas de tecnología financiera han utilizado con éxito estrategias de innovación como una herramienta para desarrollar productos bancarios más centrados en el usuario a menor costo, mejor experiencia del cliente y mejor experiencia del cliente. Según el autor, su propuesta de valor se centra en mejorar las promesas en comparación con los productos y servicios bancarios tradicionales.

La aparición de estas empresas es el resultado de una rápida innovación en los servicios financieros[19]. Hay varias razones para esto. En segundo lugar, el sistema bancario tradicional es incómodo y carece de nueva tecnología para satisfacer las necesidades de acceso a la información de la nueva generación (millennials) y, al final, lo único que se ocupa es la digitalización. Es decir, el rápido desarrollo y digitalización de los teléfonos móviles en todos los procesos de la empresa.

[17] ARNER, Duglas. FinTech: Evolution and Regulation. Asian Institute of International Financial Law University of Hong. 2016. Kong. 45 p.
[18] NOYA, ELoi. ¿Es el Fintech el mayor desafío que afronta la banca? 2016. 4 p. Disponible en: https://www.harvard-deusto.com/es-el-fintech-el-mayor-desafio-que-afronta-la-banca
[19] NOYA. Op Cit. 5 p.

4.1.2 La Gestión del riesgo

Para Hernández Diaz[20], la identificación de riesgos y el análisis exclusivo son las principales tareas de la empresa. La gestión de riesgos está vinculada a la planificación estratégica. La identificación de riesgos debe realizarse al menos una vez al año mediante el análisis de las discusiones (externas e internas) como parte de una fase del ciclo de planificación estratégica.

Por otra parte, para COSO[21] la gestión de riesgos y sus requisitos son una nueva tendencia para muchas empresas que enfrentan el desafío de comprender y gestionar la gestión de riesgos desde una nueva perspectiva. En grandes industrias como el transporte marítimo, la aviación y el turismo, la gestión de riesgos se repite, es gestionada por antepasados y, a menudo, tiene sus propios procedimientos. Sin embargo, para las PYMES, desde la década de 1990, las normas de control interno se han emitido a partir de informes y la gestión de riesgos se ha vuelto importante.

Leiva Yelandy[22], manifiesta que gestión de riesgos es practicada desde hace varios milenios atrás, sin embargo, la popularización del término tuvo sus inicios en la década del 90 del siglo XX y conceptualmente se denomina: “como las actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo. De igual forma el proceso de gestión de riesgos tiene un carácter sistémico respecto a políticas, procedimientos y prácticas de gestión, comunicación, consulta, establecimiento del contexto, e identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo.

4.1.3 Vulnerabilidades en la red

Las vulnerabilidades son por lo general fallos de diseño de procedimientos o de recursos, las vulnerabilidades existen no se fabrican, una vulnerabilidad es cualquier fallo de diseño que permite que una amenaza pueda afectar a un recurso. Si se habla de recursos informáticos se suele decir que una vulnerabilidad es un fallo de diseño de un sistema, un sistema no actualizado o un sistema mal Configurado que permite que un agente externo, acceda sin permisos apropiados al recurso o información que dicho sistema gestiona, en función del tipo de recurso al que estemos orientados existen distintas fuentes de información dónde se puede buscar vulnerabilidades aplicables a los sistemas con que se cuenta.

[20] HERNÁNDEZ DÍAZ, N, LEYVA, Yelandy M y GARCÍA, Cuza, B. Mapas cognitivos difusos para la selección de proyectos de tecnologías de la Información. México: División de Investigación de la facultad de contaduría y administración de la UNAM. Contaduría y Administración. 2013. 95-117 p.

[21] GONZALES MARTINEZ, Rafael. Committee of Sponsoring Organizations. Marco Integrado de control interno. Consejo Nacional de Política Económica y Social. 2019. 19 p.

[22] HERNÁNDEZ. Op Cit. 8 p.

La vulnerabilidad no solo pone en riesgo la integridad de la aplicación, sino que también pone en riesgo todos los datos que son previamente almacenados por los usuarios que navegan en la aplicación.

Este ataque lo realizan para poder modificar, falsificar identidades, y obtener información valiosa de los usuarios que ya se encuentran registrados en alguna aplicación, también lo hacen para borrar las bases de datos o cambiar los diferentes nombres de las tablas que ya están debidamente creadas. Esto se debe al mal desarrollo de una aplicación porque no tiene precaución con las validaciones y dejan todo expuesto.

4.1.4 TIPOS DE VULNERABILIDADES EN LA RED

4.1.4.1 Vulnerabilidad por Injection

Para saber si un sitio web presenta este tipo de vulnerabilidad se debe primero que todo evaluar con una prueba y es agregando un apostrofe luego del id en la URL de la página donde nos encontramos, si este mismo responde con error en la consulta de base de datos nos indica que si es vulnerable como tal el sitio, ejemplo:

com/amado.php?id=10’

Para saber si es vulnerable también se puede inyectar código en la URL de la siguiente manera:

com/amado.php?id=10 order by 5

4.1.4.2 Vulnerabilidad BROKEN AUTHENTICATION

Esta vulnerabilidad lo que hace es que el atacante pueda capturar como tal las credenciales de los usuarios, también evade los mecanismos de autenticación para poder tener el acceso a la aplicación, con el fin de poder robar la información, esto sucede cuando no se tiene una correcta programación en los sistemas porque no implementan el cierre de sesión automático y tienen una mala gestión de autenticación, también porque no tienen las respectivas validaciones que se requieren y por ese motivo son vulnerables a los atacantes.
Este tipo de ataque permite las contraseñas predeterminadas, utiliza como tales procesos donde recupera las credenciales débiles, es una vulnerabilidad donde expone ID de sesión en la URL entonces reescritura la URL y no valida como tal correctamente los ID de sesión, cuando ya se tiene validaciones de token de autenticación lo que hace es que no los valide durante el cierre de sesión.

4.1.4.3 Vulnerabilidad BROKEN ACCESS CONTROL

Esta vulnerabilidad lo que hace es que impone una política donde los usuarios no pueden actuar fuera de sus permisos previstos, entonces estas fallas lo que hacen es que destruyen todos los datos o realizan una función comercial sin autorización, como tal lo que hace es permitir que la clave principal se cambie a otra persona y así pueda editar la cuenta de otra persona, actúa como usuario sin haber iniciado como tal sesión o de igual manera como administrador.

Cómo descubrir que la página web está siendo vulnerada por Broken Access Control, para saber si es vulnerada lo primero es navegar como tal por el sitio web y registrar todas las páginas visitadas, luego se debe cerrar sesión y de nuevo volver a visitar todas las páginas, entonces si el contenido como tal que solo estaba disponible para los usuarios que estaban como tal registrados sigue apareciendo entonces este sitio es vulnerable.
También la página es vulnerada si se aplica fuerza bruta como tal a diferentes rutas, por decir /admin, /settings que solo se pueda visitar un administrador, si un usuario puede ingresar a estas rutas entonces es vulnerable como tal[23].

Herramienta de Injection

La herramienta que se puede utilizar para evitar este tipo de vulnerabilidades es:

•**SQLMap[24]:** esta herramienta es enfocada en ayudar a optimizar como tal la seguridad informática, está desarrollada en Python lo que hace es que las vulnerabilidades en las aplicaciones web sean detectadas por esta herramienta lo que hace es permitirle al usuario que pueda elegir las opciones, como lo es poder tener privilegios en las bases de datos y así ejecutar su SQL SELECT.
Características de SQLMap:

Tiene un soporte completo con las bases de datos relacionales, de igual manera también identifica Microsoft Access, Sybase entre otros.
Da un soporte completo para las dos técnicas de SQL, Blind Injection y Inband SQL Injection.
Evitar ataques con Injection

a. Escapar de los caracteres especiales: Se recomienda escapar de las comillas dobles, sencillas en las consultas SQL, ya que son caracteres considerados

[24] DRAGONJAR, SQLMap. Herramienta Automática de Inyección SQL. [en línea]. Disponible en: https://www.dragonjar.org/sqlmap-herramienta-automatica-de-inyeccion-sql.xhtml

peligrosos que los usan durante los ataques, hay funciones que nos ayudan a evitar estos caracteres como lo es con PHP con mysql_real_scape_string(), permite tomar como tal una cadena y la modifica de tal manera que se evite utilizar estos caracteres.

b. Delimitar valores de las consultas: Se recomienda que así la consulta tenga un numero entero es recomendable usarlos entre comillas simples de tal manera que quede string de esta manera evita la Injection de código SQL

SELECT tipo FROM electrodomésticos WHERE id = ‘1’

c. Verificar los datos que inserta el usuario: Se recomienda que cuando se esté realizando una aplicación se agreguen funciones donde validen correctamente lo que se quiere guardar, si el usuario va a guardar un nombre lo que se quiere es validar que solo sean letras o si se quiere guardar un número igual validar que solo sean números los que están ingresando si no es así no permitirle guardar los datos, tener unas medidas de seguridad ayuda a que no se realice inyección de código.

d. Privilegios a los usuarios que se conectan en las bases de datos: Cuando se crea un usuario para conectarse en una base de datos se debe tener en cuenta los privilegios para realizar diferentes acciones, no se debe usar usuarios root que tengan el acceso a toda la base de datos porque esto les permite a los atacantes que puedan acceder a cualquier información.

Herramienta de Broken Authentication

Hdiv: nos permite detectar el uso de claves codificadas dentro del código, también los tiempos de espera de sesión que son muy largos, protege las aplicaciones contra los ataques de inicio de sesión de fuerza bruta, permitiendo que se denegué el acceso a usuarios no autorizados.

Evitar ataques con Broken Authentication

- Se recomienda no exponer las sesiones a usuarios.
- Si se transmite datos de sesión de forma segura podemos evitar este tipo de ataque
- Utilizar funciones para cifrar la contraseña permite que los atacantes no les sea fácil entrar al sistema
- Se recomienda implementar la autenticación de multifactor para poder evitar como tal el relleno de credenciales.
- No implementar credenciales predeterminadas.

- Se debe comprobar las contraseñas débiles.
- Tener alineamientos en la longitud y complejidad de las contraseñas.

Herramienta de Broken Access Control

Detectify: es una herramienta de escáner de vulnerabilidades, nos permite descubrir vulnerabilidades de control de acceso roto, entonces esta herramienta prueba un rango de páginas que solo los administradores pueden acceder y ve si alguien más puede acceder a ellas.

Evitar ataques con Broken Access Control.

- Se recomienda la denegación de manera predeterminada y esto se hace desde la programación.
- Implementar funciones donde se valide el acceso único al sistema.
- Restringir la manipulación de datos de sesión para evitar que otros usuarios puedan ingresar.
- Registrar errores de acceso desde la programación.

4.1.4.4 Vulnerabilidad por exposición de datos sensibles

Cada día vemos con mayor frecuencia que en el desarrollo de aplicaciones web y APIs no se realiza un correcta protección de los datos sensibles como lo son información médica, datos bancarios, contraseñas, números de documentos personales, esta información puede estar expuesta para los atacantes tanto en el transporte como en el almacenamiento, debido a esto es necesario utilizar protocolos que envíen los datos cifrados y al momento de almacenar información debemos verificar si en realizada es necesario guardar estos datos y almacenarlos de manera adecuada[25].

Evaluación - A3 EXPOSICIÓN DE DATOS SENSIBLES

Para realizar una evaluación y verificar si nuestro sitio web presenta una exposición a datos sensibles, debemos determinar qué tipo de información maneja nuestra aplicación web, si consideramos que esta información es sensible debemos realizar un tratamiento especial para estos datos y utilizar protocolos seguros que realicen

25 OWASP.. OWASP TOP 10: exposición de datos sensibles. Disponible en https://wiki.owasp.org/images/5/5e/OWASP-Top10-2017-es.pdf

la transmisión de los datos de manera cifrada, ya que si nuestra aplicación utiliza protocolos inseguros como lo son (FTP , TELNET, SMTP, HTTP) los datos viajaran en texto plano y pueden ser interceptados por terceras personas, también debemos tener presente que si tenemos un manejo interno en el cual se comparte información entre servidores, manejos de balanceo de carga o cualquier tratamiento que le demos a la información dentro del BACKEND si poseen un encriptado con algoritmos débiles u obsoleto, como MD5, SHA1, estaremos expuestos de todas formas, también debemos ser muy cuidadosos y realizar una rotación de contraseñas criptográficas con un nivel de seguridad apropiado que garantice su protección[26].

Anticipándonos a las acciones que puede realizar el atacante, este pretenderá.

Como mitigar estas vulnerabilidades - A3 EXPOSICIÓN DE DATOS SENSIBLES.

Para lograr contrarrestar esta vulnerabilidad debemos verificar si la aplicación esta almacenando datos sensibles que realmente no son necesarios, también debemos analizar y realizar una clasificación de los datos que son almacenados y transmitidos mediante un protocolo seguro como TLS con cifradores que brinden un estándar confiable, Verificar que todos los datos sean enviados y almacenados con un cifrado adecuado, la aplicación no debe permitir que los datos sensibles sean almacenados en cache.

Herramientas y técnicas para el análisis - A3 EXPOSICIÓN DE DATOS SENSIBLES

• Descifrar los datos a los cuales tenga acceso.
• Oponerse entre los datos que transitan entre el servidor y el cliente con el fin de realizar el aprovechamiento de la información.
• Enviar solicitudes para Engañar la aplicación web y conseguir elevar los privilegios o modificar contenido accesible.

NESSUS

Tenable,[27] como herramienta para el análisis de esta vulnerabilidad podemos encontrar Nessus Vulnerability Scanner, la cual brinda un escaneo completo para encontrar vulnerabilidades en aplicaciones web, basándose en todos los criterios mencionados en el TOP 10 de OWASP, esta aplicación arroja un informe personalizado por el nivel de criticidad del riesgo permitiéndonos saber qué medidas debemos en nuestro desarrollo para mitigar estas amenazas.

[26] CWE.. CWE-359. Common Weakness Enumeration. 2020. Disponible: https://cwe.mitre.org/data/definitions/359.html
[27] TENABLE. Nessus Profesional. [en línea]. Colombia, 2020. Disponible: https://www.tenable.com/lp/campaigns/19/trynessus/?&utm_source=google&utm_medium=cpc&utm_term=%2Bnessus&utm_content=398015217483&utm_campaign=LATAM_EN_GS_HV_Nessus_Brand_BMM&utm_promoter=tenable-hv-brand-00019179&gclid=CjwKCAjw_qb3BRAVEiwAvwq6VvfB4sGPRH8

MCAfee Vulnerability Manager
Esta herramienta ofrece una monitorización la cual nos permite visualizar los puntos más críticos de la aplicación web, permite realizar pruebas de penetración conociendo los pilares en los cuales debemos enfocar los esfuerzos de programación. Abarca todas las categorías de OWASP y CWE-25[28].

Una técnica utilizada para explotar esta vulnerabilidad es MITM (Man In The Midle) ya que para un atacante es de mayor provecho atacar y capturar los datos en tránsito, que intentar vulnerar la criptografía en los datos almacenados, esto debido a que muchas veces las aplicaciones envían los datos en texto plano o sin cifrar[29]

4.1.4.5 Vulnerabilidad por entidades externas xml (XXE)

Este tipo de ataque se enfatiza en el análisis de entrada de los datos en formato XML. Cuando la aplicación procesa datos de entrada en este formato y posee un analizador XML débilmente configurado, permite la exposición de datos confidenciales y el atacante puede inyectar código XML con el fin de producir una denegación de servicio o falsificación de solicitudes del lado del servidor ocasionando la caída de la aplicación lo que genera pérdidas productivas para la compañía.

Evaluación

Se debe evaluar nuestros sitios web realizando un análisis del comportamiento y la configuración de los procesadores XML, ya que el lenguaje extensible XML se utiliza para describir datos de manera fácil y rápida. XML es una manera maleable de crear formatos de datos estructurados a través de la web, así como a través de redes corporativas, el fin es enviar datos de manera estructurada que puedan ser utilizados por el FRONTEND, podemos realizar una evaluación de estos riegos con una herramienta automatizada o simplemente construyendo un archivo XML con la estructura necesario para realizar cada uno de los ataques. (Castillo, 2019) Un ataque de este tipo puede ocasionar lo siguiente:
• Divulgación de datos y acceso a servicios
• Denegación de servicio (DoS)
• Escaneo de puertos
• Ejecución remota de código.

[28] McAfee. McAfee Vulnerability Manager. [en linea]. Colombia. 2018. Disponible en: https://www.websecurityworks.com/datasheets/ds_mcafee_vulnerability_manager.pdf
[29] kaspersky. QUÉ ES UN ATAQUE MAN-IN-THE-MIDDLE. [en linea]. Colombia. 2013. Disponible en: https://latam.kaspersky.com/blog/que-es-un-ataque-man-in-the-middle/469/

Como mitigar esta vulnerabilidad

Para contrarrestar este tipo de vulnerabilidades debemos tener actualizados los analizadores de XML de nuestras aplicaciones y configurarse de forma segura para que no permita entidades externas, como medida de prevención desde el desarrollo de las aplicaciones se debe tener una política desarrollo la cual evite la utilización de componentes desactualizados los cuales pueden presentar vulnerabilidades y no utilizar métodos desordenados que procesen directamente los XML como Java.io.File, Java.io.Reader o Java.io.InputStream se deben implementar métodos propios para el análisis de la información, otra forma de poder contrarrestar este riesgo es validar la posibilidad de usar otro tipo de formato en las aplicaciones como lo son el formato JSON y evitar estar realizando procesos de serialización de los datos. También se puede considerar la implementación de una validación y limpieza de los datos antes de enviarlos al servidor, con el fin de garantiza que no existan datos que puedan perjudicar la aplicación.

En general, es suficiente deshabilitar la resolución de entidades externas y deshabilitar el soporte para XInclude. Esto generalmente se puede hacer a través de las opciones de configuración o anulando mediante programación el comportamiento predeterminado. Consulte la documentación de su biblioteca de análisis XML o API para obtener detalles sobre cómo deshabilitar capacidades innecesarias.

Existe otra forma de validar estos datos por medio de la validación de XSD, que son estructuras configurables para validar un esquema de datos en formato XML, ofreciéndonos la seguridad de que en el XML entrante viene únicamente con la estructura de datos que el servidor puede leer y procesar. (OWASP, XML External Entity, 2020)

Herramientas y técnicas para el análisis

La gran mayoría de las vulnerabilidades XXE se pueden encontrar de forma rápida y confiable utilizando el escáner de vulnerabilidades web de Burp Suite que permite un análisis automático de todas las vulnerabilidades presentes en OWASP[30]

Si deseamos realizar las pruebas manuales debemos tener presente los siguientes aspectos:

Prueba de recuperación de archivos mediante la definición de una entidad externa basada en un archivo conocido del sistema operativo y el uso de esa entidad en los datos que se devuelven en la respuesta de la aplicación.

[30] CASTILLO, Alexander. Entidades externas XML vulnerables. [en línea]. Colombia. Disponible en: https://seguridad-ofensiva.com/blog/owasp-top-10/owasp-top-4/

Prueba de vulnerabilidades ciegas XXE definiendo una entidad externa basada en una URL a un sistema que usted controla y monitoreando las interacciones con ese sistema.

El cliente Burp Collaborator es perfecto para este propósito.
Prueba de inclusión vulnerable de datos no XML proporcionados por el usuario dentro de un documento XML del lado del servidor mediante un ataque XInclude para intentar recuperar un archivo conocido del sistema operativo[31].

4.1.4.6 CROSS- SITE SCRIPTING (XSS)

Esta vulnerabilidad de seguridad web podría permitir a un atacante poner en peligro la interacción de un usuario con una aplicación. Esto permite a los ciberdelincuentes eludir la misma política original diseñada para separar diferentes aplicaciones web entre sí.
Las vulnerabilidades de secuencias de comandos entre sitios a menudo permiten que un atacante se haga pasar por un usuario de la víctima, realice acciones que el usuario podría realizar y obtenga acceso a todos los datos del usuario. Si el usuario de la víctima tiene acceso privilegiado a la aplicación, el atacante tiene control total sobre toda la funcionalidad y los datos de la aplicación.

¿Cómo funciona?

Esta vulnerabilidad se da por medio de la manipulación de un sistema web para que retorne un código JavaScript malicioso a las personas que lo interactúan. Cuando dicho código malicioso se ejecuta dentro del navegador del usuario, el ciberdelincuente puede alterar de forma comprometedora la interacción con el sitio web.

Hay tres tipos principales de ataques Cross-Site Scripting (XSS). Estos son:

- XSS reflejado, es la variedad más simple de secuencias de comandos entre sitios. Surge cuando una aplicación recibe datos en una solicitud HTTP e incluye esos datos dentro de la respuesta inmediata de manera insegura.

- XSS almacenado, surge cuando una aplicación recibe datos de una fuente no confiable e incluye esos datos dentro de sus respuestas HTTP posteriores de una manera insegura.
Los datos en cuestión pueden enviarse a la aplicación a través de solicitudes HTTP; por ejemplo, comentarios en una publicación de blog, apodos de usuarios en una sala de chat o detalles de contacto en un pedido de un cliente. En otros casos, los

[31] CAMPOS, Pablo. Hacer testeo con Burp Suite. Colombia. 2017. Disponible en: https://openwebinars.net/blog/hacer-testeo-con-burp-suite/

datos pueden llegar de otras fuentes no confiables; por ejemplo, una aplicación de correo web que muestra mensajes recibidos a través de SMTP, una aplicación de marketing que muestra publicaciones en redes sociales o una aplicación de monitoreo de red que muestra datos de paquetes del tráfico de red.

- XSS basado en DOM, surge cuando una aplicación contiene algún JavaScript del lado del cliente que procesa datos de una fuente no confiable de una manera insegura, generalmente escribiendo los datos nuevamente en el DOM.

¿Qué fin tienen los ataques?

Lo que pretende un ciberdelincuente con estos es:

- Hacerse pasar por el usuario que interactúa con la aplicación.
- Usar los privilegios de la víctima para consultar o alterar la información.
- Obtener los datos de accesos de la víctima.
- Intentar dañar o dar de baja el sitio web.
- Intentar introducir un virus en el sitio.

Impacto de las vulnerabilidades XSS

El impacto real de un ataque XSS a menudo depende de la naturaleza de la aplicación, sus capacidades y datos, así como del estado del usuario comprometido. Ejemplo:

Para una aplicación de folleto donde todos los usuarios son anónimos y toda la información es pública, el impacto será mínimo.

Las aplicaciones que incluyen datos confidenciales como datos bancarios, correos electrónicos y registros médicos suelen tener un impacto significativo.

Si un usuario comprometido tiene privilegios elevados en la aplicación, el impacto suele ser severo y un atacante puede tomar el control completo de la aplicación vulnerable y poner en peligro a todos los usuarios y sus datos.

Cómo encontrar y probar vulnerabilidades XSS

La gran mayoría de las vulnerabilidades XSS se pueden encontrar de forma rápida y confiable utilizando el escáner de vulnerabilidades web de Burp Suite.

La prueba manual de XSS reflejado y almacenado normalmente implica enviar alguna entrada única y simple (como una cadena alfanumérica corta) en cada punto de entrada de la aplicación; identificar cada ubicación donde la entrada enviada se devuelve en respuestas HTTP; y probar cada ubicación individualmente para

determinar si la entrada adecuadamente diseñada puede usarse para ejecutar JavaScript arbitrario.

La prueba manual de XSS basado en DOM que surge de los parámetros de URL implica un proceso similar: colocar una entrada única y simple en el parámetro, usar las herramientas de desarrollo del navegador para buscar el DOM para esta entrada y probar cada ubicación para determinar si es explotable. Sin embargo, otros tipos de DOM XSS son más difíciles de detectar. Para encontrar vulnerabilidades basadas en DOM en entradas no basadas en URL (como document.cookie) o sumideros no basados en HTML (como setTimeout), no hay sustituto para revisar el código JavaScript, que puede llevar mucho tiempo. El escáner de vulnerabilidades web de Burp Suite combina análisis estático y dinámico de JavaScript para automatizar de manera confiable la detección de vulnerabilidades basadas en DOM.

Cómo mejorar la seguridad para contrarresta ataques XSS

La prevención de secuencias de comandos entre sitios puede ser fácil, pero puede ser mucho más difícil, según la complejidad de su aplicación y cómo maneja los datos que controla.

En general, las siguientes medidas deben combinarse para prevenir de manera eficaz las vulnerabilidades XSS:

Filtro de entrada. Cuando recibimos información de los usuarios, la filtramos lo más cerca posible en función de la entrada esperada o válida.

Codifica los datos de salida. Dado que los datos controlados por el usuario se envían en una respuesta HTTP, codifique la salida para que no se interprete como contenido en vivo. Dependiendo del contexto de salida, es posible que deba aplicar una combinación de codificaciones HTML, URL, JavaScript y CSS.

Utilice el encabezado de respuesta adecuado. Para evitar XSS en las respuestas HTTP que no pretenden incluir HTML o JavaScript, utilice los encabezados ContentType y XContentTypeOptions para asegurarse de que el navegador interprete la respuesta como se esperaba.

Información sobre la privacidad de los contenidos. Como última línea de defensa, puede utilizar la Política de seguridad de contenido (CSP) para mitigar la gravedad de las vulnerabilidades XSS existentes**.**

4.1.4.7 Uso de componentes con vulnerabilidades conocidas

¿Qué es OWASP A9[32]?

El atacante puede identificar componentes vulnerables mediante escaneo o análisis manual.
Los sitios web muy frecuentemente tienen o usan componentes a los cuales se les ha identificado vulnerabilidades.
En muchos casos, los desarrolladores ni siquiera conocen todo el código que se está ejecutando. Esto se debe principalmente a los complementos que a su vez importan bibliotecas que a su vez tienen sus propias dependencias, etc.

Impacto de esta vulnerabilidad.

El impacto potencial es imposible de calificar para esto, ya que depende completamente del componente vulnerable y de qué vulnerabilidad sufre. La vulnerabilidad podría ser un XSS en algún subdominio sin importancia, pero también podría conducir a una toma de control completa del sistema.

¿Cómo los atacantes hacen uso de esta vulnerabilidad?

Cuando se publica una vulnerabilidad en Internet, a menudo alguien carga una carga útil lista para usar que un atacante podría simplemente descargar y usar contra el objetivo. Esto significa que un atacante puede usarlo hacia el sitio sin siquiera saber cómo y por qué funciona. Incluso cuando un PoC no está disponible, la documentación sobre la vulnerabilidad es de fácil acceso, por lo que todo lo que el atacante debería saber es cómo seguir las instrucciones.

Sin embargo, por supuesto, también hay excepciones a esto. Algunas vulnerabilidades requieren conocimiento existente sobre el sistema, y si el componente que es vulnerable no está directamente expuesto a Internet, el atacante también necesitaría encontrar una solución para eso.

En resumen, esto es a menudo realmente fácil de explotar, pero puede ser tan difícil como cualquier otra vulnerabilidad.
En los últimos años, se han publicado aproximadamente 4500 CVE cada año, y, por supuesto, hay aún más vulnerabilidades. Por lo tanto, no sorprende que a la mayoría de los desarrolladores les resulte imposible mantenerse al día con toda esta información.

Como podemos descubrir estas vulnerabilidades.

32 Seguridad ofensiva. OWASP Top 9. Uso de componentes con vulnerabilidades conocidas. Colombia. Disponible en: https://seguridad-ofensiva.com/blog/owasp-top-10/owasp-top-9/

El primer paso es identificar todos los componentes que se están utilizando y que podrían ser vulnerables, es decir, los que de alguna manera procesan los datos del usuario. Esto incluye soluciones CMS, servidores web, sistemas operativos, complementos y todo lo demás.

El siguiente paso es buscar vulnerabilidades y vulnerabilidades en cada componente. El primer paso sería usar Google para buscar esto, y luego proceder a buscar diferentes vulnerabilidades y explotar bases de datos.

Para aumentar la probabilidad de escuchar sobre vulnerabilidades antes de que alguien más las use con fines maliciosos, las listas de correo, los foros y el boca a boca son ejemplos de los medios que sería necesario aprovechar.

¿Cómo posemos subsanar estas vulnerabilidades?

El primer paso para deshacerse de las vulnerabilidades en los componentes que está utilizando sería mantener siempre todo actualizado. Cree el sistema de manera que permita la instalación de parches de seguridad de manera oportuna.

Tenga cuidado cuando se utilizan componentes externos, complementos, softwares o incluso las dependencias de esos complementos. Asegúrese de que todo cumpla con los requisitos establecidos para el código personalizado con respecto al mantenimiento regular, pasando las pruebas de seguridad, etc.

Eliminando los complementos que no se utilizan, deshabilitando las funciones que no sirven, bloqueando los puertos que no estén en uso.

Escaneando regularmente el sitio con un escáner de seguridad que se actualice con nuevas vulnerabilidades. Al usar nuestro propio servicio, el valor predeterminado es escanear una vez por semana, ya que lo actualizamos constantemente con más vulnerabilidades, y recomendaríamos algo similar si también se usara otro servicio.

4.1.4.8 Configuración de seguridad incorrecta

El ataque se produce intentando explotar la vulnerabilidad que ocasiona el no parcheo, cuentas predeterminadas que no son cambiadas, paginas sin uso, entre otras.

Estas configuraciones incorrectas pueden ocurrir en los servicios de red, las bases de datos, Frameworks, máquinas virtuales, entre otros.
Entre más funciones desempeñe un sistema estará más vulnerable a los ataques.

Para dar solución a esta vulnerabilidad se deben tener en cuenta estas características:

• En los entornos de desarrollo se pueden configurar idénticamente dos sistemas con credenciales distintas para realizar configuraciones de entornos seguros.

• Tener políticas fuertes en claves seguras que pidan cambios en tiempos cortos.

• Se debe implementar un proceso automatizado donde se verifique la efectividad de los ajustes y configuraciones en todos los ambientes.

• Realizar un control de los permisos de almacenamiento de la nube.

• Se debe realizar un seguimiento para revisar y actualizar las configuraciones según los resultados de las advertencias de seguridad y continuar un proceso de gestión de actualizaciones y parches.

Se conoce que en internet la web se maneja bajo el protocolo http que permite la comunicación con el servidor web donde se aloja la información y estructura de la página.

Esta información se encuentra dividida en cabecera y cuerpo, la cabecera si no se encuentra bien configurada puede revelar información importante que puede ser utilizada por un atacante.

Cabeceras HTTP más habituales según el portal webempresa[33]:

Server: indica el tipo de servidor HTTP empleado.
Age: indica el tiempo que ha estado el objeto servidor almacenado en un proxy cache.

Cache-control: lo usa el servidor para decirle al navegador que objetos cachear, durante cuánto tiempo, etc..

Content-Encoding: se indica el tipo de codificación empleado en la respuesta

Expires: indica una fecha y hora a partir del cual la respuesta HTTP se considera obsoleta. Usado para gestionar caché.

P3P: se usa para especificar el tipo de política de privacidad empleado en la web.

[33] NOGUERA, David. Cabeceras HTTP más comunes. [en linea]. Colombia. 2020. Disponible en: https://www.webempresa.com/blog/cabeceras-http-mas-comunes.html

Set-Cookie: sirve para crear cookies. Las famosos cookies viajan entre el servidor y el navegador a través de estas cabeceras HTTP.

Existen otras cabeceras no estándar como:

X-Powered-by: usado para especificar con que software se ha generado la respuesta por parte del servidor.

X-Pingback: Cabecera HTTP que añade WordPress donde especifica la dirección de pingback del blog.

Como ejemplo de evitar esta vulnerabilidad se puede asegurar las cabeceras utilizando HTTP Strict Transport Security (HSTS).

Esta capa de seguridad solicitara siempre que un navegante intente conectar a un usuario lo haga usando el protocolo HTTPS.

Para el servidor apache seria: Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

4.1.4.9 Registro y Monitoreo Insuficientes

Al no realizar el registro y monitoreo eficiente de un sistema hace que sea la base de todas las vulnerabilidades de seguridad.

Para la explotación de esta vulnerabilidad se deben tener en cuenta estas características:

• El sistema debe lograr detectar, alertar, informar ataques en tiempo real.

• Los niveles requeridos de alerta y escalamiento no tienen la eficacia que se requiere para la información que manejan.

• Cuando se revisan los registros de las aplicaciones estas se guardan sin ninguna política de almacenamiento, lo que hace que sea riesgoso perder la información.

• En el sistema no se tiene con una implementación de algún software o herramienta de monitoreo, adicional no está siendo revisada por alguien idóneo o no es clara la información que arroja.

Para dar solución existen varias herramientas de monitoreo, como por ejemplo la herramienta PRTG.

Esta herramienta permite monitorear servidores de correo, servidores de internet, servidores de bases de datos, servidores virtuales logrando la detección y posteriormente la respuesta oportuna para evitar fraudes y ataques a los servicios en sistemas.
Las soluciones a estas vulnerabilidades abarcan:
• Hay que asegurar los inicios de sesión, controles de acceso estén registrados y clasificados para poder identificar cuentas sospechosas.
• Esos registros deben tener políticas de almacenamiento controlando la integridad de esos datos y evitando la modificación y borrado.
• Realizar controles de auditoria donde en la evidencia de actividades no confiables sean detectadas y arregladas en el tiempo menos posible.
• Implementar un plan de recuperación de incidentes.

4.1.4.10 Deserialización insegura

Una serialización de datos en un proceso de agrupación de información contenida en un objeto, este proceso se realiza para enviar los datos a través de la red o como un método de almacenar de forma persistente en un almacenamiento rígido la información[34]
Los formatos utilizados para serializar información son estructuras de datos conocidas como JSON y XML entre las más conocidas.

Como proceso opuesto existe la deserialización que consiste en tomar la información proveniente de la red o de la lectura en disco. Con el fin de crear nuevamente un objeto de datos con el cual la aplicación pueda entender y manipular según las necesidades.

Explosión de la vulnerabilidad Deserialización insegura

Para explotar esta vulnerabilidad se hace uso de estructuras serializadas como un JSON el cual contiene código malicioso que puede ser interpretado por una aplicación web y así manipular su flujo normal de funcionamiento y así obtener información deseada por el atacante[35]

No existe patrones de código que permitan protegerse de este ataque, pero en cambio se pueden seguir una serie de recomendaciones para estar protegidos de forma parcial ante esta vulnerabilidad.

[34]JIMENEZ, Carlos David. UNIDAD ACADÉMICA DE INGENIERÍA CIVIL. [En línea]. Colombia 2019. Disponible en: http://repositorio.utmachala.edu.ec/bitstream/48000/13606/1/ECUAIC-2019-S IS-DE00010.pdf.
[35] BARRAGAN, Alejandro. Seguridad lógica usando entornos de desarrollo en aplicaciones web empresariales. [En línea]. Colombia 2020. Disponible en: https://repository.unad.edu.co/handle/10596/33794

• Denegar todos los objetos serializados que provengan de lugares no autorizados
• De ser posible solo permitir objetos serializados que contengan datos primitivos
• Realizar verificación de firma digitales en los archivos serializados recibidos por el sistema
• Monitorear constantemente a los usuarios para determinar si alguno de ellos se encuentra desrealizando constantemente y de forma sospechosa

ANAYA[36], concuerda que existen diversas vulnerabilidades y amenazas en los servicios web tales como ataques externos e internos debido a que los servicios web están diseñados para ser abiertos e interoperables. Al configurar los firewalls para permitir tráfico HTTP, las solicitudes a los servicios por dicho protocolo pasan a través de los firewalls fácilmente, dejando a la red interna expuesta. En este estudio se demuestra que la utilización de tokens SAML utilizados como mecanismo de seguridad puede resolver el problema de la autorización y autenticación en el consumo de servicios web. Lo que permite que el servicio web no se encuentre disponible a terceros autorizados y que solo pueden acceder al servicio aquellos que están definidos en la política de seguridad

4.1.5 La economía digital

Actualmente en Colombia, desde el Consejo Nacional de Política Económica y Social adscrito al Departamento Nacional de Planeación, en conjunto con el Ministerio de Tecnologías de la Información y las Comunicaciones, se expidió la Política No. 3975 del 8 de noviembre de 2019 para la transformación digital e inteligencia artificial, en la que se definió el concepto de economía digital como “una amplia gama de actividades económicas que utilizan información y conocimiento digitalizados como factores clave de producción, las tecnologías digitales se utilizan para recopilar, almacenar, analizar y compartir información digitalmente y transformar las interacciones sociales” (Consejo Nacional de Política Económica y Social, 2019, p.19 [37]

La economía digital en algunos productos ya no tienen que ser empaquetados y distribuidos a través de una tienda física (software, noticias, música, video, etc.). Ahora una diversidad de productos y servicios son distribuidos directamente a través de Internet (Boletos de avión, obras musicales, servicios personalizados de noticias, reservaciones turísticas, servicios bancarios). Distintos sectores de

[36] ANAYA LOPEZ, Emilio. Implementación de Controles de seguridad en arquitecturas orientadas a servicios (SOA) para servicios Web. Upiiesa, México 2010. 54 p.
[37] Consejo Nacional de Política Económica y Social. [en línea]. CONPES. Colombia. 2019. p.19. Disponible en: https://www.dnp.gov.co/CONPES/Paginas/conpes.aspx

diferentes industrias cambiaron la forma de operar sus negocios, obteniendo beneficios significantes por el desarrollo de productos y servicios digitales.[38]

4.1.5.1 Características de la economía digital

Según la revista de economía digital,[39] esta cuenta con características como:

- Conocimiento

En la economía digital el conocimiento es el motor, mientras que los recursos tradicionales como capital o trabajo pasan a ser secundarios.

- Digitalización

La información es almacenada digitalmente lo que permite la transferencia de enormes cantidades de conocimientos prácticamente de forma instantánea.

- Virtualización

En la economía digital las objetos físicas y tangibles se convierten en elementos virtuales. Esto cambia las reglas de interacción y las posibilidades. Ejemplo, una aplicación que reemplace el uso de la regla o metro para medir.

- Molecularización

Cambia las estructuras tradicionales de trabajo por formas más flexibles. a economía digital amplía el alcance y viabilidad de formas de trabajo como teletrabajo o coworking.
Las organizaciones sobrevivientes son aquellas que se adaptan rápidamente a los cambios.

- Desintermediación

Se reduce el uso de intermediarios pues la tecnología facilita el intercambio de información y productos directamente.

- Convergencia

La convergencia de la computación, las comunicaciones y los contenidos es la creadora de la nueva economía digital.

- Innovación

[38] ROIG C. J. M. Revista digital de economía digital. El Centro de Tesis, Documentos, Publicaciones y Recursos Educativos más amplio de la Red. 2002. © Monografias.com S.A. Disponible en: https://www.monografias.com/trabajos82/economia-digital/economia-digital.shtml
[39] ROIG. Op. cit pág. 3

A partir de las tecnologías de información se desarrollan nuevos productos y servicios. La imaginación y creatividad se vuelven más valiosos.

- Prosumidores

Las personas se convierten en tanto productores como consumidores de contenidos digitales. Los consumidores personalizan sus productos y además participan de la producción de los bienes que compran.

- Inmediatez

Los consumidores esperan que los productos sean distribuidos más rápido gracias a las nuevas tecnologías.

- Globalización

No existen conocimientos nacionales, con la economía digital se fortalece la globalización. Las compañías tienen mayor acceso a mercados extranjeros.

- Discordancia

Las nuevas tecnologías pueden dividir a la sociedad en cuanto van a existir personas que se adaptan rápidamente y aprovechan las tecnologías, mientras que otras quedan por fuera y no se benefician.

4.1.6 Asobancaria sus funciones y responsabilidades

Asobancaria que representa el sector financiero en Colombia, se reconoce como una entidad sin ánimo de lucro y por tanto, de ella hacen parte establecimientos bancarios, nacionales y extranjeros; así como corporaciones financieras, compañías de financiamiento, instituciones oficiales especiales y la Titularizadora colombiana.[40]

4.1.6.1 Asobancaria tienes las siguientes responsabilidades

Dentro de las responsabilidades que tiene esta entidad están, representar y defender los intereses de sus miembros agremiados, debe promover y mantener la confianza del público en el sector financiero, además de ampliar y mejorar permanentemente el conocimiento público acerca de la naturaleza y función de la actividad financiera y aportar a la continua modernización del sector.
Además, es importante resaltar que, Asobancaria no actúa solamente como un ente regulador, sino que también busca promover el desarrollo del sector financiero a través de tres principios esenciales: confianza, sostenibilidad y competitividad.

[40] CASTRO, Santiago. Asobancaria, banca y economía. Edición 04. Colombia. 2016. 48 p.

Es decir, logrando mantener la confianza de la sociedad colombiana en el sector financiero, podrá fortalecer la confianza de esta ante los entes reguladores, legisladores y la comunidad financiera internacional.
Otro de sus principios está encaminado en velar por el futuro del negocio bancario financiero, promoviendo acciones que impacten positivamente en la sociedad y que permitan una proyección del sector financiero la banca como sector fundamental para el desarrollo del país. Y finalmente, la competitividad permitirá promover el sano y libre desarrollo de la competencia en el sector bancario colombiano.

4.2 MARCO CONCEPTUAL

De manera importante se destacan los siguientes conceptos

4.2.1 El modelo financiero tradicional

El modelo bancario tradicional es ese en el que los clientes consultan el saldo de su cuenta y el historial de movimientos bancarios a través de su cartilla bancaria; pero si bien es cierto la banca tradicional ha conquistado gran cantidad de usuarios brindándoles atractivas ofertas financieras, también hoy se ha visto enfrentada a otros servicios que evolucionaron a partir de la era digital y la modernización de procesos. Hoy por hoy, los consumidores exigen contar con servicios rápidos, transparentes y seguros, y que estos mismos servicios o productos financieros les ayuden a optimizar tiempos.

4.2.2 Transacciones online

Actualmente en Colombia, el sector fintech ha liderado e impulsado el tema digital, logrando llevar al público los servicios bancarios en línea, permitiendo así que los ciudadanos progresivamente se involucren y conozcan de cerca el funcionamiento de los créditos y pagos online o las transacciones en línea. A pesar de los esfuerzos de la industria por impulsar el uso de herramientas tecnológicas para la evolución no solo del mismo sector sino de todo el país, aún estos intentos quedan grises en su implementación. En realidad, la necesidad de la población por acceder a servicios financieros ha generado que el sector sea cada vez más atractivo y atento ante la demanda; sin duda, acceder a un servicio bancario a través de internet es una puerta de entrada a la bancarización y es allí donde la banca tradicional se convierte en un aliado para este innovador sector.[41]

[41] ASOBANCARIA. Semana Económica 2018. “Disrupción digital en los mercados financieros”. Edición 1161. 6 Colombia. 2018. Disponible en: https://www.asobancaria.com/wp-content/uploads/1161.pdf

Para Rivera Víctor[42] analista de semana "es fundamental desarrollar nuevas herramientas y nuevos productos, en donde es fundamental desarrollar la economía digital, como las fintech [...] Considero que estamos afrontando una necesidad de actualizar y modificar el sistema financiero para que tenga nuevos productos".

4.2.3 Las Fintech

Según López[43] El término de Fintech nace de la integración de dos palabras, 'Finance' - Finanzas- y 'Technology' -Tecnología-, la cual agrupa a todas aquellas empresas financieras que utilizan la última tecnología para poder ofrecer sus productos y servicios altamente innovadores.

Según Falguni[44], el termino Fintech como su nombre lo indica, se refiero al uso de la tecnología como factor para la prestación de servicios financieros de una forma más dinámica y eficiente. A través de los años se puede observar como este término presenta pequeñas variaciones en su definición dependiendo del contexto en que se definió y las connotaciones que cada autor decidió darle basados en los conocimientos de este nuevo mercado en determinado momento del tiempo. Muchas personas asumen las FinTech como un fenómeno de la actualidad gracias al auge que ha experimentado esta industria en los últimos años de la mano de avances tecnológicos como la inteligencia artificial y los teléfonos inteligentes, si nos adentramos en los límites que implica su significado podemos darnos cuenta que las Fintech han sido un factor importante en la historia y desarrollo de la industria financiera, puesto que desde la década de los 50' con la introducción de las tarjetas de crédito se ha evidenciado como el ser humano busca mejorar constantemente la confiabilidad y eficiencia con la que se prestan los servicios financieros ayudados principalmente por factores de carácter fundamental como lo ha sido la tecnología.

Rojas[45], define el sector Fintech como: el conjunto de empresas no financieras que usan la tecnología digital y herramientas asociadas –computación en la nube, blockchain, Big Data, inteligencia artificial, redes sociales, etc. – para prestar servicios financieros a consumidores y empresas de una forma innovadora y bajo nuevos modelos de negocio.

---

[42] RIVERA, Victor. El sistema financiero requiere productos nuevos y especializados, revista semana. Colombia 2021.
[43] LÓPEZ, Esteban. Crowdlending.es ¿Qué es Fintech?. [en línea]. Disponible en: https://www.crowdlending.es/blog/que-es-fintech
[44] FALGUNI, D. The Evolution of FinTech. FORBES GONZÁLEZ, Victor 2009, Global Technology servicios y tecnologías de la información. 2015
[45] ROJAS, L. La revolución de las empresas FinTech y el futuro de la Banca. Disrupción tecnológica en el sector financiero. Políticas públicas y transformación productiva, 24, Caracas 2016. CAF. Recuperado de http://scioteca.caf.com/handle/123456789/976

4.3 MARCO LEGAL

Para determinar el aspecto normativo y de legislación políticas que regulen la economía digital y sus transacciones digitales. Dentro de la basta normatividad legal y jurídica, se destacan las referidas a continuación:

DECRETO NÚMERO 704 DE 2018 "Por el cual se crea la comisión intersectorial para el desarrollo de la Economía Digital y se adiciona un artículo en el título 2 de la parte 1 del libro 1 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015[46]

La Ley 1273 de 2009 [47] es una legislación que también involucra los movimientos del sistema financiero digital en Colombia, pues cobija a la banca digital tipificando los delitos informáticos en Colombia, incluyendo las infracciones por y para canales financieros electrónicos.

La Ley 1430 de 2010, en los artículos 62 y 63[48], en esta norma se obliga a que las tarifas por consultas de saldo y transacciones que se realicen a través de internet, o canales digitales, no pueden ser superiores a las cobradas por los canales tradicionales.

La Ley de Protección de Datos Personales o Ley Estatutaria 1581 de 2012. [49]Los antecedentes de esta normativa se basan en que la información es el activo más importante en el mundo actual; por ello, era necesario dictar las disposiciones generales para la protección de datos personales.

En la búsqueda de una inclusión financiera en el país, se sancionó la Ley 1735 de 2014 creó las Sociedades Especializadas en Depósitos y pagos Electrónicos (Sedpe), [50]destinada a promover la inclusión financiera a través de productos financieros transaccionales, como transferencias, pagos, giros y recaudo, que posteriormente se expidió mediante el Decreto Número 1491 del 13 de julio de 2015.

[46] SUIN Sistema Único de Información Normativa, DIARIO OFICIAL. AÑO CLIII. N. 50570. 20. 2018. 39 p.
[47] ANDRADE, Hernan y RAMÓN OTERO Emilio. Diario Oficial LEY 1273 (DE 2009), 1- 4 p
[48] SEMANA. La banca digital transforma la vida de los usuarios. [en línea]. Abril 15 DE 2021. Disponible en: HTTPS://WWW.SEMANA.COM/TECNOLOGIA/ARTICULO/COMO-TRANSFORMA-LA-VIDA-DE-LAS-PERSONAS-LA-BANCA-DIGITAL/278826/
[49] Ibid, diario oficial. año cxlviii. n. 48587. (18, octubre de 2012). 1 p.
[50] DURAN, Maria Antonia. Las sociedades especializadas en depósitos y pagos electrónicos. 2015. Disponible en: https://www.asuntoslegales.com.co/consultorio/las-sociedades-especializadas-en-depositos-y-pagos-electronicos-2237746

El Congreso de la República aprobó, en mayo de 2019, un *fast track* de licencias para las ***fintech*.**[51]
Comercio Electrónico. Legislación Nacional – Colombia. Ley No 527 [52]Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

La Ley de Delitos Informáticos: la Ley 1273[53], también conocida como Ley de la Protección de la Información y de los Datos (Congreso de la República, 2009); sin embargo, no se explicará cada uno de sus artículos. En este caso, se señalarán los artículos que mencionan los riesgos más factibles de materializarse en la computación en la nube.
Los riesgos identificados son los siguientes:

- Artículo 269A: acceso abusivo a un sistema informático
- Artículo 269C: interceptación de datos informáticos.
- Artículo 269D: daño informático.
- Artículo 269F: violación de datos personales.
- Artículo 269J: transferencia no consentida de activos.

4.3.1 Norma ISO 27001 de 2013

ISO 27001 del 2013, es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.[54]

51 Colombia Fintech. Congreso de Colombia aprueba fast-track de licencias para Fintechs. [en línea]. Bogotá. 2020. Disponible en: www.colombiafintech.co
[52] Ibid., diario oficial. año cxxxv. n. 43673. 21, agosto, 1999. 1 p
[53] Colombia. Diario Oficial LEY 1273 (enero 5 de 2019)
[54] Blog especializado en Sistemas de Gestión de Seguridad de la Información 11 mayo, 2016

5. LAS FINTECH DESDE SU OPERATIVIDAD, INFRAESTRUCTURA TECNOLOGICA Y MECANISMOS DE SEGURIDAD DE LA INFORMACIÓN

En el siglo XXI, cuando surgió la tecnología financiera, está se empleó en las instituciones ya establecidas, con cambios que han sido orientados al consumidor de servicios. Según Rodríguez Ivan[55] el término tecnología financiera podía ser aplicado a cualquier innovación que les permitiera a las personas realizar transacciones comerciales, pero, desde que internet revolucionó con su tecnología que solo era aplicada a oficinas administrativas de bancos, o empresas comerciales, pudo establecerse ahora realizando intervenciones tecnológicas en personal y finanzas comerciales.
Por ello, soportados en nuevas tecnologías las Fintech ofrecen soluciones financieras, orientadas a algún aspecto de las finanzas, con una gran innovación y como reto para la banca; por tanto, poseen una propuesta concreta en cuanto a préstamos, captación de recursos, medios de pago, pagos y asesoramiento financiero.

5.1 Operatividad y servicios financieros Fintech

Haciendo uso de las nuevas tecnologías las Fintech pueden ofrecer a sus clientes soluciones a problemas financieros o a situaciones que no fueron bien atendidas por la banca; principalmente con el uso de los dispositivos móviles, colocando al servicio de las personas aplicaciones fáciles de manejar, pensados para ser usados por personas no expertas, se han hecho confiables y transparentes permitiendo esto que sea una verdadera innovación tecnológica.
Están orientadas a cubrir una necesidad financiera central, que las hace intuitivas y amigables, permitiendo al cliente interactuar con un componente de tranquilidad y transparencia, centrado en solucionar el problema de forma rápida y eficaz.
Estos negocios con ideas innovadoras sobresalen en el mercado por el apoyo que encuentran en las nuevas tecnologías, presentando productos y servicios, que tienen su diseño y comercialización orientados completamente al cliente. Suelen operar con costos mínimos, pero obtiene ganancias que crecen exponencialmente, mantiene una comunicación continua y abierta con los clientes, y se orienta a la masificación de las ventas. Cada startup está respaldado por una idea que busca simplificar procesos y trabajos complicados, con el objetivo de que el mercado tenga una experiencia de uso simplificada y fácil.

Para comprender y profundizar en dichos servicios, nos basaremos en el Análisis de clasificaciones existentes de las Fintech, de acuerdo a sus servicios financieros, estudio realizado en 2016 sobre la Radiografía del FinTech por los hermanos Bosch

[55] RODRÍGUEZ, Ivan. ¿Qué es Fintech, tecnología financiera y cuál es su importancia? Colombia. 2020.

Liarte.[56] Este estudio permite ver como la financiación alternativa se hace habitual haciendo uso de los canales tradicionales de la banca comercial, pudiendo estas Fintech articularse de maneras muy distintas a través de: Los préstamos, ofreciendo productos de activos para sus balances y de pasivos para sus clientes. Por otra parte, también las líneas de crédito con plataformas unilaterales donde la financiación no depende de la inversión que hagan otros usuarios en la plataforma. Además, el adelanto en efectivo, que está básicamente dirigidos a un público con un riesgo elevado, pues estos adelantos son costosos. Las marketplaces de préstamos p2p, que ofrecen a sus clientes no solamente prestamos sino otras opciones de inversión, con plataformas unilaterales que benefician a ambos usuarios, creando necesidades de los unos con otros. La financiación procedente de e-commerce y retailers, es la financiación ofrecida por nuevos jugadores del mercado como son los grandes e-commerce como Alibaba o Amazon ya que son un 100% online y sus ofertas son totalmente innovadoras.
Los descuentos de facturas están dirigidos a pymes, con un coste menor y más flexible, esto consiste en vender las facturas a cobrar a un inversor con tal de recibir el dinero por anticipado, de manera que el inversor asume el riesgo de impago del cliente. También, las finanzas para la cadena de suministro, esto permite que los proveedores tengan la posibilidad de pagar facturas anticipadas con el fin de obtener un descuento. Las Fintech que están en el entorno financiero del comercio internacional, cuentan con la financiación del comercio que actúa como un intermediario más, proponiendo un camino nuevo completamente independiente de los bancos, siempre y cuando sean Fintech innovadoras y con un modelo de negocio escalable.

Por otra parte, para Bosch Liarte[57] los productos y servicios de inversión son aquellos que engloban las Fintech que ofrecen productos y servicio de inversión tanto para particulares, como profesionales e instituciones, dentro de los cuales se encuentran: La copy-investing son Fintech que ofrecen servicios de inversión apalancadas en un modelo de red social, permitiendo que un usuario copie la táctica que otro utiliza en el medio; también la gestión del patrimonio e inversiones, son plataformas que ofrecen consejos automatizados en base a las inputs dadas por el cliente. En cuanto a la financiación del comercio, están presentes en las importaciones y exportaciones, actuando como intermediario y proponiendo caminos nuevos e innovadores con modelos de negocio escalable.
En cuanto a la provisión del mercado, agrupa aquellas Fintech que dan soporte a instituciones financieras tradicionales como la infraestructura bancaria ya que frecen software a las instituciones financieras tradicionales y a otras Fintech para que éstas

[56] BOSCH LIARTE, Javier. BOSCH LIARTE, Joan. Radiografía del Fintech, clasificación, recopilación y análisis de los principales startups. Universidad Politecnca de Catalunya. España. 2016. 42 p. Disponible en: *https://upcommons.upc.edu/bitstream/handle/2117/97361/TFM_Memoria_Bosch_Liarte_Joan_i_Bosch_Liarte_Xavi.pdf?sequence=1*

[57] BOSCH, Op Cit. 45p

puedan desarrollar sus actividades y procesos. Dentro de este grupo también se encuentran las APIs que permiten a otras Fintech poder integrarse con otros bancos e instituciones financieras de una forma sencilla.

Según la clasificación de Bosch[58] existe otro grupo de Fintech de datos y analíticas cuya propuesta gira en torno a las tecnologías de la información, captando, tratando y analizando datos, dentro de los cuales se encuentran: el riesgo crediticio que está dirigido principalmente a los particulares ya que utilizan mayores fuentes de información contrario a los tradicionales. Los datos de mercado de capitales que directa o indirectamente facilitan el contacto entre los diferentes agentes de los mercados de capitales con tal de agilizar las comunicaciones mediante flujos de información más eficientes y eficaces.
Al hablar de los productos y servicios bancarios, estas Fintech ofrecen servicios a los particulares, como los Neo bancos, ofreciendo la combinación de cuenta bancaria más tarjeta de débito, pero que no cuentan con licencia bancaria. El challenger Banks que ofrecen la combinación de cuenta bancaria más tarjeta de débito y sí disponen de licencia bancaria. También ofrecen solo cuenta corriente, con la combinación de cuenta bancaria más tarjeta y licencia, disponen de una gran ventaja competitiva respecto de los neo-bancos ya que se guardan la opción de poder diversificar en cualquier momento su cartera de productos y servicios. Además, estas Fintech cuentan con el mix de producto completo que competir de tú a tú con la banca tradicional. ofreciendo de un lado productos de pasivo para su balance como las cuentas corrientes y de ahorro, y de otro lado, productos de activo para su balance como préstamos personales, hipotecas o líneas de crédito. La gestión de las finanzas personales con servicios y soluciones para que estos puedan administrar debidamente su dinero, generalmente vía app y web.

También estas Fintech ofrecen los servicios de pagos y transacciones, siempre y cuando estas se relacionen de forma digital, por ejemplo, la infraestructura y redes de pago que recoge todas las empresas Fintech que no prestan servicio directamente al usuario final (ya sea receptor o emisor del pago) sino que dan soporte a las Fintech e instituciones financieras tradicionales en sus procesos de pago y transferencia de fondos. Los emisores y agregadores de tarjetas son empresas tradicionales calificadas como Fintech que cuentan con las tarjetas de crédito y débito físicas como parte de su propuesta de valor que además, contiene a los emisores de tarjetas de pre -pago, muy extendidas en los últimos años gracias a sus bajas comisiones y sus aplicaciones móviles asociadas, y los agregadores de tarjetas como Coin, que unen en un único elemento físico varias tarjetas distintas. También los pagos de factura telefónica, esta permite pagar de forma online mediante un smartphone apalancándose en los operadores de telecomunicaciones y sus redes. La forma de hacer estos pagos es cargando el importe de la compra en la factura telefónica o en su defecto en la tarjeta telefónica de pre-pago, o bien

[58] BOSCH, Op Cit, 47p.

utilizando sus p untos de recarga, tarjetas SIM y redes comerciales para proporcionar servicios de pagos móviles.

Lo anterior nos permite ver cómo, la infraestructura tecnológica, es decir, de computo, redes de telecomunicaciones, sistemas operativos, bases de datos, software y aplicaciones, son las que permiten que la población pueda acceder con agilidad y eficiencia a los servicios financieros.

5.2 Infraestructura Fintech

El tipo de tecnología que utilizan las Fintech (startups) ha permitido que diversas oportunidades de negocio se adapten a las necesidades de los usuarios. Asimismo, tiempo para quien quiera emprender un nuevo camino, invertir dinero en producción y gestionarlo al mismo tiempo. al mismo tiempo. Así que Fintech ha abierto un nuevo panorama para aquellos que quieran participar en proyectos de economía real. Ofrece a individuos y grupos la oportunidad de financiar sus proyectos mientras cosechan beneficios económicos. Estas empresas se dedican principalmente a promover y simplificar los servicios bancarios y de seguros para los usuarios. Para lograr este objetivo, utilizan tecnologías como base sobre la que operan. Análisis de datos, inteligencia artificial y blockchain.

Las Fintech operan con plataformas que han ido evolucionando poco a poco en las redes complejas que no se dedican solo a prestamistas, sino también a las transacciones de divisas entre particulares, sin la participación de una entidad financiera tradicional. El principio de la economía de plataforma por medio de la cual los usuarios pueden comprar una variedad de productos a revolucionado el comercio moderno. Desde eBay, pasando por Amazon hasta Airbnb, los productos y bienes se vendieron por primera vez a través de plataformas digitales.

Gracias a los avances tecnológicos se hizo posible almacenar una gran cantidad de información, que permiten ver el comportamiento de compra de los potenciales clientes, pero es la que menos atención recibe en la tecnología Fintech, pues como ya lo hemos visto puede ser usado para pronosticar eventos, teniendo en cuenta los datos existentes, que se conoce como análisis predictivo.

Para Mercury Cash[59], la inteligencia artificial será muy importante para las empresas Fintech en un futuro próximo. Por ejemplo, desde el punto de vista del servicio al cliente, la máquina ya puede enviar a la persona adecuada al problema presentado después de la llamada. La llegada y el desarrollo de chatbots ha reducido el esfuerzo de los administradores al crear respuestas a preguntas sencillas. El aprendizaje automático mejorará la calidad del servicio en los próximos años. Cuanto más rápida e inteligente sea la IA, mayor será el rendimiento potencial.

[59] Mercury CASH. 5 tecnologías más utilizadas por las empresas fintech .[en línea]. 2018. Disponible en: https://blog.mercury.cash/es/2019/09/02/5-tecnologias-mas-utilizadas-por-las-empresas-fintech/

Además, para Parrondo Luz[60], la tecnología Blockchain, es una tecnología clave para las Fintech, ya que representa una cadena de bloques que contienen información y que están entrelazados entre sí. Este término se hizo popular gracias a la tecnología Bitcoin, sin embargo, la aplicación de la tecnología blockchain transciende el entorno de las criptomonedas permitiendo el futuro desarrollo de diferentes aplicaciones y servicios. Blockchain utiliza bloques que poseen una especie de «huella» o «marca» especial llamada «hash», cada hash es único y se podría comparar con una huella digital, para que un blockchain funcione debe haber bloques con cierto contenido específico: hash propio, hash del bloque anterior y datos de la transacción. Según la autora las Blockchain ofrecen un sistema en el que las transacciones son públicas y de esta manera los participantes solo encuentran una verdad, y es esa la verdad que esta codificada y está distribuida en todos los nodos de la red, además estas transacciones se aceptan si todos los usuarios validan su legitimidad.

Existen tres tipos fundamentales de Blackchain:

- Blackchain publica: es una red ala que cualquier persona puede acceder, pudiendo entonces crear bloques y participar en el proceso de consenso o de validación.
- Blackchain de consorcio: es una cadena de bloques donde el proceso de consenso es controlado por un conjunto de nodos preseleccionados.
- Blackchain privada: un conjunto de bloques en los que los permisos de escritura se mantienen centralizados en una organización.

Para David Igual,[61] las empresas Fintech proceden de la cultura de la innovación y desde las estartups creadas desde cero, con una filosofía de romper con los anteriores formatos. Conviven y se desarrollan en un contexto de redes sociales, con una cultura de compartir entre iguales más que de sumisión a una entidad poderosa como la que representan los bancos.

5.3 Mecanismos de seguridad de la información en las Fintech

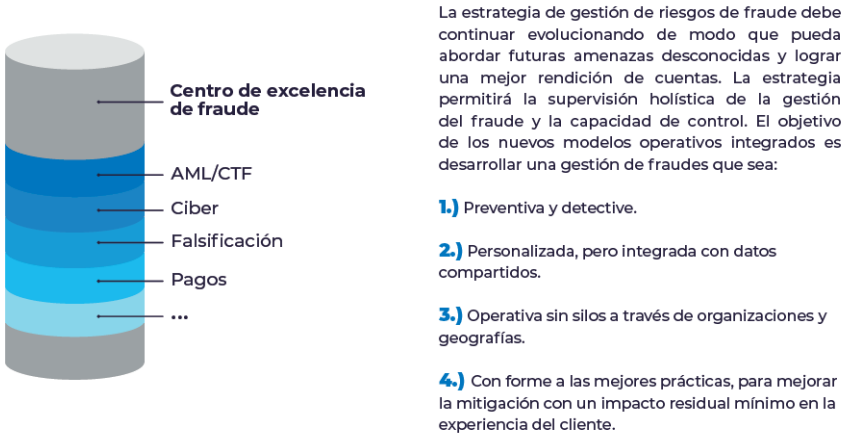
Las empresas de tecnología financiera, por otro lado, son alternativas difíciles a los sistemas bancarios tradicionales. La propuesta es muy positiva para los productos bancarios, cara y obsoleta.
Por ello las empresas de servicios financieros se han visto en la obligación de desarrollar y poner en marcha nuevos modelos operativos y plataformas con el fin

[60] PARRONDO, Luz. Tecnología Blockchain, una nueva era para la empresa. Volumen 27. Barcelona 2018. 27 p.
[61] MOLINA IGUAL, David. Lo que la tecnología hace por las finanzas. Profit. España 2016. 43 p.

de combatir los riesgos cibernéticos, haciendo uso de análisis inteligentes de la información que apoya la prevención y detección rápida de fraudes. Con el análisis de datos pueden identificar la información desencadenante para fraude, o distinguir el fraude potencial de otra actividad normal. Además, la identificación biométrica mejora y da seguridad a las identidades de los usuarios. Esto con el fin de que el cliente se sienta bien, con una experiencia rápida, no dispendiosa, pero si eficaz, que confirme con rapidez la identidad del mismo y evite las transacciones fraudulentas.

Según un estudio realizado por Asobancaria y la OEA en el año 2019 llamado: "Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina"[62], algunas empresas financieras están desarrollando centros de fusión de fraude, desde una estructura plana con departamentos independientes, realizando así: Investigaciones cibernéticas, investigaciones de seguridad física, investigaciones de equipo inteligencia, investigaciones blanqueo capital, investigaciones auditoría interna. La siguiente ilustración muestra que esta fusión es holística.

FIGURA 1: Fraude



Fuente: Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina

En este sentido, David Igual[63],, a diferencia de las pequeñas Fintech, es leal a las instituciones financieras a través de su capacidad para crear servicios altamente innovadores e intuitivos basados en nuevas tecnologías y alcance de millones de personas. Del cliente propietario de este producto. Su fortaleza económica también

[62] ASOBANCARIA, OEA 2019. Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina. 4 p.
[63] IGUAL. Op Cit, 37 p.

es muy fuerte, en pocos años se han convertido en una de las empresas más grandes del mundo por capitalización de mercado. Sin embargo, estos negocios no afectan fácilmente a los bancos. Las fortalezas de la seguridad y la regulación son precisamente las debilidades de estas grandes tecnologías, y el riesgo se ha destacado recientemente como un ejemplo de las preocupaciones de seguridad de datos de Facebook.

Por otra parte, la colaboración entre las Fintech y los bancos puede aportar valor complementario a los dos tipos de compañías. Por un lado, las Fintech, con su orientación a la tecnología y capacidad de explorar caminos nuevos, pueden generar nuevas ideas. En cambio, no disponen de licencia bancaria para determinadas operaciones, ni de capacidad para escalar un servicio hasta alcanzar la masa crítica necesaria. Entonces, en un trabajo mancomunado, Fintech y bancos pueden crear un nuevo ecosistema que les permita cubrir mejor las necesidades de sus clientes.

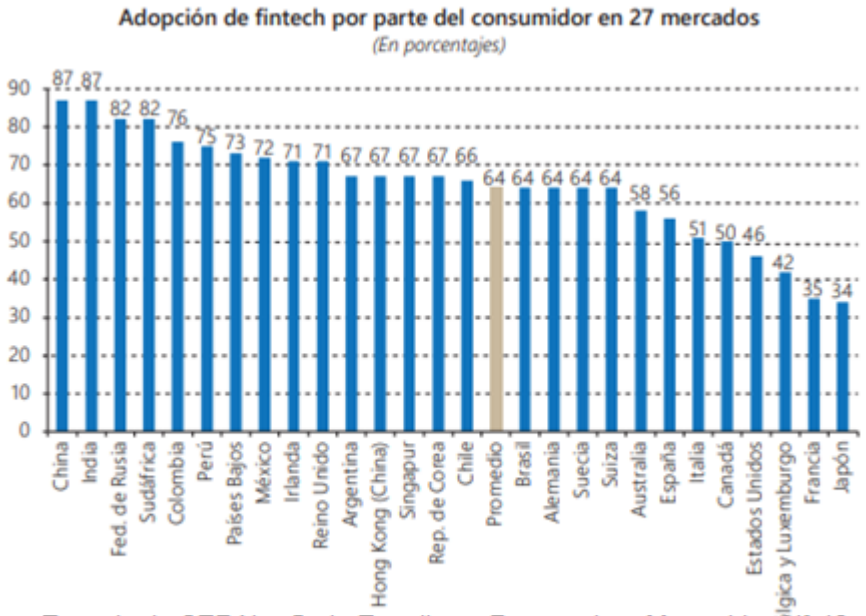
Todo lo anterior, nos deja ver con claridad que los cambios en el sector financiero son cada vez más intensos, ya que los productos bancarios necesitan ser reinventados para responder a las necesidades de los nuevos clientes digitales, que encuentran en muchos bancos estructuras ineficientes. Girar la mirada hacia un nuevo cambio digital e innovación tecnológica, infraestructura, seguridad y operatividad, genera una apertura al modelo interno que tenía la banca en el pasado.

Por tanto, el sector bancario debe transformarse mediante servicios de reinversión. Por otro lado, los nuevos participantes hacen que los nuevos participantes realicen servicios en áreas de transacciones vecinas, como el pago de compras, remesas y microfinanzas. Este es el punto donde los bancos todavía tienen algunos anclajes a su favor. Su fortaleza es proporcionar información financiera completa del cliente y proteger los datos del cliente. Es un valor no compartido y tiene muy poca seguridad debido a ciertas tecnologías.

Es importante resaltar que a pesar de los riesgos y beneficios que implica el uso de las tecnologías, la demanda de consumidores Fintech ha aumentado significativamente; ya que los mercados emergentes a nivel mundial han aumentado la adopción de Fintech como lo vemos en la siguiente gráfica[64]:

Figura 2: Adopción de Fintech

[64] LAVALLEJA, Martín. Panorama de las Fintech. CEPAL. Paraguay 2020. 13 p.



Tomado de CEPAL - Serie Estudios y Perspectivas-Montevideo N° 48

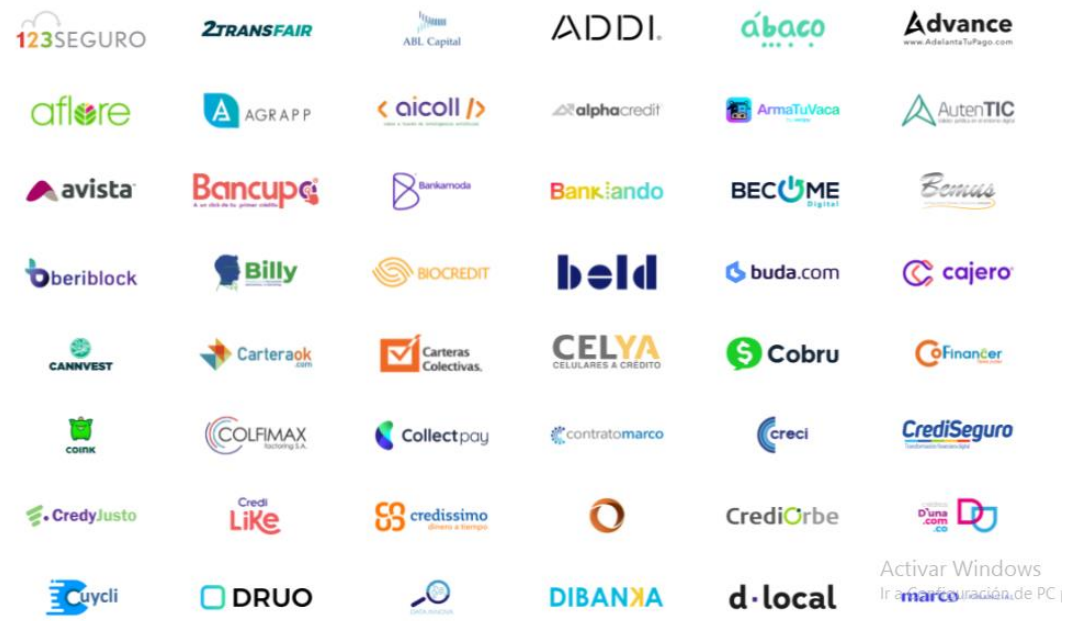
Esto nos permite ver con claridad, que la innovación de Fintech está en el proceso y en el producto. En el proceso, ya que, permite una explotación del input más importante de la industria financiera, la información, haciendo útil aquella que hasta el momento parecía no serlo. Así de esta manera puede reducir las asimetrías informativas que invaden la actividad financiera. En cuanto al producto, la Fintech puede ampliar la competitividad y eficacia, gracias a una mayor disciplina en el mercado.

5.4 Empresas Fintech en Colombia y sus beneficios

En el caso colombiano, de acuerdo a lo escrito en el portal de Colombia Fintech, tiene como propósito desarrollar un ecosistema Fintech innovador con productos y servicios financieros confiables, que mancomunadamente entre gobierno y sector financiero fortalezcan la inversión económica; todo ello bajo la premisa de la transparencia, la innovación, la seguridad, la colaboración y la inclusión.
A le fecha Colombia Fintech cuenta con 101 empresas asociadas, 3 corporativas, las cuales se presentan a continuación:

5.4.1 Empresas asociadas

Estas son las empresas asociadas a Colombia Fintech que creando una red generan un entorno dinámico, aportando al desarrollo de la industria, llegando a generar cambios que favorecen a los emprendedores y los usuarios.



FUENTE: Colombia Fintech. 2021. Disponible en: https://www.colombiafintech.co/novedades/con-50-empresas-asociadas-colombia-fintech-se-consolida-como-el-gremio-de-la-tecnologia-e-innovacion-financiera-del-pais.

FUENTE: Colombia Fintech. 2021. Disponible en: https://www.colombiafintech.co/novedades/con-50-empresas-asociadas-colombia-fintech-se-consolida-como-el-gremio-de-la-tecnologia-e-innovacion-financiera-del-pais

5.4.2 Fintech Corporativas

FUENTE: Colombia Fintech. 2021. Disponible en: https://www.colombiafintech.co/novedades/con-50-empresas-asociadas-colombia-fintech-se-consolida-como-el-gremio-de-la-tecnologia-e-innovacion-financiera-del-pais

Según el Ministerio de Hacienda y Crédito Público del Gobierno de Colombia y según datos de Banca de las Oportunidades, poco más del 78% de la población colombiana tiene, por lo menos, un producto financiero y, según el reporte de EMarket, más del 70% cuenta con un celular, por lo cual, un gran porcentaje de los colombianos debería beneficiarse de los desarrollos Fintech, pero no es así[65].
Para Felipe Lega[66], la mayoría de la población, la mayor conexión a este tipo de producto tecnológico es una tarjeta de débito, o en el mejor de los casos una aplicación de gestión de cuenta móvil, que se puede registrar en unos sencillos pasos. Puede recolectar dinero (de salarios, pensiones, beneficios estatales como "familias trabajadoras") sin pasar por una oficina (generalmente en la capital fuera del país). “Lo que está sucediendo es que estas personas van a una sucursal bancaria o a un corresponsal y retiran todo el dinero y el resto de las transacciones las realizan en efectivo, con lo cual se diluye un poco el sentido de la tecnología”.

Para finalizar es importante, reconocer los grandes beneficios que la industria Fintech presenta a la banca en lo relacionado con la tecnología financiera. Según Castellnou[67], los beneficios en función del producto financiero son:

El ahorro, ya que las gestiones que se logran hacer de manera más rápida mejoran la eficiencia empresarial, traducida principalmente en el ahorro económico y de tiempo.
La flexibilidad, permite un flujo de trabajo más ágil, que permite guardar datos, hacer operaciones a través de una financiación alternativa, es decir esta es aplicada al 100% al Fintech.
Otro beneficio es la transparencia aplicada en las empresas a través de la tecnología que, acompañada de la agilidad, puede ser gestionada y aplicada a las finanzas.

65 Colombia Fintech. Tecnología para facilitarnos la vida. [en línea]. Colombia. 2020. Disponible en: https://fiter.io/?gclid=Cj0KCQjw24qHBhCnARIsAPbdtlIeGXLxqIuLQ2-lCkUchhOdItb4cCZQGMd7AzeyQJM_dr_wT0kfQ2saAuREEALw_wcB

66 LAGA, Felipe. La industria Fintech en Colombia. 2019

67 CASTELLNOU, Rosa. Los beneficios de la tecnología Fintech para su empresa. 2019. 1 p.

La tecnología financiera también hace de las Fintech más eficientes, ya que la automatización permite la especialización y por tanto poder ofrecer servicios muy concretos con alta calidad y de manera rápida y ágil.
El uso de este tipo de tecnología mejora el análisis de los procesos, con información de datos detallados, permitiendo conseguir ventajas competitivas con otras empresas o competidores que no hacen uso de estas plataformas.

Lo anterior hace que los temas de ciberseguridad sean muy importantes para el sector financiero, ya que, los clientes y empresas deben ver siempre en el entorno digital un espacio confiable y seguro para la realización de sus interacciones. La detección de eventos de seguridad digital es una tarea diaria de las entidades bancarias, y el uso, de soluciones basadas en tecnologías digitales emergentes ha sido clave. De allí la necesidad de que para encontrar formas innovadoras de entregar servicios seguros y proporcionar mejores experiencias a los usuarios las organizaciones deben seguir enfocándose en adaptar nuevas y mejores tecnologías.

6. MODELO FINANCIERO TRADICIONAL VS LAS FINTECH EN RELACION CON EL CONTROL DE RIESGOS FINANCIEROS INFORMATICOS

Desde sus orígenes, los bancos han sido instituciones centradas en la oferta de productos, con un papel principal como intermediarios entre personas que desean guardar su dinero para ahorrar y quienes buscan financiación. Sus competidores siempre fueron otros bancos.
Para LNE [68] compendio financiero, lejos de ser una amenaza las Fintech para el sistema financiero tradicional, se ha convertido en la puerta de su transformación. Lo cual le ha implicado un giro y un cambio de mentalidad hacia los digitales que responden a las necesidades que los usuarios.

[68] LNE Compendio Financiero. Fintech: la evolución de la banca tradicional. Recuperado: 29 de mayo de 2020. Disponible en: http://lanotaeconomica.com.co/finanzas/fintech-la-evolucion-dela-banca-tradicional.html

Tabla 2. Comparativos entre el modelo financiero tradicional y las Fintech

BANCA TRADICIONAL	LAS FINTECH
Captar fondos de ahorradores o personas con superávit de capital.	El ordenador personal como herramienta de gestión financiera
Ser intermediarias financieras entre ahorradores e inversores	El internet y de la telefonía móvil, transformo los hábitos y preferencias de los consumidores, quienes están y ya familiarizados con la operativa digital, cada vez más habituados a operar por internet.
Servicio de financiación a corto, mediano y largo plazo	El rol de las redes sociales, así como la popularización de dispositivos móviles, han jugado también un papel esencial en esta transformación.
Ofrecer al cliente un lugar seguro para almacenar su liquidez y obtener rendimientos	Los tipos de interés obtenidos son más competitivos, debido a que su estructura de costes es más simple.
Contar con dos grandes ventajas: sus clientes y la existencia de una red establecida de cajeros y sucursales.	Englobar todos los servicios financieros ofrecidos a través de canales no presenciales como ordenadores, teléfonos inteligentes o tabletas.
Permitir tener un trato más cercano con el personal de la oficina.	Tiene menos letra pequeña y mayor transparencia
No es necesario el uso de aparatos electrónicos, por lo que el cliente no tiene por qué tener conocimientos informáticos.	Sin necesidad de que el cliente se desplace.
Es fácil que, con el tiempo, conozcamos al personal de la oficina y esto nos permita poder pedir algún favor en el futuro.	Atención al cliente las 24 horas.

Fuente: Propia

Se podría decir que la transición de la banca tradicional hacia la electrónica inicia con la aparición de los teléfonos y los cajeros automáticos, permitiendo la distribución retoma y la atención las 24 horas. Según Román Suarez[69] luego aparece el ordenador personal y luego la operatividad a través de internet, prestando servicios a larga distancia.

Para otros, existe una especie de batalla entre la banca tradicional y las Fintech, pero lo cierto es que las Fintech pueden con su innovación transformar el sistema bancario tradicional. Lo cierto es que hace un tiempo los bancos no se preocupaban tanto por la satisfacción del cliente pues no contaban con alternativas suficientes para ello, hoy las múltiples alternativas apuntan a que el cliente se siente satisfecho con los servicios. Es así, como Pablo Furche y otros[70], muestran el impacto comercial de las empresas Fintech a través de dimensiones específicas que se muestran en la siguiente tabla.

Tabla 3. Dimensiones de las innovaciones Fintech

[69] SUÁREZ GÓMEZ, Román. La banca electrónica en España., Tesis Universidad de La Coruña. 2013. 10-12 p.
[70] FURCHE, Pablo, MADEIRA Carlos y MARCEl Carlos. Fintech y la banca central en la encrucijada. 98- 107 p. Disponible en: https://www.estudiospublicos.cl/index.php/epublicos/article/view/2/2pág. 98- 107.

Actividad	Cambio en el Producto a través de Fintech
Pagos, transferencias y liquidaciones	Pagos móviles, billeteras digitales, divisas y contabilidades
Obtención y entrega de préstamos e intermediación financiera	Financiamiento colectivo, plataformas digitales, mayor uso de bases de datos de reconocidas fuentes parea calificación de créditos
Manejo de Riesgos	Aval en las transacciones
Apoyo al Mercado	Activos digitales en línea y verificación de la identidad
Manejo de Inversiones	Plataformas de comercio electrónico, asistentes robóticos, contratos inteligentes
Auditoría y Aspectos Legales	Revisiones mediante inteligencia artificial, consejería legal automatizada
Apoyo al cliente	Asistentes inteligentes

Fuente: elaboración propia con base en Furche

El estudio incluido en el informe Millennial Disruption Index[71] encuestó a adolescentes y adultos de hasta 30 años. A la edad de 73 años, los servicios financieros proporcionados por Google y Apple pueden ser más atractivos que los bancos normales. Estos nuevos negocios han entrado en la industria**.**

La ventaja está en cuanto que las Fintech se han convertido no en una competencia para la banca tradicional, sino en una oportunidad con un enfoque de colaboración entre ambos. La banca reconoce que culturalmente son vistos con procesos que han ralentizado la innovación, y que estas empresas pueden ayudarles a adaptar su oferta de productos y servicios a la nueva demanda de los clientes.
Goméz Silva[72], afirma, que en este acelerado proceso de integración que se ha venido dando, incluso algunos han hablado de “Fintegration”, haciendo referencia a la estrategia de compras e inversiones de los bancos en estas empresas de innovación financiera, con lo que aceleran su transformación digital, obteniendo tecnología y talento. Combinando fuerzas se pueden ofrecer nuevos productos, más rápido y a muchos más clientes. Esto lo que demuestra que juntos podrán satisfacer las necesidades de los clientes, pues la decisión mancomunada de colaboración, adquisición y alianza permitirá lograr beneficios mutuos.

[71] RITHOLTZ, Barry. The Millennial Disruption Index”, ritholtz.com. 2015. Disponible en: https://ritholtz.com/2015/04/millennial-disruption-index/.
[72] GÓMEZ SILVA, María. Fintegration: así se relacionan las fintech y los bancos. Finanzas.com. 2017 Disponible en: http://www.finanzas.com/noticias/mercados/20170309/fintegration-relacionan-fintechbancos-3576590.html.

Para Erick Rincón[73] presidente de Colombia Fintech, resalta cinco aspectos importantes en los que gracias a la tecnología el tejido empresarial, ha acercado a los consumidores a servicios financieros que siguen estando atados al modelo tradicional.

Tabla 4. Principales aspectos de la industria Fintech

Innovación	Las nuevas herramientas digitales y los avances tecnológicos, son la base de las Fintech, y sin estas sería imposible hablar de servicios en plataformas como pagos online y crowdfunding.
Confianza con el cliente	Fintech ha acortado las distancias con las instituciones financieras, pues la seguridad de los servicios generado confianza en los usuarios.
Alianzas con otras instituciones	El sistema bancario tradicional ha accedido a utilizar las herramientas de la Fintech, permitiéndoles esto acercarse y un público mucho más amplio y con necesidades específicas, integradas por la colaboración y la adquisición
Tecnología blockchain	Blockchain es un registro único y consensuado, distribuido en varios nodos de una red. Su mayor ventaja es la seguridad que ofrece ante posibles manipulaciones o fraudes.
Democratización	Un gran número de personas acceden a los servicios Fintech por su facilidad y viabilidad, pues estas se adaptan a las necesidades de los usuarios.

Fuente: elaboración propia con base Rincón

También en un análisis realizado por Sandra Varela García en 2017[74], sobre las razones de cooperación entre la banca y Fintech destaca:

- Los bancos, colaborando con empresas fintech, recortan su curva de aprendizaje, aprendiendo en mucho menos tiempo sobre negocios fundamentalmente, diferentes a los que ellos han manejado por años.
- Se promueve una cultura más innovadora y colaborativa dentro de la organización.
- Se atrae talento con potencial disruptivo, ya que la colaboración con las fintech permite que los bancos usen el talento que estas poseen al mismo tiempo que invierten en formar el recurso humano que necesitan en diferentes áreas.

[73] RINCON, Erick. Industria Fintech, Colombia. 2021. Disponible en: https://www.semana.com/economia/empresas/articulo/la-revolucion-fintech-en-colombia/202100/

[74] VALENCIA GARCÍA, Sandra. Análisis de la banca tradicional frente a la digital. Fintech o las tecno finanzas orientadas a la banca. Colombia. 2017. 43 p.

- La salida al mercado con soluciones fintech que ya han sido aprobadas por el mercado es menos arriesgado que salir con innovaciones propias, además de menos costos.

Por otra parte, las Fintech han traído una disrupción aportando y fortaleciendo grandemente el sistema financiero, Maricarmen García y Hermes Castañón[75] hablan de los principales modelos de negocios surgidos a partir de las Fintech donde los más beneficiados son los clientes:

- ✓ Los pagos digitales sin necesidad de efectivo, involucrando a diversos participantes
- ✓ Prestamos alternativos, usando modelos de scoring alternativo, con tiempos de aprobación inferiores a los tradicionales
- ✓ Gestión de finanzas personales
- ✓ Activos financieros y mercado de valores, con el surgen plataformas para invertir como bonos, capitales, derivados, monedas e instrumentos de deuda.
- ✓ Seguros o insurtech, herramientas que ayudan a la promoción venta y operación de productos y servicios de las aseguradoras.
- ✓ Financiación alternativa, para instituciones bancarias y no bancarias
- ✓ Gestión de finanzas empresariales
- ✓ Gestión patrimonial, plataformas de soluciones para la administración del patrimonio por medio de canales digitales y asesores robotizados.
- ✓ Transferencia de dinero
- ✓ Bancos digitales

Lo anteriormente dicho hace ver que las Fintech han roto las barreras creando modelos innovadores para conocer al cliente y la combinación de ambas en mutua colaboración permite que puedan sobrevivir en el mercado.

Es importante destacar que en el caso de América Latina la industria Fintech ha tenido grandes avances, por ejemplo, en México es imparable desde el 2016, según Finnovista,[76] México ha conseguido un crecimiento del 52% hasta el día de hoy, pues se destacan de manera especial las inversiones realizadas por Venture capital en dicho sector. Brasil es reconocido como el mayor Fintech hub de A.L, reconociéndose por su crecimiento en la banca digital, prestamos, seguros, trading y mercado de capitales. En Argentina, los pagos y remesas, prestamos, finanzas empresariales y tecnologías empresariales para instituciones financieras. En el caso de Chile, lideran los pagos y las remesas y el notable crecimiento tecnologías empresariales para instituciones financieras y gestión de finanzas empresariales, registrando un crecimiento del 49%.

[75] GARCIA, Maricarmen y CASTAÑON, Hermes. Diez modelos de negocio que han surgido a partir de Fintech. [en línea]. Colombia. 2019. Disponible en: https://www.delineandoestrategias.com.mx/blog-de/diez-modelos-de-negocio-que-han-surgido-a-partir-de-fintech

[76] Finnovista. Guía para Conocer una Fintech. Recuperado: 29 de mayo de 2020, desde: https://www.finnovista.com/tag/fintech-radar/

En el caso colombiano, según un informe de Asobancaria[77] ya se han dado pasos, pues la superintendencia financiera de Colombia (SFC), creo el grupo de Innovación financiera y tecnológica (InnovaSFC), con el fin de tener un mayor contacto y actuar en bien de la innovación en este sector; además este grupo hace parte de la Dirección de Investigación de la SFC, que investiga y analiza las metodologías de riesgos, supervisa y expide instrucciones normativas.

También en el 2009 fue establecido el Financial Stability Board (FSB), o Consejo de Estabilidad Financiera[78], como un órgano de coordinación internacional con el fin de promover la reforma que regulación y supervisión financiera internacional.

Por otra parte, hablando de los riesgos financieros tanto en la banca como en la Fintech funcionan de la misma manera, pero no deben tomarse así, ya que, en la banca tradicional estos se enfocan principalmente a los riesgos de crédito, de liquides, de mercado; mientras que en Fintech se enfocan hacia el riesgo cibernético, riesgo de modelo y el riesgo reputacional.

Hay varias razones por las que ha cambiado el riesgo financiero de las empresas Fintech. De hecho, estas empresas se han especializado desde el principio en la prestación de servicios financieros específicos. Al proporcionar servicios específicos, puede minimizar los riesgos que no afectan directamente a su negocio y gestionar otros niveles altos de riesgo. Además, la adopción de avances tecnológicos ha permitido a las empresas de tecnología financiera automatizar procesos, reducir el riesgo comercial y reducir el tiempo requerido para la evaluación. Por ejemplo, el riesgo de crédito se reduce gracias a los modelos de scoring que analizan de manera instantánea una gran cantidad de información del cliente obteniendo así un perfil detallado del cliente; el riesgo de mercado puede ser reducido mediante el uso de los roboadvisor que permiten a las Fintech realizar infinitas operaciones simultaneas con el fin de alcanzar los resultados deseados en sus inversiones.
Según Holgado,[79] en cuanto al riesgo operacional se da por el aumento del uso de la tecnología, que tiene como consecuencia el ciberataque que es llevado a cabo por personas ajenas a la compañía con el fin de sustraer, bloquear o destruir información que pertenece a dicha plataforma.

Otro aspecto a tener en cuenta es la seguridad de los datos almacenados, ya que la tecnología como la Big Data, por ser muy grande la cantidad de datos guardados estos están muy expuestos a ciberataque.

[77] Asobancaria. Segmento Fintech en Colombia: ¿en qué vamos? Vol. 18 (1162). 2019. 6-7 p.
[78] LÓPEZ REIG, Paula. Financial Stability Board qué es y cuáles son sus funciones. Colombia 2017. 27 p.
[79] HOLGADO, M. Los Riesgos Financieros De Las Fintech. 2017. Disponible en: https://repositorio.comillas.edu/rest/bitstreams/135609/retrieve

El riesgo legal[80] también forma parte del riesgo operacional y se define como la posibilidad de ser obligado a pagar sanciones, multas o daños punitivos como parte de las medidas de control o un acuerdo separado entre las partes. Desde una perspectiva de Fintech, los servicios que ofrecemos son obvios. Deben ser muy transparentes al proporcionar la información que procesan.

Con respecto al riesgo reputacional, Morgan JP[81] lo define como el riesgo de conducta, circunstancias, transacciones o inversiones que pudieran afectar la confianza en la integridad y competencia de los clientes, accionistas, empleados o el público en general. Para las empresas Fintech, esto sucede cuando un sistema informático bloquea el acceso de un usuario, dañando su reputación y haciendo que los usuarios pierdan la confianza en el servicio. Sus vulnerabilidades también se ven afectadas por los comentarios de las redes sociales, que incluso pueden conducir al fracaso.

En cuanto al riesgo de modelo, este afectaría las Fintech en alguna entidad bancaria si alguno de los algoritmos utilizados por la empresa funcione de manera incorrecta o desarticulada.

Lo anteriormente dicho, nos deja ver que, las Fintech no se exponen a riesgos financieros que enfatizan en las entidades bancarias, sino que gracias a las ventajas de su modelo de negocios son capaces de reducir dichos riesgos.

7. ESTRATEGIA DE LINEAMIENTOS DE SEGURIDAD PARA GARANTIZAR LA CONFIDENCIALIDAD, DISPONIBILIDAD E INTEGRIDAD DE LA INFORMACIÓN EN EL SISTEMA FINANCIERO COLOMBIANO

Para Colombia el desarrollo de una economía digital solida es muy importante, ya que esta contribuye positivamente en la prosperidad económica y social del mismo. Por ello, para su correcto funcionamiento se requiere un entorno digitan abierto y confiable acorde con el aumento dinámico de las actividades digitales de las personas. Pero, estas características se logran más efectivamente desde un enfoque de gestión del riesgo que involucra a todas las partes interesadas, lo cual es estratégico al permitirles tomar decisiones socioeconómicas informadas para maximizar las oportunidades en el entorno digital.

Según Gonzales Fajardo[82], retomando la opinión de la consultora mundial en seguridad de la información Infosecurity, con la pandemia surgieron tres tendencias con gran riesgos cibernéticos: cambios en las preferencias de los consumidores, digitalización de los bancos y migración hacia el trabajo remoto. Por lo cual la

[80] WEICHWE, Guillemo. Comité de Supervisión Bancaria de Basilea. Suiza. 2004.
[81] MORGAN, J.P.(2015). “Manual gestión de riesgo reputacional”
82 GONZALEZ, Diana. ¿Cómo está la seguridad de los servicios financieros en 2021?. [en línea]. COBIS. Financial Agility Patners. 2021. Disponible en: https://blog.cobiscorp.com/ciberseguridad-banca-2021

ciberseguridad debe convertirse en una prioridad para todos los productos y servicios prestados por los bancos.

Además, los riesgos de seguridad de la información que las entidades financieras de Colombia consideran que merecen mayor atención, sin importar el tamaño de la organización, son la pérdida y robo de activos de información clasificada (confidencial o sensible), la indisponibilidad de infraestructura crítica, y el compromiso de credenciales de usuarios privilegiados.

La seguridad es un proceso multidimensional continuo que debe ser considerado en la definición, gestión y reestructuración de los procesos empresariales y corporativos[83].. Para ello el sistema de gestión de seguridad de la Información debe estar orientado por estándares como ISO / IEC 27001 de 2013, especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de los anuncios de la organización. También incluye requisitos de gestión y evaluación de riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requisitos establecidos en ISOMEC 27001: 2013 son generales y están destinados a aplicarse a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza.

Es importante resaltar que actualmente, las 20 entidades bancarias operativas en Colombia cuentan con algún tipo de desarrollo tecnológico propio o asociaciones con Fintech, las cuales han permitido avances significativos en materia de inclusión financiera. Esta integración ha permitido a dichas compañías crear grandes innovaciones haciendo uso de la inteligencia artificial, que según Barr y Feigenbaum[84] es una parte de la ciencia que se encarga del diseño de computación inteligente, es decir, sistemas que exhiben las características que asociamos a la inteligencia en el comportamiento humano que se refiere a la comprensión del lenguaje, el aprendizaje, el razonamiento y la resolución de problemas. Esta además también cuenta con el machine learning que permite a las maquinas aprender directamente de los datos, sin que sean explícitamente programadas. En palabras de Jakhar y Kaur[85] el objetivo de machine learning se basa en entrenar a las máquinas en base a los datos y algoritmos proporcionados, para que aprendan por sí mismas a tomar decisiones. Por ello el aspecto de aprendizaje dentro del machine learning significa que los programas de machine learning intentan minimizar los errores y maximizar la probabilidad de que sus predicciones sean verdaderas.

[83] BERTOLIN, Areitio. La seguridad. Paraninfo. Cengage Learnin. 2008. 2 p.

[84] BARR y FEIGENBAUM. El Manual de Inteligencia Artificial, volumen 1. Stanford, California y Los Altos, California. EA, editores. 1981. Primero de cuatro volúmenes; otros volúmenes publicados por separado como [Barr et al., 1989] [Cohen y Feigenbaum, 1982] [Barr y Feigenbaum, 1982] .

[85] JAKHAR, D., y KAUR, I. Artificial intelligence, machine learning and deep learning: Definitions and differences. Clinical and Experimental Dermatology, 45(1), 131-132. doi:10.1111/ced.14029. 2020

Además, para Dhar y Stein el aprovechamiento de la inteligencia artificial ha permitido la prestación de servicios como el Big Data, que brindan a los grupos una mejor manera de entender el mercado y a los clientes con el análisis de la data de una manera confiable y exacta, permitiendo la reducción del fraude mediante el uso de redes de información compartida que eliminen toda posibilidad de que exista información ambigua en cuanto a la transaccionalidad y las operaciones financieras. Por ello, las Fintech satisfacen las necesidades de un vasto segmento de la población, que se ha visto desintegrado por el mercado bancario tradicional, haciendo que las empresas que se integran a él saquen gran provecho de la innovación, llegando a hacer un gran análisis de sus clientes en su totalidad: perfiles de riesgo, patrones de compras, comportamiento de pago, entre otros factores, los cuales han permitido a los startups construir una oferta de productos más asequible y completa.

Es por ello, que con la continua consolidación de este mercado en Colombia, se pueda dimensionar el impacto positivo que este tiene sobre el día a día de los usuarios con estos servicios confiables y eficientes, respondiendo a temas sensibles como la eliminación del fraude que dentro de la gestión de la seguridad de la información, es muy importante conocer y controlar los riesgos a los cuales está expuesta la información y para ello suelen adoptar metodologías que las que les brinden un marco de trabajo definido que facilite la administración de los riesgos y además permita mejorarla.

Se plantea como estrategia la metodología de análisis y gestión de riesgos MAGERIT que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para de esta forma implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados. MAGERIT se basa en analizar el impacto que puede tener para la empresa la violación de la seguridad, buscando identificar las amenazas que pueden llegar a afectar la compañía y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas.

El primer estándar metodológico implementado fue ISO / IEC 27000. Se eligió porque es un estándar de gestión de seguridad continua y se basa en la identificación de riesgos a largo plazo. Es importante porque el banco está a cargo. Brinde asistencia virtual para que los usuarios puedan ver información confidencial[86]. Por lo tanto, es importante seguir los estándares que ayudan a mantener el sistema revisado y controlado para prevenir todo tipo de ciberataques que pongan en peligro la información del cliente.

86 Intedya. ISO 27000 de 2013 y el conjunto de estándares de Seguridad de la Información. Disponible en: http://www.intedya.com/internacional/757/noticia-iso-27000-y-el-conjuntode-estandares-de-seguridad-de-la-informacion.html#:~:text=ISO

Además, se incorporará a este modelo el estándar El RFC 2196. Se trata de proporcionar una descripción general y una descripción general de la seguridad[87] de la información, incluida la seguridad de la red, la respuesta a incidentes o las políticas de seguridad. Esto es fundamental, ya que puede orientar el proceso en caso de un ciberataque al sistema financiero. Cabe destacar que la implementación en el sector bancario.
Colombia maneja diferentes tipos de visiones de seguridad para poder abordar de manera integral el tema de seguridad, tomando en cuenta los siguientes aspectos:

- Tecnologías de la información (firewalls, antivirus, prevención de intrusiones
- Bases de datos (Registros de información y patrones de comportamientos)
- Inteligencia artificial
- Análisis forense y de comportamientos
- Informes de seguridad

Además, el modelo Zero Trust apalancado con este estándar aporta a la confianza y seguridad y por ello la banca debe:

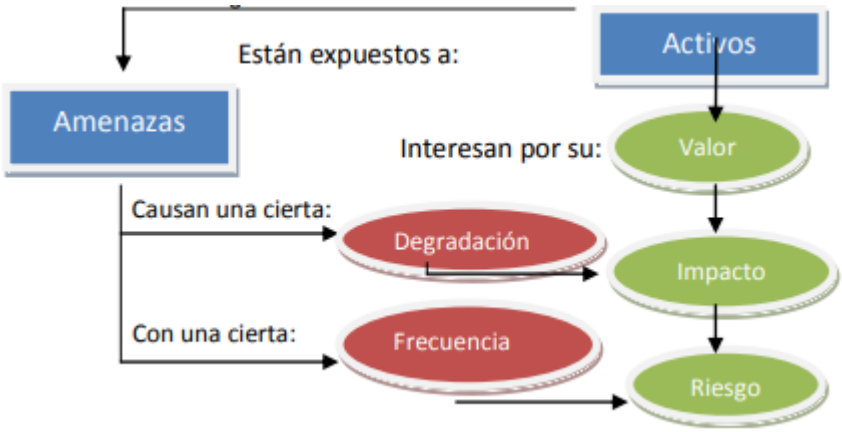
- Verificar el usuario
- Verificar su dispositivo.
- Limitar el acceso y privilegio
- Aprender y adaptar

7.1 Controles del modelo

Las fases que se tendrán en cuenta en la implementación del modelo MARGERIT son:

Figura 3. Fases del modelo Margerit

87 MOYA, S. Los Estándares de Seguridad Informática, ¿Cuál Aplica a la Industria? Y su Estado Actual. 2018. Disponible en: https://www.isamex.org/intechmx/index.php/2018/02/26/los-estandares-seguridad-informatica-aplica-a-la-industria-actual/



Tomado de Gupta, 2011

Gupta,[88] propone los siguientes pasos para aplicar dicha metodología de acuerdo a las siguientes actividades:

- Identificar activos.
- Identificar salvaguardas de seguridad existentes.
- Valorar los activos.
- Identificar amenazas.
- Valorar amenazas
- Identificar vulnerabilidades.
- Estimar vulnerabilidades.
- Identificar impacto
- Valorar impactos
- Evaluar el riesgo intrínseco
- Evaluar el riesgo efectivo

Una vez definido todo este proceso de aplicación, se procede a hablar de los controles que se van a implementar en cada una de las fases de este modelo, tomando el listado de controles de seguridad CEUPE[89]

7.1.1 Anexo A 8. Gestión de activos

[88] GUPTA, C. . Metodología para identificación y valoración de riesgos y salvaguardas en una mesa de ayuda tecnológica. 2011. 1–38 p.
89 CEUPE. Listado de controles de seguridad. Magazine. Disponible en: https://www.ceupe.com/blog/listado-de-controles-de-seguridad.html

Este permite Identificar activos, Identificar salvaguardas de seguridad existentes, y valorar los activos. Este se va a implementar, permitiendo Identificando los activos de la organización y definiendo las responsabilidades de protección adecuados, además, asegurándose que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización, por último, logrando que se evite la divulgación, modificación, retirada o destrucción de activos no autorizada e interrupciones en las actividades de la organización.

7.1.1 Anexo A 12. Seguridad en las operaciones

Identificar amenazas, identificar vulnerabilidades, identificar impacto, y estimar vulnerabilidades. Este se implementa asegurando la operación correcta y segura de los recursos de tratamiento de la información, permitiendo que las instalaciones garanticen la disponibilidad de la información en la organización frente a la perdida de datos, registrando eventos y generando evidencia, garantizar la integridad de los sistemas operativos, minimizando el riesgo de explotación de vulnerabilidades técnicas, y minimizando el impacto de las actividades de auditoría en los sistemas operativos.

7.1.1 Anexo A 14 y A 16. Adquisición, desarrollo y mantenimiento. Gestión de incidentes de seguridad.

Permite, valorar impactos, evaluar el riesgo intrínseco y evaluar el riesgo efectivo. Estos controles garantizan que la seguridad es parte integral de los sistemas de información, mantener la seguridad del software del sistema de aplicaciones y la información, evitando errores, pérdidas, modificaciones no autorizadas o mal uso de la información en las aplicaciones, además, garantizando que los eventos y debilidades en la seguridad asociados con los sistemas de información se comuniquen de modo que se puedan realizar las acciones correctivas oportunas y prontas.

Con el fin de que a los controles anteriormente mencionados se les pueda integrar el modelo Zero Trust, se deben tener en cuenta los siguientes aspectos:

- **Fase de comprobación previa de la aplicación**

  Se debe tener muy en cuenta y asegurar que la aplicación cumpla con protocolos y parametrizaciones en el proxy que se haya previamente configurado.

- **Fase de preparación del proxy de acceso**

  Realizar la configuración técnica del proxy, de modo que realizando todo el aprovisionamiento de acceso reconozca la aplicación, también se parametrizan

los derechos de seguridad y accesos específicos. Una vez realizada esta configuración se debe indicar como se desplegará a los usuarios y el tipo de ambiente donde se alojará, nube o local.

- **Fase de inscripción en laboratorio de pruebas**

Una vez parametrizado podemos destinar un ambiente de pruebas para realizar configuración de usuarios, este laboratorio o pruebas se encargarán de la etapa de validación donde verificaran el funcionamiento integral de la aplicación, cuando se realizan este tipo de pruebas se busca validar un funcionamiento integro donde se valida, el tipo de autenticación, la autenticación multifactorial, y validación que el inicio de sesión este operativo en todas las aplicaciones previamente configuradas.

- **Fase de actualización de seguridad**

Una vez se realice el proceso de pruebas, se debe determinar un proceso de seguridad avanzada, en el modelo perimetral debemos implementar lo siguiente:

1. Firewall de aplicación web (WAF) contra inyección SQL y ataques de inyecciones comunes.
2. Protección avanzada contra amenazas.
3. Control del navegador y sistemas operativos.
4. Restricción para dispositivos.
5. Bloqueo geográfico y limitaciones basadas en IP.

- **Fase de actualización de rendimiento**

Para el tema de rendimiento de la aplicación es muy viable generar la siguiente implementación para mitigar fallas de este tipo, de tal manera se debe tener en cuenta lo siguiente:

1. Almacenamiento en cache
2. Red de distribución de contenido
3. Optimización de rutas
4. Corrección de errores de reenvió
5. Replicación de paquetes

- **Fase de inscripción de usuarios externos**

Para este tipo de despliegue estas pruebas deben salir satisfactorias en la etapa de validación, se debe tener muy en cuenta que, una vez superada esta etapa se hace el despliegue de la aplicación, se procede a validar la seguridad e integridad de estas conexiones externas pues son más vulnerables que las que

están en la red local, se debe realizar todo el proceso de autenticación y monitorear muy al detalle el tema de rendimiento de la aplicación, ya que suelen afectarse por ser externos.

- **Fase de inscripción de usuarios internos**

En esta fase se despliega la autenticación a usuarios internos, se puede configurar la aplicación para que la autenticación sea a nivel de LDAP o directorio activo, una vez validada toda la configuración los usuarios podrán acceder por este proxy sin problema

- **Fase de migración a VLAN**

Para garantizar la seguridad de la aplicación frente a vulnerabilidades como malware y de este tipo debemos aislar la aplicación en una VLAN referencial que la aislé de la red local y con esto buscar en robustecer el nivel de seguridad de la aplicación.

7.3 aspectos financieros de integración

Según los controles definidos anteriormente, se hará un presupuesto de cuanto le puede costar a la banca implementarlos, esto se verá en la siguiente tabla.

Tabla 5. Costos e implementación de controles

Presupuesto		
Personal	**Modalidad**	**Valor**
Persona especializada en control A8	Virtual y presencial	2.000.000
Persona especializada en control A12	Virtual y presencial	4.000.000
Persona especializada en control A14	Virtual y presencial	8.000.000
Persona especializada en control A16	Virtual y presencial	2.000.000
TOTAL		**16.000.000**

Fuente: propia

8. RESULTADOS OBTENIDOS

El primer objetivo de este trabajo plantea explicar las Fintech desde su tecnología, infraestructura, la seguridad de la información y su operatividad, lo cual permite ver que las entidades que operan en este ámbito Fintech son emergentes pues nacen bajo el formato de startup, que se basan en la tecnología digital, haciendo un uso intensivo de las mismas, especialmente de las tecnologías de la información el análisis de datos, y las prestaciones financieras digitales. Además, su infraestructura permite evaluar los clientes y aquellos perfiles que pueden representar un riesgo, prevenir el fraude o el ciberataque, por ello, mejoran continuamente la tecnología utilizada, con el fin de brindar eficacia a las entidades buscando mejorar constantemente la seguridad, el cumplimiento de las normas facilitando y haciendo cómodo su uso.

Actualmente la información es considerada como un activo de altísimo valor, pues esta permite realizar al día millones de transacciones acelerando el crecimiento de las economías, su mal manejo, es decir la fuga de información podría hacer desplomar las acciones de compañía llevándola a la quiebra. Es por esto que una de las tareas principales de las Fintech es proteger la información de cualquier ataque tanto interno como externo. Por ello la seguridad de la información garantiza la disponibilidad y accesibilidad de la misa y la hace disponible solo para el personal autorizado, la integridad de la información permite que la información que se encuentra almacenada no sea alterada, modificada o borrada de manera parcial o total. En cuanto a la confidencialidad esta permite que los datos sean de uso privado durante al almacenamiento y envió de datos entre personal interno y externo de la compañía.

En cuanto al modelo financiero tradicional que durante tantos años domino la industria de servicios financieros, se encontró con la crisis del 2008 y con el acelerado avance de la tecnología, haciendo que entrara en una crisis, que los ha obligado a replantearse el modelo de negocio asumiendo la necesidad de adaptarse al nuevo contexto, con un negocio digital más innovador, eficiente con precios que satisfacen al cliente pues esto es lo que ofrece las Fintech; pues, estas principalmente brindan a sus clientes soluciones tecnológicas de seguridad, que permiten asegurar las transacciones evitando el fraude y garantizando que todas las operaciones se llevan a cabo de acuerdo a las disposiciones regulatorias. Se destaca la identidad digital, que permite la identificación online de los clientes, garantizando la confianza en cualquier operación financiera. También los servicios de detección del fraude en los que se realizan exhaustivas búsquedas de actividades fraudulentas a través de algoritmos.

Los modelos y estándares de seguridad de la información son herramientas importantes para ayudarlo a evaluar y diagnosticar la seguridad de la información

en su organización. Todo tipo de mejoras para proteger y proteger las vulnerabilidades de seguridad de TI deben diseñarse en una metodología completa para que puedan ser aplicadas muy fácilmente al análisis por parte de los profesionales de seguridad de TI.

Por tanto, con el fin de buscar buenas prácticas que ayuden a mejorar y administrar de manera segura los sistemas de información se plantea la implementación de la metodología Magerit, una metodología que define objetivos claros trazables y alcanzables para las organizaciones y que permite realizar un seguimiento exhaustivo del avance de los mismos, ya que, analiza los activos que son los datos y las amenazas que pueden afectar a dichos activos; también analiza la posibilidad de la materialización de una amenaza sobre dicho activo que sería la vulnerabilidad y el impacto que esta genera.
Esta metodología planteada, permite la Identificación de los activos más relevantes de la organización, además la descripción de los servicios e información que maneja. Para valorizar los activos lo realiza de manera cualitativa, teniendo en cuenta la confidencialidad, su integridad, su disponibilidad y autenticidad del servicio. La gestión de riesgos juega un papel muy importante y mediante la metodología Magerit se logra hacer una identificación clara de los activos más importantes para la organización y se realiza una valoración de riesgo

9. ENLACES DE VIDEOS

Primer Video:

https://youtu.be/DUdiMazwv_Y

Segundo Video:

https://youtu.be/3xhLUriKkxo

Tercer Video:

https://youtu.be/saqyflNMeVo

10. CONCLUSIONES

El acelerado cambio social, principalmente la digitalización ha provocado cambios en cuanto a las expectativas de los consumidores, permitiendo la aparición de un cliente digital, dotado de gran poder en sus decisiones a comparación del cliente tradicional. La comunicación entre la organización y el cliente se produce a través de canales digitales, destacando la transparencia en las relaciones financieras, cuyo principal objetivo es la satisfacción del cliente, pues al mejorar la calidad de los servicios se mejora la eficiencia en la oferta de soluciones financieras.

La industria Fintech es un eslabón importante en la provisión de servicios financieros, permitiendo la implementación de estrategias que indican la evolución de las finanzas y permitiendo que las personas tengan cada vez más opciones en su vida. Servicio y selección de productos específicos. La realización de avances tecnológicos permite a los proveedores de servicios utilizar la mejor tecnología como insumo básico para crear productos que satisfagan las necesidades de mercados cada vez más exigentes. Las principales categorías de Fintech se especializan en innovación en los segmentos relacionados con pagos, finanzas, banca digital y blockchain.

El conocimiento y experiencia de las Fintech hace que, en la gestión, tratamiento de riesgos y amenazas puedan prevenir, detectar, responder, proteger, defender y anticipar, pues al desarrollar una madurez organizacional está preparada para prevenir el fraude y la ciberseguridad. Además, de que no solo cuenta con una apropiada infraestructura inmobiliaria y tecnológica, sino de una infraestructura ética acorde con la protección que se espera de un sector que pertenece a una infraestructura critica.

La propuesta de la metodología Magerit es favorable en cuanto que, permite la identificación a profundidad de los riesgos en seguridad de la información, pues en su aplicabilidad está comprometida la evaluación del impacto que la violación de la seguridad tiene en una organización, además de señalar los riesgos existentes, identifica las amenazas que espían al sistema de información, determinando la vulnerabilidad a la que está expuesto, logrando la prevención de dicha amenaza, obteniendo resultados. Resultados, que permiten a la gestión de riesgo recomendar cuales son las medidas más acordes que deben adaptarse para conocer, prevenir, impedir, reducir o controlar los riesgos que se han identificado, comprimiendo al mínimo su potencialidad o sus posibles prejuicios.
.

11. RECOMENDACIONES

- ✓ Con el fin de lograr un bien común las Fintech y los bancos deben trabajar en conjunto, pues estas ofrecen la innovación en soluciones financieras acordes con las necesidades del mundo actual, logrando que los clientes se sientan satisfechos con sus servicios.

- ✓ Las innovaciones disruptivas tienden a crear nuevos mercados, las Fintech por tanto jugando con la imaginación, prestando servicios tecnológicos a los bancos, pueden también crear plataformas de pago que favorezcan a los para comercios digitales.

- ✓ Que algunos de los sistemas financieros tradicionales reconozcan que la colaboración que las Fintech ofrece les puede proporcionar una serie de programas, iniciativas y alianzas para fortalecer su sistema y de esta manera puedan cubrir las brechas no atendidas en los servicios que deberían ofrecer.

- ✓ Se puede reducir la pobreza, crear nuevos empleos y dar un aporte a la igualdad con la aplicabilidad de las Fintech, pues estas empoderan a los individuos y las organizaciones con servicios asequibles y seguros que fomentan el crecimiento equitativo.

- ✓ Si los bancos tienen la tarea de asegurarse de tener una estructura corporativa y de gestión de riesgo acorde, que les permita identificar y administrar dichos riesgos con la afiliación de nuevas aplicaciones tecnológicas y modelos de negocios que provienen de las Fintech.

BIBLIOGRAFÍA

ANAYA LOPEZ, Emilio. Implementación de Controles de seguridad en arquitecturas orientadas a servicios (SOA) para servicios Web. Upiiesa, México 2010. p.54.

ANDRADE, Hernán, RAMÓN OTERO Emilio. Diario Oficial LEY 1273, Colombia, 2009. p.1- 4.

ARNER, Duglas; BARBERIS, Janos y BUCKLEY, Roos. *The Evolution of Fintech: A New Post- Crisis Paradigm, 2015*

ARNER, Duglas. *FinTech: Evolution and Regulation.* Asian Institute of International Financial Law University of Hong Kong. 2016

ASOBANCARIA, OEA. Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina, 2019. p.45

Asobancaria. Segmento Fintech en Colombia: ¿en qué vamos? 18(1162), 2018. p.6-7.

ASOBANCARIA. Semana Económica. "Disrupción digital en los mercados financieros". Edición 1161. 6 de noviembre de 2018. Disponible en: https://www.asobancaria.com/wp-content/uploads/1161.pdf

Barr y Feigenbaum. El Manual de Inteligencia Artificial, volumen 1. California y Los Altos, California. EA, editores. 1981. Primero de cuatro volúmenes; otros volúmenes publicados por separado como [Barr et al., 1989] [Cohen y Feigenbaum, 1982] [Barr y Feigenbaum, 1982] .

BARRAGAN, Alejandro. Seguridad lógica usando entornos de desarrollo en aplicaciones web empresariales. [En línea]. Colombia, 2020. Disponible en: https://repository.unad.edu.co/handle/10596/33794

BERTOLIN, Areitio. La seguridad de la información. Paraninfo. Cengage Learnin. 2008. p.2

Blog especializado en Sistemas de Gestión de Seguridad de la Información. 2016. Disponible en: https://www.pmg-ssi.com/2016/05/iso-27001-2013-pasos-seguir-evaluacion-riesgos/

CAMPOS, Pablo. Hacer testeo con Burp Suite. 2017 Disponible en:https://openwebinars.net/blog/hacer-testeo-con-burp-suite/

CASTELLNOU, Rosa. Los beneficios de la tecnología Fintech para su empresa, 2009. p.1.

CASTILLO, Alexander. Entidades externas XML vulnerables. 2019 Disponible: https://seguridad-ofensiva.com/blog/owasp-top-10/owasp-top-4/

CASTRO, Santiago. Asobancaria, banca y economía. Edición 04. Colombia. 2016. p.48.

Consejo Nacional de Política Económica y Social. [en línea]. CONPES. Colombia. 2019. p.19. Disponible en: https://www.dnp.gov.co/CONPES/Paginas/conpes.aspx

Colombia Fintech. Congreso de Colombia aprueba fast-track de licencias para Fintechs. [en línea]. Bogotá. 2020. Disponible en: www.colombiafintech.co

CHISHTI, Susane y BARBERIS, Janos. El Futuro es Fintech, Una guía para inversores, emprendedores y visionarios para entender la nueva revolución tecnológica. Deusto. Ussa. 2016. p.213.

Colombia Fintech, Tecnología para facilitarnos la vida. Colombia. Ministerio de Hacienda, 2020. Disponible en: https://www.colombiafintech.co/novedades/tecnologia-para-facilitarnos-la-vida

Diario Oficial LEY 1273. Congreso de Colombia. 2009. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

DRAGONJAR, SQLMap. Herramienta Automática de Inyección SQL. [en línea]. Disponible en: https://www.dragonjar.org/sqlmap-herramienta-automatica-de-inyeccion-sql.xhtml

DURAN, María Antonia. Las sociedades especializadas en depósitos y pagos electrónicos. 2015. Disponible en: https://www.asuntoslegales.com.co/consultorio/las-sociedades-especializadas-en-depositos-y-pagos-electronicos-2237746

Ecured, Ataque Informático. [En Línea]. Colombia 2017. Disponible en: https://www.ecured.cu/Ataque_inform%C3%A1tico

FALGUNI, D. The Evolution of FinTech. Forbes. 2015. Disponible en: https://www.forbes.com/sites/falgunidesai/2015/12/13/the-evolution-of-fintech/#17e3cc1c7175

Finnovista. Guía para Conocer una Fintech. 2019. Disponible en: https://www.finnovista.com/tag/fintech-radar/

FURCHE, Pablo, MADEIRA Carlos, MARCEl Carlos. Fintech y la banca central en la encrucijada. Revista Estudios Públicos (148). [en línea]. 2018. p.39-78. Disponible en: https://www.estudiospublicos.cl/index.php/epublicos/article/view/2/2pág. 98-107.

GARCIA, Maricarmen y CASTAÑON, Hermes. Diez modelos de negocio que han surgido a partir de Fintech. [en línea]. 2019. Disponible en: https://www.delineandoestrategias.com.mx/blog-de/diez-modelos-de-negocio-que-han-surgido-a-partir-de-fintech

GÓMEZ SILVA, María. Fintegration: así se relacionan las Fintech y los bancos. [en línea]. 2017. Disponible en: http://www.finanzas.com/noticias/mercados/20170309/fintegration-relacionan-fintechbancos-3576590.html

GONZALES, Victor. La ciberseguridad. Madrid España. [en línea]. 2018. Disponible en: https://es.linkedin.com/in/victorjgonzalezarcos

GONZALEZ, Diana. ¿Cómo está la seguridad de los servicios financieros en 2021?. COBIS, Financial Agility Patners. [en línea]. 2021. disponible en: https://blog.cobiscorp.com/ciberseguridad-banca-2021

GONZALES MARTINEZ, Rafael. Committee of Sponsoring Organizations. Marco Integrado de control interno. Consejo Nacional de Política Económica y Social, 2019. p.19.

GUPTA, C. . Metodología para identificación y valoración de riesgos y salvaguardas en una mesa de ayuda tecnológica. 2011. p.1–38.

HERNÁNDEZ DÍAZ, N, LEYVA, Yelandy M y GARCÍA, Cuza, B. . Mapas cognitivos difusos para la selección de proyectos de tecnologías de la Información. México: División de Investigación de la facultad de contaduría y administración de la UNAM. Contaduría y Administración. 2013. p.95-117.

HERREA, Diego. y Vadillo. Sonia. Sandbox regulatorio América Latina e Caribe para o ecosistema FinTech e o sistema financiero. 2018. p.7.

HOLGADO, Martin, Los Riesgos Financieros De Las Fintech. [en línea]. 2017 Disponible en: https://repositorio.comillas.edu/rest/bitstreams/135609/retrieve

Intedya. ISO 27000 y el conjunto de estándares de Seguridad de la Información. [en línea] 2015. Disponible en : http://www.intedya.com/internacional/757/noticia-iso-27000-y-el-conjuntode-estandares-de-seguridad-de-la-informacion.html#:~:text=ISO

JIMENEZ, Carlos David. UNIDAD ACADÉMICA DE INGENIERÍA CIVIL, Macahala. Colombia. 2019. [En línea]. Disponible en: http://repositorio.utmachala.edu.ec/bitstream/48000/13606/1/ECUAIC-2019-SIS-DE00010.pdf.

kaspersky. QUÉ ES UN ATAQUE MAN-IN-THE-MIDDLE. 2019. Disponible en: https://latam.kaspersky.com/blog/que-es-un-ataque-man-in-the-middle/469/

LAGA, Felipe. La industria Fintech en Colombia. 2019. p.47

LAVALLEJA, Martín. Panorama de las Fintech. CEPAL. Paraguay. 2020. p.13.

LNE Compendio Financiero. Fintech: la evolución de la banca tradicional. [en línea] 2019 disponible en: http://lanotaeconomica.com.co/finanzas/fintech-la-evolucion-dela-banca-tradicional.html

LÓPEZ NEIRA, Agustín, RUIZ SPOHR, Javier. El portal de ISSO 27001 en español. [en línea]. ISSO 27000 de 2013. Disponible en: https://www.iso27000.es/index.html

LÓPEZ REIG, Paula. Financial Stability Board qué es y cuáles son sus funciones. Colombia 2017. p. 27.

LÓPEZ, Esteban. Crowdlending.es ¿Qué es Fintech?.[en línea]. Disponible en: https://www.crowdlending.es/blog/que-es-fintech

McAfee. McAfee Vulnerability Manager. [en línea]. 2018. Disponible en: https://www.websecurityworks.com/datasheets/ds_mcafee_vulnerability_manager.pdf

Mercury Cash Blog. 5 TECNOLOGÍAS MÁS UTILIZADAS POR LAS EMPRESAS FINTECH. 2018. Disponible en: https://blog.mercury.cash/es/2019/09/02/5-tecnologias-mas-utilizadas-por-las-empresas-fintech/

MOLINA IGUAL, David. Lo que la tecnología hace por las finanzas. Profit. España, 2016. p.43.

MORGAN, J.P. Manual gestión de riesgo reputacional. [en línea]. Buenos Aires. 2015. p.25. Disponible en: https://studylib.es/doc/7312448/manual-de-gesti%C3%B3n-del-riesgo-reputacional-final-2015

MOYA, S. Los Estándares de Seguridad Informática, ¿Cuál Aplica a la Industria? Y su Estado Actual. [en línea]. 2018 Disponible en: https://www.isamex.org/intechmx/index.php/2018/02/26/los-estandares-seguridad-informatica-aplica-a-la-industria-actual/

NOGUERA, David. Cabeceras HTTP más comunes. [en línea]. Colombia. 2020. Disponible en: https://www.webempresa.com/blog/cabeceras-http-mas-comunes.html

NOYA, ELoi. ¿Es el Fintech el mayor desafío que afronta la banca? [en línea]. 2016. p.4. Disponible en: https://www.harvard-deusto.com/es-el-fintech-el-mayor-desafio-que-afronta-la-banca

ORTIZ, Ángel Eulises. HostDimeBlog. Historia de las Fintech, origen, evolución. [en línea]. 2020. Disponible en: https://blog.hostdime.com.co/historia-de-las-fintechorigen-evolucion/

PARRONDO, Luz. Tecnología Blockchain, una nueva era para la empresa. Revista de Contabilidad y dirección. Volumen 27. Barcelona 2018. p.27.

RAMIREZ, Javier. Retos regulatorios de las Fintech 3.0, en busca del equilibrio entre estabilidad, innovación y competitividad. 2000. p.21. Disponible en: https://newdirection.online/2018-publications-pdf/NDreportFinTech.pdf

RINCON, Erick. La revolución Fintech en Colombia. [en línea]. Colombia 2021. Disponible en: https://www.semana.com/economia/empresas/articulo/la-revolucion-fintech-en-colombia/202100/

RITHOLTZ, Barry. The Millennial Disruption Index", ritholtz.com. [en línea]. 2015. Disponible en: https://ritholtz.com/2015/04/millennial-disruption-index/

RIVERA, Víctor. El sistema financiero requiere productos nuevos y especializados. Revista semana. [en línea]. 2021. Disponible en: https://www.semana.com/economia/articulo/sistema-financiero-en-colombia-tendencias-y-futuro-de-la-banca/309392/

RODRÍGUEZ, Ivan. ¿Qué es Fintech, tecnología financiera y cuál es su importancia?. Colombia. 2020

ROJAS, L. La revolución de las empresas FinTech y el futuro de la Banca. Disrupción tecnológica en el sector financiero. Políticas públicas y transformación productiva, 24. [en línea]. Caracas: CAF. 2016. Disponible en: http://scioteca.caf.com/handle/123456789/976

SEMANA. La banca digital transforma la vida de los usuarios. [en línea]. Abril 15 de 2021. Disponible en: HTTPS://WWW.SEMANA.COM/TECNOLOGIA/ARTICULO/COMO-TRANSFORMA-LA-VIDA-DE-LAS-PERSONAS-LA-BANCA-DIGITAL/278826/

SINGAPURWOKO, A. Do Financial Technology Startups Disrupt Business and Performance of Financial Institutions in indonesia? International Journal of Business & Management Science, 9, 2019. p.67-81.

SKAN, Dickerson y MASOOD. Fintech, Regtech y la importancia de la ciberseguridad.2014. p.38.

SUÁREZ GÓMEZ, Román. La banca electrónica en España, Tesis Universidad de La Coruña, 2013. p.10-12.

SUIN Sistema Único de Información Normativa, DIARIO OFICIAL. AÑO CLIII. N. 50570. 20, Abril, 2018. p.39.

TARAZONA, Cesar, Amenazas informáticas y seguridad de la información.
TENABLE. 2020. Nessus Profesional. p.137. Unisdr. 2017. Disponible en: https://www.unisdr.org/2004/campaign/booklet-spa/page9-spa.pdf)

VALENCIA GARCÍA, Sandra. Análisis de la banca tradicional frente a la digital. Fintech o las tecno finanzas orientadas a la banca. 2017. p.43.

VASILLEJA, Tatiana & LUKANOVA, Kristina. “Commercial Banks and Fintech Companies in the Digital Transformation: Challenges for the Future”. Journal of Business Management. 2016. vol. 11. p.25-33.

WEICHWE, Guillemo. Comité de Supervisión Bancaria de Basilea. Suiza. 2004.